Global Cyber Bi-Weekly Report by INSS 15 September 2019

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

Contributors: Simon Tsipis, Robin Veldwijk, Donal Byrne, Lea Abramski

ISRAEL

Exclusive: Israel needs to be ready for terrorist "dirty" cyber bomb

Former deputy head of US Cyber Command, Lt.-Gen. (ret.) Vincent Stewart, cautioned of the risk that a sophisticated attack from terrorist organizations would pose, speaking at the ICT-IDC Herzliya counter-terror conference and equated the effects to that of a "'dirty' [nuclear] bomb." Stewart further described the "persistent engagement" strategy, adopted during the Trump administration, enabling the Cyber Command more autonomy and illustrating a shift in approach against threats in the cyber domain, contrary to the previous rational, influenced more so by "fears of escalation." Stewart continued to echo the policy in the context of current US engagement with adversaries such as Russia, China, and Iran, as well as against the activities of the US intelligence community, namely in the Cyber Command's hack against Iran's intelligence unit in the Persian Gulf. In line with the "arms race" analogy (loosely speaking), Stewart discussed China's unchecked efforts and quantum computing, a category by which dominant capacity attained "would allow code-breaking and hacking at a previously unheard-of-level."
https://bit.ly/2m9cwSu

Report: Israel most likely behind wiretapping near the White House

Several former top US officials have confirmed that the FBI and other federal agencies were confident, based on detailed forensic analysis, that Israeli agents had placed cellphone surveillance devices at sensitive locations near the White House and in other sensitive locations in Washington DC, according

to a report published by Politico. The miniature "StingRay" devices were meant to spy on US President Donald Trump and his closest aides. The StingRays, technically referred to as IMSI-catchers, work by acting as regular cell towers that are then able to obtain the locations and identities of mobile devices, in addition to data and call content. According to Politico, President Trump has been notoriously careless in security protocols.
https://bit.ly/2lNckZa

Israel, Japan sign defense agreement in Tokyo

Israel and Japan signed a Memorandum of Understanding at the headquarters of the Japanese Ministry of Defense in Tokyo. The agreement will deepen and strengthen security relations between the countries and is expected to strengthen and deepen defense cooperation. This agreement emerged from a series of six partnership deals signed by the countries earlier this year in the fields of cybersecurity, digital health technologies, and the automotive industry, along with a Memorandum of Understanding on cooperating in the field of digital health. Sun D'Or airlines, a subsidiary of El Al airlines, also has unveiled new direct flights between Ben Gurion and Narita airports.
https://bit.ly/2lPsilz

Cybersecurity startup Kovrr raises $5.5 million

The cybersecurity startup Kovrr Inc., based in Tel Aviv and London, has raised $5.5 million in seed money. The company, founded in 2017, develops an artificial intelligence-based cybersecurity risk modeling service for insurers and businesses. The company's technology is able to estimate the financial losses that different cyberattacks will generate, CEO and co-founder Yakir Golan said in an interview with Calcalist.
https://bit.ly/2lPep6K

Some of Israel's largest companies chose to ignore warnings of a severe cybersecurity breach

Many top Israeli organizations and entities failed to act following a double warning regarding a security flaw in some of the VPN servers they use. The Israel National Cyber Directorate published an urgent warning regarding the vulnerabilities, along with a recommendation for every related organization utilizing the VPN servers to download a security patch or update immediately. When activist hacker Noam Rotem tested various Israeli organizations a few days later, he found many had disregarded the warning. Some organizations did not fix the vulnerability, enabling any person with a browser to access files off the server's operating system, including password and user management files. Among the organizations affected were the Ministries of Finance, Health, and Environmental Protection, University of Haifa, Bezeq, Cellcom Israel Ltd., satellite television company Yes, Israeli defense contractor Elbit Systems Ltd., car leasing companies Albar and Eldan, detergent company Sano-Bruno's Enterprises Ltd., investment houses Migdal Capital Markets and Excellence, insurance company Menora Mivtachim Holdings, investment and holding group Shlomo Group, IP communication company AudioCodes Ltd., real estate company Naaman Group, fashion retailer Castro, dairy compay Tnuva, Israel's national lottery Mifal HaPais, and advertising agency McCann Tel Aviv.
https://bit.ly/2kjpe0A

UNITED STATES

What does state-of-the-art cybersecurity look like to the Pentagon?

