Global Cyber Bi-Weekly Report by INSS 1 November, 2019

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

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

ISRAEL

Israeli tech companies raise $2.24 billion in third quarter, most since 2013

Israeli tech firms raised $2.24 billion in 142 deals in the third quarter, marked by the most deals made and the highest amount of capital since 2013, and reaching 37 percent more than the third quarter in 2018. The six largest deals totaled $841 million, led by $200 million raised by the cybersecurity firm Cyberreason. The software sector raised $1.4 billion in 52 deals, followed by life sciences with $350 million, and clean tech with $85 million. Although early stage companies raised 30 percent more than the third quarter of 2018, IVC Research Center noted, capital investment in such companies have declined over the past year.

https://bit.ly/2MY5Ykz

WhatsApp sues Israel's NSO for allegedly helping spies hack phones around the world

The messaging service WhatsApp, a subsidiary of Facebook, filed a lawsuit against the Israeli surveillance firm NSO Group. WhatsApp accused NSO of aiding government hacking of about 1,400 users across 20 countries, including Mexico, the UAE, and Bahrain, targeting diplomats, political protesters, journalists, and government officials. WhatsApp stated its video calling system was exploited in order to employ the malware and, in turn, breach the mobile devices of the targeted users. "In the strongest possible terms, we dispute today's allegations and will vigorously fight them, NSO said in a statement. The sole purpose of NSO is to provide technology to licensed

government intelligence and law enforcement agencies to help them fight terrorism and serious crime."

https://reut.rs/2qWnDRk

https://cnet.co/2BSl051

Fortinet buys Israeli cybersecurity company enSilo

The US security solutions firm Fortinet will acquire the Herzliya-based cybersecurity company enSilo for an undisclosed amount, estimated to be in the "tens of millions." Founded in 2014, enSilo specializes in endpoint security solutions. "enSilo's information protection platform safeguards end user stations and stops malicious attacks in real time before they occur and while they are taking place, while reducing the time it takes to detect an event and hedging the response costs in the event of an attack. This is achieved through full orchestration of prevention, automatic detection, halting, and taking automatic counter measures against advanced malware and ransomware. The platform can be applied on the cloud or within an organization, and it supports a large number of users."

https://bit.ly/32ZGRDI

Spy games: The dark side of the web

The Israeli Security Agency (ISA) recently revealed an uncovered network utilized to recruit individuals in Israel from the districts of Judea and Samaria and the Gaza strip. The network was administered by a Syrian constituent, functioning through social media. Following the initial phase of "raising a connection," in which the recruited individual's commitment in delivering information is established, they were transferred by means of messaging apps to a different communication channel. Some of the recruitment objectives included "staging terrorist attacks," gathering "positive intelligence" regarding "infrastructures, the social characteristics of the country, the political situation, and so forth." Such activities have become prevalent through social media—"technological contact"—often enabling the dissemination of knowledge and tools rendered from the Darknet, and for the purpose of recruiting.

https://bit.ly/36dBrqB

UNITED STATES

FCC chair pitches rules to block Huawei, ZTE

The Federal Communications Commission (FCC) revealed that it might ban US communications companies from using federal subsidies to buy Huawei and ZTE equipment and services. This would avert communication companies from exhausting the FCC's $8.5 billion Universal Service Fund from purchasing equipment that pose a threat to national security. This aligns with the Trump administration's ongoing efforts in blocking the use of Chinese-owned communication equipment and services. As the upgrade to 5G networks evolve, in addition to Chinese laws, such as those requiring companies to comply with Chinese intelligence departments, the risk to national security is heightened. This proposal would also require companies to remove Huawei and ZTE equipment, which Rural Wireless Association assesses it would cost $1 billion to eradicate and replace equipment purchased from Huawei and ZTE. The Senate Commerce Committee approved legislation that would provide $700 million in grant funds to help remove Huawei equipment.
https://bit.ly/2Wo0rqF

New contract will help communication during disasters

The Department of Homeland Security (DHS) awarded a single contract, worth up to an estimated $325 million, to CSRA, an affiliate of General Dynamics Information Technology. CSRA will work with "DHS Cybersecurity and Infrastructure Security Agency's Emergency Communications Division to provide priority telecommunications services (PTS) to [improve] communication during disaster response," in addition to supporting the agency when implementing 5G network technology.
https://bit.ly/2WrII1v

What is going on with the Cyber Command's unified platform

The next phase for Cyber Command's unified platform program is "an environment for consolidating applications and developing new tools." The unified platform will consolidate and standardize tools and systems of all the organizations under the Cyber Command, and, in turn, increase interoperability and information sharing. Five companies were awarded subcontracts under the program Cyber Enterprise Services, while Northrop Grumman was awarded $54 million system coordinator contract for the "software factory" program.
https://bit.ly/2PshaaU

US cyberattack against Iran

According to Reuters and two US officials—in response to the attacks against oil facilities in Saudi Arabia a year ago—the US initiated an operation against Iran in late September known as "cyber revenge," suggested to be targeting Tehran's propaganda efforts. "One of the officials said the strike affected physical hardware, but did not provide further details. It highlights how President Donald Trump's administration has been trying to counter what it sees as Iranian aggression without spiraling into a broader conflict," Reuters stated. Although the operation seems limited, it could take months to determine the actual impact. Reuters also reported that a hacking group seemingly associated with Iran hacked the United States this month, in attempt to infiltrate email accounts related to Trump's re-election campaign.
https://bit.ly/2qQavwS

How Microsoft's newest PC could pave the way for the future of computers

Surface Pro 7 and Surface Pro X, Microsoft's next generation in its line of PCs were unveiled at its recent tech keynotes. The latter is powered by Microsoft SQ1, "a central processing unit that's an entirely different species of computer chip than the typical power-hungry Intel processor found in the vast majority of Windows machines today." This is the first Surface Pro to use a "chip

optimized for mobile devices," which was designed by Microsoft and Qualcomm over three years.
https://bit.ly/2WlZAa0

Top civilian cybersecurity official exiting post

Kevin McAleenan, acting secretary of the Department of Homeland Security (DHS) is leaving his post. The replacement—which has yet to be named by President Trump—will be the third secretary for the DHS. McAleenan oversaw different activities, including leading civilian agencies on cyber and election security responsibilities. President Trump tweeted McAleenan's desire to "spend more time with his family and go to the private sector."
https://bit.ly/32VV8Bg

EUROPE

German automation giant still down after ransomware attack

The German company Pilz, one of the world's biggest automation tool producers, is still incapacitated as a result of a ransomware attack. Since mid-October, all server and PC workstations, including the communication network of the company, have been affected worldwide. The firm offers a range of products vital to automate industrial environments. The company was forced to notify the prosecutor's office and the Federal Office for Security in Information Technology after the latest attack.
http://bit.ly/2BFnGTC
https://bit.ly/2WrFefI

EU Data Regulator finds "serious concerns" over Microsoft contracts

Microsoft's contracts with EU agencies are found to have "significant scope for improvement" where it comes to protecting citizens' data. The European Data Protection Supervisor (EDPS) began an investigation into the degree of compliance with the set of General Data Protection Regulations that were

introduced last year. Agencies such as the European Commission outsource the processing of large amounts of citizens' personal data to software and services groups such as Microsoft. The regulations describe that the EU agencies remain accountable, meaning they are obliged to ensure compliance of their arrangements with the data processors— in this case, Microsoft. Preliminary results indicate that there is reason for concern over compliance.
http://bit.ly/360RJmB

UK Defense Agency DASA to host tech competition to boost UK "precrime" industry, tackle fake news

Roughly 30 groups funded by the UK government will join the competition in early November. The aim of the Defense and Security Accelerator (DASA) is to innovate the UK defense industry by promoting the creation of predictive technologies to counter terrorist attacks and to spot alleged fake news. A total of 2.4 million pounds in funding is made available to the competing groups. The events follows a trend of the British government to rely on artificial intelligence for security and administrative matters.
https://bit.ly/31SKcmM