The Department of Defense (DoD) is issuing a new framework focused on the cybersecurity of suppliers. Although the 2017 criteria from the National Institute of Standards and Technology are required, most companies have yet to meet compliance deadlines. The new grading framework, "Cybersecurity Maturity Model Certification," will designate a value of one through five signifying basic to advanced hygiene. It is implied that the policy is in

progress, as the DoD is first meeting with experts in the industry and gaining insight. Beyond measures and controls, the threat landscape in relation to the cybersecurity of the suppliers is the defense industrial base.
https://bit.ly/2mlQSdZ

US power grid "cyber incident" was caused by hackers rebooting firewalls

In March "a first-of-its-kind" cyberattack against US power grids (impacting the Western United States) resulted in "outages lasting up to five minutes at a time at multiple low-impact generation sites." According to the recently published report issued by North American Electric Reliability Corporation (NERC), "Lesson Learned," the breach was caused by reboots, enabled by firewall vulnerabilities exploited by hackers "for hours on end." The report conveyed the necessary steps of actions, including those of power companies, which include an assessment of cybersecurity policies and procedures, initiating timely and consistent firmware updates, and overall increasing system resilience. The event occurred two years after a report issued by Symantec suggested the probability of such an occurrence. The Symantec report described the attack against the power grid in Ukraine, which was attributed to the hacking group "Dragonfly."
https://bit.ly/2lMbr36
https://bit.ly/2k9SVkw
https://ubm.io/2lTmDLk
https://bit.ly/2lYaVih

Targeting in cyber operations: FOIA release discusses considerations of US military targeting doctrine

Recent declassified and redacted materials from US Cyber Command (USCYBERCOM) pertaining to the targeting process of cyber operations allude to a relationship between cyber and conventional military force. A suggested correlation was further grounded by the "joint targeting cycle framework"

(JTC) issued in Joint Publication 3-60 in January 2013. This framework relates to the application of kinetic means across operational domains. The redacted and curated presentation from the declassified materials, "Improving Targeting Support to Cyber Operations," notably describes the cycle as "optimized for lethal effects, and therefore JTC is sub-optimized for non-lethal and temporary effects," among other implied findings. Furthermore, the effectiveness of JTC is in application of a "cyber operations specific function."
https://bit.ly/2kpR4ID

Google and YouTube will pay record $170 million for alleged violations of children's privacy law

YouTube, a subsidiary of Google LLC, was found in violation of the Federal Trade Commission's (FTC) "Children's Online Privacy Protection Act (COPPA) Rule," which was ratified in 1998, for "illegally collecting personal information from children without their parents' consent." YouTube used cookies to track viewers of the "child-directed channels," and distribute tailored ads to them, in addition to using child-directed channels that are operated by toy companies. The viewers in this case are those under the age of thirteen, in which COPPA requires disclosure of data practices and parental consent in advance from "child-directed websites and online services," such as YouTube, and "third parties, such as advertising networks," and in this case the toy companies as well. Google and YouTube's monetary penalty is $136 million to the FTC and $34 million to New York, in addition to other requirements in an effort to ensure COPPA compliance.
https://bit.ly/2ktM8lP
https://bit.ly/2lKTnpQ

EUROPE

The "best woman spy" in the United Kingdom nominated to head new cyberwarfare initiative

A "top female spy" in the United Kingdom has been nominated to head the country's new cyber warfare agency, the National Cyber Force (NCF). The individual, who cannot be named for security reasons, is a veteran of GCHQ, the controversial signals intelligence agency. The new NCF, which has a budget of £250 million, will conduct both proactive and retaliatory attacks against state and non-state actors accused of perpetrating cyberattacks against the United Kingdom. It will also target the promotion of "fake news" on social media and shut down digital platforms used by terrorists and criminals. It is scheduled for launch before the end of 2019 and will be initially staffed by 500 people, which is expected to increase to 3,000 by 2030. The NCF is the latest UK cyberwarfare initiative to be announced and has received much hype. Previous endeavors have failed to live up to official and anticipated expectations. For instance, the British Army's shadowy psyops unit 77th Brigade, which engages in online information operations among other dubious clandestine activities, has fallen short of recruiting targets ever since its launching in 2014. Furthermore, the Joint Committee on the National Security Strategy said that "We are struck by the Government's apparent lack of urgency in addressing the cyber security skills gap, which is of vital importance to both national security and the economy." The committee said the government and private sector was affected by the shortage in skilled cybersecurity workers.