Georgia hit by massive cyberattack

In Georgia, a large-scale cyberattack has caused more than 2,000 websites to crash as well as the state broadcaster. In addition, court websites containing case materials and personal data have also been hacked. In most cases, website home pages were replaced with an image of former Georgian president, Mikheil Saakashvili, with the caption "I'll be back." The origin of the attack is currently unknown and is under investigation. Numerous journalists have claimed that Russia may have been behind the attack given that the Georgian government websites are poorly protected and vulnerable to attack. More than 15,000 websites were affected, including that of the president, non-government organizations, and private companies. Irakli Chikhladze, head of the news at Imedi TV station, posted on Facebook that there was no signal, and the station was unable to broadcast. Both Imedi and another network,

Maestro, were affected, he said. Imedi TV was paralyzed for just under an hour while Maestro's computers and other equipment were reportedly damaged or destroyed. "The scale of this attack is something we haven't seen before," said Prof. Alan Woodward, a cybersecurity expert at Surrey University. "With the scale and the nature of the targets, it's difficult not to conclude that this was a state-sponsored attack." Prof Woodward added that while the disruption caused had been "significant," critical national infrastructure did not appear to have been affected.

http://bit.ly/2JxJNzA

https://bit.ly/2JxPxJE

Without naming Huawei, European Union warns against 5G firms from "hostile" powers

The European Union has warned of increased cyberattacks by state-backed entities and groups from outside the European Union and said that the risks posed by telecoms equipment suppliers that have a significant market share should be assessed. The comments came in a report prepared by EU member states on cybersecurity risks to next-generation 5G mobile networks, whose timely launch is crucial to the bloc's competitiveness in an increasingly networked world. While the report does not name any specific country or company, observers have frequently cited China and the world's biggest telecoms equipment vendor, Huawei Technologies, as potential threats. "Among the various potential actors, non-EU states or state-backed are considered as the most serious ones and the most likely to target 5G networks," the European Commission and Finland, which currently holds the rotating EU presidency, said. In this context of increased exposure to attacks facilitated by suppliers, the risk profile of individual suppliers will become particularly important, including the likelihood of the supplier being subject to interference from a non-EU country The US government wants Europe to ban Huawei's equipment, because it says it can be used by Beijing for spying, something the company has repeatedly denied. Fifth-generation networks will

hook up billions of devices, sensors, and cameras used in futuristic "smart" cities, homes, and offices. With that ubiquity, security becomes an even more pressing need than it is in existing networks. The European Union will seek to come up with a so-called toolbox of measures by the end of the year, to address cybersecurity risks at both national and EU levels.
https://nyti.ms/36ir5FV

RUSSIA

Russian government hacking group now becomes a trend

An unknown hacker gang has been attacking under the guise of the notorious Russian hacking group, which was believed to be sponsored by the Russian authorities and was involved in multiple hacking attacks, including the meddling in the 2016 US elections. According to cyber analysts, a group of criminals has been launching DDoS attacks against companies in the financial sector and demanding ransom payments while posing as Fancy Bear, the infamous hacking group associated with the Russian government, known for apparent meddling in US elections in 2016. According to one specialist, the group is launching large-scale, multi-vector demo DDoS attacks when they send the ransom letter. The group has been sending ransom letters on behalf of the Fancy Bear hacking group, asking for payments in bitcoin. However, according to the analysts, it is worth mentioning that they are not the real Fancy Bear group. Russia's elite cyber-espionage and hacking unit have never been known to launch DDoS attacks. Their targets usually include embassies, NATO bases, US political parties, and government agencies. Other groups did not bother imitating better known hacking groups and tried making a name for themselves. Some of the better known and impudent Russian hacking groups that "dangle around" the internet are Kadyrovtsy (named after Chechnyan security forces), RedDoor, ezBTC, Borya Collective, Stealth Ravens, XMR Squad, ZZb00t, Meridian Collective, Xball Team, and Collective Amadeus.
https://zd.net/2Nc5qXj