http://bit.ly/2kI8251

Israel and Croatia sign cybersecurity cooperation agreement

A momentous agreement between the governments of Israel and Croatia was signed this week. The agreement aims at fostering cooperation against increased cyber activity. The agreement was signed by Croatia's Interior Minister Davor Božinović and Yigal Unna, the chief executive director of the

Cyber Technologies Unit at Israel's Ministry of Public Security. In a statement, Mr. Unna said that it had been a great honor to sign the "historic agreement" in the area of cybersecurity, which, he noted, is one of the fundamental threats facing the world today. He went onto note that cooperation is a must for all countries that share the same values. He also noted "Croatia and Israel now have a way for our two countries to also protect Europe from cyber threats." Božinović also said that the institution in Israel with which the agreement was signed was one of the leading agencies of its kind in the world. The interior minister underlined the seriousness of the problem of cybersecurity and how its international nature requires a growing effort and innovation as well as cooperation among countries. Cooperation on the national, regional, and international level is essential for proper functioning and security in a digital environment and the ministry is convinced that this agreement will contribute to the cybersecurity of Croatia, its citizens, and institutions. The Cyber Technologies Unit provides incident handling services and guidance for all civilian entities as well as critical infrastructures in the Israeli economy, and works toward increasing the resilience of the civilian cyberspace.

http://bit.ly/2mdauRn

European Union targets big tech by floating potential data rules

The European Union's new antitrust chief, Commissioner Vestager, has called for more rules to monitor how companies collect and use information. This offers the first insights into how she may use new powers to target big technology firms. A present, the EU data-protection legislation, although rigorous, does not cover how data can be used "to draw conclusions about me or to undermine democracy," Margrethe Vestager said in a speech in Copenhagen recently. "When a few companies control a lot of data about us, that can also help them influence the choices we make." Europe "may also need broader rules to make sure that the way companies collect and use data doesn't harm the fundamental values of our society," she said. This comes as

one of the first indications for how she may use her second term as competition commissioner, which comes with enhanced new laws to shape potential regulation for digital companies. Vestager's massive fines for Google and a tax crackdown on Apple have made her a much-feared enforcer for technology giants. She is also investigating how Amazon.com may handle data on rival sellers on its marketplace, and her team has been asking questions about how Facebook deals with apps and its planned new cryptocurrency, libra.

https://bloom.bg/2mfZy5D

Artificial Intelligence mimics CEO voice to scam UK energy firm out of £200k

A CEO's voice has been impersonated by criminals using artificial intelligence-based software. This was done in order to deceive an unnamed UK-based CEO into making a fraudulent transfer of £200,000, according to a report in the Wall Street Journal. Catherine Stupp reported that the CEO of a UK-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA. Rüdiger Kirsch, a fraud expert at Euler Hermes, a subsidiary Allianz SE was reported as saying that the UK CEO recognized his boss' slight German accent and the melody of his voice on the phone. The CEO made the requested transfer to a Hungarian supplier and was contacted again with assurances that the transfer was being reimbursed immediately. According to cyber experts, a huge rise in machine-learned cyber-crimes is expected in the near future. For example, the Deepfake app is able to imitate celebrities and public figures in video format; however, it takes up to seventeen hours of footage to create these videos in a convincing manner. In contrast, being able to fake voices takes fewer recordings to produce. As computing power increases, the world is starting to see that

imitations are becoming even easier to create, which paints a scary picture ahead. The case is currently under investigation by the UK authorities.
http://bit.ly/2lMjXiy

RUSSIA

Apparently, the biggest obstacle for the United States to combat Russian cyberattacks is Donald Trump

FBI Director Chris Wray stated a warning that Moscow is determined to interfere in the 2020 US elections, and Director of National Intelligence Dan Coats has warned that Vladimir Putin's regime will concoct new methods for messing with American politics in 2020. However, these warnings notwithstanding, the US intelligence and cybersecurity community is experiencing other misgivings, particularly the incumbent president's reluctance to receive any advice about enforcement and countermeasures against any future Russian meddling in the 2020 elections, saying that he does not believe that Russia interfered or will interfere in US elections in the future. Some senior officials have even been told not to raise the issue with President Trump. In the months before Kirstjen Nielsen was booted out from her post as secretary of Department of Homeland Security, she was instructed not to raise the issue of preventing Russian interference in 2020 with President Trump. The apparent atmosphere in Washington is that any talk of Russia's attempted subversion of US elections apparently irks Trump—and it should—for his election victory is indeed tainted by Moscow's intervention.
http://bit.ly/2kH7nkn

The three NATO cybersecurity dilemmas

NATO Secretary General Jens Stoltenberg says all 29 NATO member countries would respond to a cyberattack on one of them. In particular, the secretary general stated that "We have designated cyber-space as a domain in which NATO will operate and defend itself as it does in the air, land, and sea." However, the first dilemma is what to do in case of an attack on a non-NATO

member or a NATO "mere" ally? The second question is what if the attack is conducted by one state, from a territory of another? The final dilemma is were the attackers private individuals or state or state-sponsored organizations? When Estonia saw its infrastructure hit through cyberattacks in 2007, the attacks were blamed on Russia. But was it the Russian state or patriotic hackers operating within Russia? And at whose direction? Another issue that is tormenting NATO leaders is what should be considered a cyberattack. Russia is accused of turning off a power station in Ukraine in December 2015, a non-NATO member. The crippling of infrastructure is one possibility for reaching a threshold for Article 5. But what about in 2017 when Russia is alleged to have launched the Notpetya computer virus against Ukraine, but which then spilled over into other countries, including NATO members? The idea that an attack on one country is an attack on all underpins NATO, but adapting it to cyberspace raises complicated issues. During the Cold War, a missile launch or an advancing tank column would have left little doubt of what constituted an attack.

https://bbc.in/2kGsao1

Most of the cyberattacks on India come from Russia and the CIS

India, which is under a permanent threat of terrorist attacks, is steadily being cyberattacked, and the majority of the attacks originate from Russia and the ex-Soviet Commonwealth of Independent States (CIS) states. According to India's National Critical Information Infrastructure Protection Center, India's power sector faces cyberattacks with at least thirty events reported daily. As such, there are growing concerns that the country's power infrastructure could be the next target of terrorists looking to cripple India's economy. A government official said that "The attacks come from everywhere. A majority of the attacks come from Russia, and the CIS countries." The Intelligence Bureau had warned the government in 2009 that power sub-stations and regional load-power-dispatch-centers, both key components of power network, could be targeted. Power sub-stations play a critical role in the

generation, transmission, and distribution of power throughout the country. The only body responsible for the states' cybersecurity is the Indian Computer Emergency Response Team (CERT-In), which coordinates efforts on cybersecurity issues and is tasked with responding to cyberattacks, whereas the Indian National Technical Research Organization is the elite technical intelligence agency.
http://bit.ly/2lPLb7D

Russian-Canadian Arctic competition expands into cyber warfare

A new study by the University of Calgary predicts Russian interference in Canada's federal election campaign to serve what it describes as the Kremlin's long-term interest of competing against Canada in the Arctic. According to the study's assessment, Russia has a growing interest in dominating the Arctic, where it sees Canada as its main competitor. Thus, Canada is a prime target in the information wars, with Russia potentially meddling in Canada's upcoming federal elections in October 2019. The research concludes that Ottawa should be ready for a new surge in cyberattacks, disinformation, and propaganda leveled against Canada in the near future.
http://bit.ly/2lO5aE4

Russia warns Google and Facebook not to meddle in its elections

The Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) has demanded that Google and Facebook not spread any political advertising on their social networks regarding the Russian state municipal elections held on September 7–8. It was noted that if these measures are not taken, Russia will regard this as an interference in the sovereign affairs of the country and as obstruction to holding democratic elections. In this case, "the Russian side reserves the right to an adequate reaction," Roskomnadzor stated.

http://bit.ly/2kbRnXg

APAC

"Deepfake" app causes fraud and privacy fears in China

Zao, a face-swapping app that allows users to imitate famous actors or TV characters, is embroiled in a major privacy controversy in China as a clause in the app's user agreement allows developers to retain facial images and sell them to third parties without needing users' consent. The app, owned by the Chinese social media developer Momo, provides filters that allow users to pretend to be in movies by uploading pictures of themselves onto the app. It creates simulated video clips using "Deepfake" technology based on artificial intelligence (AI) that creates human image synthesis. Several lawyers have slammed the app for invading the privacy of the users, calling for its boycott. Momo has since deleted the controversial clause and issued an apology. Its updated app clause says that the transferring of data to third parties would require the user's authorization. As payment through facial recognition is now enabled across several platforms including Alipay, the mobile payment of the Alibaba Group, some users also worry that the leak of their facial images and the simulated video clips could result in potential financial losses. Ant Financial, which owns Alipay, nevertheless, said Deepfake technology cannot fraud its facial payment technology as it uses 3D facial recognition technology. The company also added that 3D facial recognition technology combines software and hardware to determine whether the facial information is generated by a photo, video, or software simulation. China is currently tightening regulations governing AI face-stitching technology.
https://bbc.in/2kucu7y