"Fake news" problem solved—Russian style

The Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) is to build online registry for "fake news" internet sources. According to the bill, initiated and signed in March 2019 by Russian President Vladimir Putin in his struggle against "fake news agencies" and against information considered as "offending the state and the Russian leadership," Roskomnadzor will block internet sites, news agencies, and personal opinions online, that it considers either fake or insulting and inappropriate for the reputation of the Russian state and the leader of its government.

http://bit.ly/340tALe

United Nations to produce a common anti-Russian cyber front

Twenty-seven countries have signed a joint agreement condemning Russia's aggressive and unfair behavior on the internet. According to the statement, released at the United Nations and ahead of the beginning of the UN General Assembly's General Debate, countries should behave in cyber space according to international law. While views of what constitutes acceptable state-sponsored hacking vary, the United States, for instance, and its allies generally agree on basic rules. It is fair game for intelligence services to hack targets purely to spy and to attack military targets, but attacking civilian infrastructure or to give a country an economic advantage is off limits. In particular, the document blames Russia for creating the infamous NotPetya ransomware worm, which spiraled out of control and locked computers around the world. Russia has been repeatedly accused of hacking political campaigns to meddle in multiple elections to favor candidates it perceives as more friendly to the Kremlin, including Ukraine in 2014, the United States in 2016, and France in 2017.

https://cnn.it/2Wb37If

Check Point: Russia has managed to build a massive "cyberattack machine"

The US director of National Intelligence has appointed an Election Threats Executive, explaining that election security is now "a top priority for the intelligence community—which must bring the strongest level of support to this critical issue." This decision came on the background of a recently released new report from the cybersecurity powerhouse Check Point, which clearly and confidently states that "it is unequivocally clear to us, that the Russians invested a significant amount of money and effort in the first half of this year (2019) to build large-scale espionage capabilities. Given the timing, the unique operational security design, and sheer volume of resource investment seen." Check Point warns, "we may see such an attack carried out near the 2020 U.S. Elections." Check Point stresses that Russia managed to build a "cyberattack machine," extensively organized, with staggering investments. And the most chilling finding is that Russia has built its ecosystem to ensure resilience, with cost being no object. It has formed a fire-walled structure designed to attack in waves. Check Point believes this has been a decade or more in the making, rendering concerted Russian attacks on the United States in 2020 "almost impossible" to defend against.
http://bit.ly/2Wfc8jC

Two Israeli cyber powerhouses demonstrate: all Russian hacking groups are state-sponsored

A "map" of connections using code matches and similarities, conducted by two Israeli companies, 'Check Point' and Intezer, have revealed an impressive picture rendering almost all Russian hacking groups connected to Russian government authorities. The map reveals the actual connection of the Russian hacking groups with Russia's intelligence and security agencies. In particular, the revelation shows direct connection to the Russian Military Intelligence (GRU), the Foreign Intelligence Agency (SV), and the Federal Security Structure (FSB). However, more striking, according to the results, is that those distinct hacking groups and their operations also hint at the notoriously cutthroat competition between Russian intelligence services—a competition that often

drives them to outdo one another in brazen acts of information-stealing, disruption, and sabotage—as they vie for the Kremlin's favor.
http://bit.ly/2N7CP5u

APAC

No info on India purchasing Israeli spyware Pegasus: MHA

In response to a Right to Information (RTI) plea, the Indian government denies planning or purchasing Pegasus – 'spyware' developed by Israeli cyber intelligence company NSO Group. Amidst the scandal and lawsuit involving WhatsApp against NSO, Indian human rights activists and journalists were confirmed by WhatsApp to be among those targeted by the software, resulting in rising tensions, in particular regarding privacy, reaching the political arena. "Pegasus allegedly exploited WhatsApp's video calling system with installing the spyware via giving missed calls to snoop on 1,400 select users globally, including over 20 people in India."
https://bit.ly/2NaxuM1