Hong Kong: Protesters using offline app Bridgefy to avoid being identified

The Hong Kong protests, which started months ago and originally were sparked by an extradition law, continue in this autonomous Chinese territory,

but have exposed the many problems faced by local residents when it comes to their rights online. The unrest in Hong Kong also highlights China's censorship. Like many other countries around the world, China wants to control the internet and impose online surveillance. What sets it apart is the efficiency with which it does this, with the Great Firewall being one of the tools the country uses. Despite this, Hong Kong is not behind this digital iron curtain, meaning that it has unrestricted access to the internet. Nevertheless, its residents are becoming increasingly aware of Beijing's surveillance, and have favored dropping communications via text messages and China's social media giant WeChat in favor of other solutions. They are using radically different solutions that do not require the internet or phone operators to function. Instead, Bridgefy, FireChat, and other apps now reportedly gaining popularity in Hong Kong employ the concept of mesh networking. These "offline" peer-to-peer apps send and receive messages via Bluetooth and Wi-Fi radios to connect directly with another device in close proximity, and onto the next until the recipient is reached. These apps also promise that mesh network nodes in between the sender and the recipient, that is, "people in the middle," cannot access the messages sent in this way, but they broadcast them even if they are not among the sender or the recipient's contacts. Bridgefy has seen its downloads grow nearly 4,000 percent over the past two months. Both apps are said to have had dramatic progress on Apple and Google's app stores.
http://bit.ly/2m3JyU2

Cyber Command's biggest VirusTotal upload looks to expose North Korean-linked malware

The US Cyber Command had uploaded malware samples that have been linked to hackers from the "Lazarus Group," which are connected to the North Korean government. These samples appear to be "HOPLIGHT," trojan malware that has been used to gather information on victims' operating systems and uses a public SSL certificate for secure communications with attackers. Many have noted that this discovery highlights that the North Korean government is

not able to remain anonymous in cyberspace. It is hoped that this discovery may change North Korea's behavior, although, according to experts, this is unlikely. The announcement comes weeks after the United Nations warned that North Korea has used dozens of cyberattacks to fund its nuclear weapons program. Hours before the US Cyber Command had posted the North Korean-linked samples online, the US secretary of state said the administration hopes to return to talks with Pyongyang in the coming days or weeks.

http://bit.ly/2kvS3ah

Reports say China devised iPhone malware campaign to track Muslims; Android and Windows devices also targeted

A malware campaign that was recently exposed is believed to have used watering-hole attacks to target iPhone users for more than two years. Furthermore, it was reportedly part of an effort to track Uyghur Muslims based in China's Xinjiang state. The campaign was broader than originally thought, and attempted to infect Android and Microsoft Windows devices as well. Citing sources with knowledge of the matter, TechCrunch on the weekend reported the campaign is the work of a state actor, most likely the Chinese government. It is believed the Chinese government has sought to keep close tabs on its Uyghur minority group for many years. A Microsoft spokesperson reportedly told Forbes that the research team that discovered and publicized the malware operation "was very specific in its blog post that the recently publicized attacks used unique iPhone exploits and they have not disclosed similar information to us." Google, meanwhile, did not provide any comment regarding its Android operating system. It was researchers at Google's Project Zero who last week revealed the targeting of iPhone in the malware operation, which attempted to infect device users with a malware implant, using exploits delivered via a small number of compromised websites.

http://bit.ly/2meBMa7

MIDDLE EAST

The Basij creates 1000 cyber battalions in Iran

Gholamreza Soleimani, commander of the Basij organization, announced the creation of 1000 cyber battalions around the country, through pro-regime user accounts on the internet. A battalion is composed of around 500 soldiers, meaning that the regime probably launched more than half a million pro-regime social accounts. He stayed silent regarding the means and budget used by the Basij organization to achieve this project. Despite the ban on most of the social networks like Twitter (since 2009), political officials still use their own social media accounts (for example, President Hassan Rohani). Soleimani also stated that "The enemy has expressed concern over the organized presence of revolutionary youth in cyberspace on several occasions, and that reflects the momentum that has been created. This presence will expand and be enhanced." However, in spite of this new initiative aiming to spread pro-regime views on the internet, Iran is likely to face difficulties since Twitter has been removing thousands of state-backed accounts lately (including accounts believed to be linked to the Iranian government).