Cyber Security Strategy 2020: Civil society experts slam "national security" agenda

Australia is reviewing its national strategy, having released an early version of its 2020 cyber security strategy in September of this year. According to speakers from NetThing, held at the University of Technology Sydney, "the framing of cybersecurity had shifted from that of the original 2016 strategy issued by then-Prime Minister Malcolm Turnbull." Among the elements, the goal of an "open, free and secure internet," has been left out of the 2020 draft. Lucie Krahulcova, an Asia policy analyst at Access Now, describes two narratives in cybersecurity: national security, in terms of control like China and Russia, and the narrative of the internet, regarding "integrity of the system and the protection of individual users." Australia seems to be positioned in the middle of the two narratives, though surprisingly, some parts of the government lean toward the former narrative, according to Krahulcova.

https://zd.net/2q9Qnp5

Australian firms need to rethink their cloud security

According to a recent study released by Palo Alto Networks (PAN), reviewing cloud security in businesses with over 200 employees across the Asia Pacific, found 70% held low confidence in their cloud providers' security (CPS). Sean Duca, PAN vice president and regional chief security officer of Asia Pacific and Japan, stated that "organizations need to recognize that cloud security is a shared responsibility," and further explained that companies need to protect their information and applications stored in the cloud. Some other findings include 87% of companies either never conducted a security audit or do not conduct an audit on a yearly basis, and "more than a quarter of audits don't include cloud assets, and 79% of companies only conduct internal audits." Australian businesses are described in implementing their own cloud security measure, with 52% using more than 10 tools at the same time, 37% use threat intelligence and analytics to identify new threats and take the appropriate actions, while 16% equip themselves with real-time threat monitoring capabilities. However, Duca adds that "multiple tools creates a fragmented security posture and makes managing security more difficult—especially if the companies are using multiple clouds."
https://bit.ly/2NtX6lM

Cyberattacks are North Korea's new weapon of choice

North Korea has been supporting its weapons program using sophisticated cyberattacks to hack banks and cryptocurrency exchanges. The attacks are reportedly getting more sophisticated and harder to trace. The report, compiled by independent experts monitoring Pyongyang's compliance with international sanctions over the past six months, said that North Korea is carrying out "widespread and increasingly sophisticated" cyberattacks. The experts say these measures have so far netted the rogue state over $2 billion (€1.7 billion). The report also said that North Korea is using "increasingly sophisticated attacks to steal funds from financial institutions and

cryptocurrency exchanges to generate income." At least 35 reported instances in 17 countries of North Korea-affiliated actors attacking financial institutions and cryptocurrency exchanges are currently under investigation, according to the report. Using cyberattacks allows North Korea to "generate income in ways that are harder to trace and subject to less government oversight and regulation than the traditional banking sector." North Korea is cut off from conventional revenue sources by UN sanctions and is forbidden from exporting coal, iron, lead, textiles, and seafood.
http://bit.ly/2qPtUhr

Fancy Bear hackers targeted at least 16 athletic organizations ahead of Tokyo Olympics

Microsoft has claimed that a hacking group, backed by Russia, has targeted at least 16 national and international sporting and anti-doping organizations ahead of the 2020 Summer Olympics in Tokyo. The campaign of attacks is said to have began shortly before reports emerged about possible action by the World Anti-Doping Agency(WADA) against Russian athletes. Microsoft has not disclosed the exact specifics of the attack but stated it had notified all the targeted customers and those that it worked alongside. "Some of these attacks were successful, but the majority were not," Microsoft's Tom Burt said. The Fancy Bear group, active since 2004, is known for its cyber espionage activity and has been notorious for its involvement on the attack against the Democratic Party and attacks against Ukrainian banks and infrastructure. In addition, APT28 has a history of going after anti-doping agencies and sporting event infrastructure. It breached WADA in 2016 and leaked confidential athlete medical data. It also released the Olympic Destroyer malware targeting the 2018 Winter Olympics after the Russian team was suspended over doping charges, temporarily paralyzing IT systems, killing wifi, and taking down the Olympics' website to prevent visitors from printing tickets. Then late last year, US authorities managed to indict several Russian intelligence officers in connection with the 2016 WADA hack, although they

were never arrested. These events have brought the Olympics of 2020 and the threats being posed into focus.
http://bit.ly/2pnoudk