https://bit.ly/2mddzkp

https://bit.ly/2kKD5gt

International cybercrime gang dismantled with Turkey's help

An international operation named "reWired" was conducted over a four-month period and resulted in the dismantling of a cybercrime gang, the arrest of 281 of its members, and the seizure of almost $3.7 million. The arrests took place in Turkey with the help of the Turkish authorities and in other countries (United States, Ghana, France, Italy, Japan, Kenya, Malaysia, Nigeria, and the United Kingdom). The criminal organization is accused of cybercrime, implying Business Email Compromise (BEC) schemes such as phishing. Phishing activities are attempts via email or text messages to obtain personal and sensitive information such as names, passwords, financial credentials, by pretending to be a legitimate institution (bank, public office, and so forth).

According to the FBI, phishing-related activities conducted by cyber criminals have represented a loss of around $26 billion in the past three years.
https://bit.ly/2kybxet
https://bit.ly/2kGOZYT

Egypt to work on $2.4 billion telecom network for first phase of new capital city

The Egyptian cabinet announced that the Communications Ministry will start working on a $2.4 billion (40 billion Egyptian pounds) new telecommunications network as a first step in the construction of a new capital city. This new capital city will be located to the east of Cairo. A cooperation agreement was signed between the Communications Ministry and the Administrative Capital for Urban Development (ACUD), the new capital's owner and developer. The new city will be named the New Administrative Capital and is expected to be covering almost 700 square km. The center of the new capital will include ministries and diplomatic representations, a financial district, and a residential area. The head of the ACUD, Ahmed Zaki Abdeen, declared that the company will fund the telecom network. The Egyptian government is hoping to be able to conduct its affairs from the new capital by mid-2020.
https://reut.rs/2kkMziw

Revealed: How a secret Dutch mole aided the US-Israeli Stuxnet cyberattack on Iran

Yahoo News has revealed that the Stuxnet virus attack against Iran was enabled thanks to an inside mole recruited by Dutch intelligence officers at the request of the Israelis and the Americans. Stuxnet is one of the most famous cyberattacks, renamed the "Olympic Games" and designed to slow down the progress of the Iran's Nuclear program. It certainly launched the "era of digital warfare." According to the report, an Iranian engineer was recruited by the Dutch intelligence agency (AIVD) and provided critical information helping the US developers to target Natanz's computer systems.

The mole also assisted when access was needed to implement their malware onto computer systems via a USB stick. This disclosure implies new information about the virus attack, which was always surrounded by mystery, especially regarding the involvement of the AIVD, which did not comment on the report. The CIA and the Mossad remained silent as well.
https://yhoo.it/2luqVbE

LATIN AMERICA

Venezuela paralyzed for days by power blackout that President Nicolas Maduro blames on US attack

20 out of 23 Venezuelan regions were left without electricity. The blackout of power and communications led to the stalling of schools, public offices, industries, and public transportation. It also paralyzed critical infrastructures and hospitals, causing the deaths of at least seventeen people. The National Electric Company explained that an accident at the Simon Bolivar hydroelectric power station (which supplies around 80 percent of the electricity in Venezuela) provoked the shutdown. Since then, many Venezuelan politicians have accused the United States of being responsible for the shutdown as an attempt to disrupt the Venezuelan regime. Vice President for Communications and Culture Jorge Rodriguez said Venezuela will lodge a complaint to Michelle Bachelet, the United Nations High Commissioner on Human Rights, against the United States. The United States denied its implication in the accident.
https://bit.ly/2lNQEvS
https://bit.ly/2kvPXap

Brazil records the first blockchain-based birth certificate

For the first time in history, a birth certificate was recorded with blockchain technology in Brazil. Alvaro de Medeiros Mendonça is the first child to be registered in the blockchain without also having to be recorded in a centralized registry office. This first birth certificate issued with the blockchain

technology is the result of a project launched by the Growth Tech company in partnership with IBM. Carlos Rischioto, IBM's blockchain leader in Latin America, explained that the baby's registration took place in three stages: The hospital makes a "live birth statement"; the parents then create a digital identity on Growth Tech's Notary Ledgers platform; and finally, the information is sent to the notary office to complete the certificate. The platform will allow more efficient, more transparent, and faster registration (it took only five minutes to register).

https://bit.ly/2lUzdK5

https://bit.ly/2mgZrqv