China adopts law on cryptography

China has passed a new cryptography law regulating how the technology will be used by the government, businesses, and private citizens once it comes into effect on January 1, 2020. The new law will be used to protect China's confidential information, such as state secrets. Under the law, confidential information of the state sent over wire and wireless communications as well as the information systems that store and dispose of this information must use core and common cryptography for their encrypted protection and security certification. China's new law will also require that institutions working on cryptography will have to establish "management systems" in order to guarantee the security of their encryption. These management systems will not be able to ask private encryption developers to turn over their source code or other proprietary information, but any business secrets they do obtain will have to be kept confidential. By passing a cryptography law, China is both allowing and encouraging the commercial development and use of encryption. However, the development, sales, and use of encryption "must not harm the state security and public interests." Those who fail to report security risks they encounter will be punished as well as anyone who provides cryptographic systems for sale which "are not examined or authenticated" by the government. China's existing cybersecurity laws already punishes the use of encryption in any way that can threaten the state and this new law includes stricter provisions.
http://bit.ly/34eBksW

MIDDLE EAST

Palestinian journalists protest against websites' shutdown

Following a court decision ordering the shutdown of more than fifty news websites, tens of Palestinian journalists demonstrated in front of a court near Ramallah in the West Bank. The news channels were depicted as criticizing the Palestinian Authority by the court. Indeed, the order stated that the websites involved were constituting threats against the national security and peace of the Palestinian Authority. This event follows a controversial law enacted in 2017 and amended in 2018 on cybersecurity, apparently restraining individual freedoms. It was denounced by Amnesty International as imposing restrictions on the freedom of press and allowing arbitrary detentions and condemnations up to fifteen years of jail for anyone criticizing the authorities on the internet, including journalists.

https://bit.ly/346zDOg

https://bit.ly/2MPrFTP

Encrypted phone company helped plan crime blogger's murder, cops and source say

Martin Kok, a criminal turned blogger, was shot to death outside a venue in Amsterdam in December 2016. It is believed that he had written about the criminal underworld, including Moroccan criminal figures who were not pleased with the coverage. James and Barrie Gillespie, known as "The Brothers" and the creators of encrypted phone company (MPC), are believed to have to entrapped and ultimately have Kok killed. "The Brothers arranged a scheme to build trust with Kok, paying him to run MPC adverts on his websites . . . and eventually, MPC put him on a plate for the Moroccans to pull the trigger." The Brothers, Christopher Hughes, another MPC employee, and Ridouan Taghi, a Moroccan gang leader allegedly linked to the killing, are wanted in connection to the murder.

https://bit.ly/31VAikn

Russian hackers cloak attacks using Iranian group

The Russian-based group Turla compromised the operations of the Iranian group OilRig in order to target other victims, which the National Cyber

Security Center (NCSC) uncovered during an investigation into an attack on a UK academic institution. It is suspected that Turla was gathering information, as well as capabilities and tools, which OilRig was stealing and utilizing, in addition to running their own operations using Iranian access, while keeping their tracks covert. "Attacks were discovered against more than 35 countries with the majority of the victims being in the Middle East. At least 20 were successfully compromised. The ambition was to steal secrets, and documents were taken from a number of targets, including governments."
https://bbc.in/2MUtoY4

UAE-based intelligence firm said recruiting IDF veterans from elite cyber unit

DarkMatter, a private intelligence firm based in the United Arab Emirates, has been recruiting graduates of the Israel Defense Forces' Unit 8200 according to a report published by Yedioth Ahronoth. The newspaper stated that several security companies in the Gulf were trying to attract former IDF officers offering very lucrative conditions of employment, including huge bonuses and luxury properties. The company created in 2015 has offices in Singapore, China, Finland, Canada, and Cyprus, where Israeli former intelligence-officers are allegedly working. According to an Associated Press Report in 2018, DarkMatter provides intelligence for the UAE government, which could become a considerable concern for Israel. Despite the fact Israel and the UAE do not have formal diplomatic relations, the two countries are reportedly developing a strong cooperation in the security field.
https://bit.ly/2ohP2vU

Thousands of Twitter accounts have been amplifying pro-Turkish propaganda

The Atlantic Council's Digital Forensic Research Lab reported that thousands of Twitter accounts have been posting pro-Turkish propaganda and disinformation, including the hashtag #BabyKillerPKK, in the past weeks. This

social media campaign is the last example of Twitter bots supporting a government military operation as it started during the Turkey's invasion in the Kurdish regions of northern Syria. Indeed, 118,000 mentions of the hashtag were registered over a period of twelve hours, making it a trending topic in Turkey. Tweets also referred to the Kurdish parties the PKK and YPG (the former is considered a terrorist organization by the United States, the latter as a US ally), claiming that both groups were murdering children without differentiation. The tweets are a tactic to influence the international public opinion on the recent events.
https://bit.ly/2BL5x6V

AFRICA

GlobeX Data launches key cybersecurity partnership in Africa for its secure data management and secure communication applications

GlobeX Data and Rockland Overseas Offshore, a multi-industry conglomerate, announce a preferred partnership, which expands its telecommunications and cybersecurity operations in Ethiopia and other regions in Africa. The partnership includes developing and investing in data centers in Ethiopia, considered the "fastest growing internet and mobile penetration in the world." Rockland Group plans to expand strategic partnerships located throughout the African Horn Region, as in Ethio-Telecom. The Ethiopian government commits to reach 100% mobile access, 54% internet access among other goals by 2030, as part of its Digital Transformation program.
https://yhoo.it/3697wA1

South Africa's banks, and its largest city are grappling with separate cyber incidents

Multiple banks were hit with "ransom-driven" DDoS attacks across the country; in particular, Johannesburg is dealing with the second breach to its network in three months. According to the South African Banking Risk

Information Center (SABRIC), the attacks are utilizing DDoS attacks and demanding a fee to stop overwhelming victims with web traffic. According to the Johannesburg-based Standard Bank, online services were restored after a short period of time, although the city's online billing and other services were going to be temporarily shut down for safety precautions. SABRIC stated that "despite the disruption, it is confident that customer impact will be kept to a minimum."

https://bit.ly/2JsQGSH

https://bit.ly/2WoJxZ5

LATIN AMERICA

Privacy: Bolsonaro announces the creation of a big data that will even record citizens' way of walking

Brazil's President Jair Bolsonaro approved two decrees that will enable the development of a national big data initiative for gathering and storing citizens' information and official documents. According to Luis Felipe Monteiro, the secretary of Information Technology and Communication in the Ministry of Economy, the purpose of this initiative is to ease citizens' access to government services. The decrees also mention that the big data will improve public management and increase the reliability of existing registrations. The data will be stored in a centralized database and its use by federal entities will not need any additional authorization. Despite the advantages of such a measure, it will represent a new challenge for public services, since combining critical data will need both protection and respect of privacy, according to Coin Telegraph experts.

https://bit.ly/36bTSMg

Argentina adopts blockchain technology for traceability in the citrus industry

The Argentine Citrus Federation (Federcitrus) started to use blockchain technology in the agency's informatics system in order to better trace fruit

export products. Using blockchain is supposed to secure transactions and make the export process more transparent and efficient. Argentina is one of the first countries to apply the blockchain technology to trace fruits. This initiative was chosen due to the difficulty to trace the citrus supply chain, one of the most fragmented and complex. It should improve the function of the whole industry and reduce counterfeiting and fraud. According to the federation, the use of blockchain could be a way for Argentina to become a leader in the citrus field.

https://bit.ly/2BNYCtK