NAPIER MERIDIAN

Cyber Weekly for Scotland

For the week commencing 3rd September 2018

UK government funded, supported by Scottish Government, in partnership with the National Cyber Resilience Leaders' Board.

Scottish Government
Riaghaltas na h-Alba
gov.scot

Please use the following links to skip to the different areas of the Cyber Weekly for Scotland:

Article of the Week

Cyber resilience deadline looms for public sector. Did you know that next month (October 2018) the deadline arrives for Scottish public sector bodies to have achieved Cyber Essentials or Cyber Essentials Plus certifications? Yes, we are nearly a whole year on from the Scottish government's announcement of Scotland's Cyber Resilience Strategy – the grand plan to improve cyber security and promote cyber resilience in Scottish public sector organisations. If you haven't yet achieved the scheme's minimum level of compliance, it's not too late to start, no matter what stage you're at. With cyber security fears more heightened than ever, the Scottish Cyber Resilience scheme was developed in 2017 to lay the groundwork for the Scottish government's long-term goal of being a world leader in cyber resilience. If Scotland is to achieve this goal, its public sector must set a precedent for all others to follow. But with 60% of small businesses having been breached in the past year and with almost 40% of Scottish SMEs (small and medium-sized enterprises) spending nothing on IT security, it seems that most of the public sector is yet to act. (Holyrood)

UK News

Universities join forces with £6m cybersecurity scheme for Manchester's SMEs. The University of Manchester will be part of a new £6 million cybersecurity scheme launching today. The initiative, which will be known as the GM Cyber Foundry, is in collaboration with Manchester Metropolitan University (MMU), Lancaster University and the University of Salford. The scheme will protect Greater Manchester's small and medium-sized companies against malicious computer attacks. (University of Manchester)

Met Police cuts "unfortunate" for cyber security. AlienVault's Javvad Malik has commented in response to the Metropolitan Police declaring that they are breaking point in terms of finances, despite selling £1bn worth of property over the past six years, including the New Scotland Yard building. "It's unfortunate to see the Met Police budget being impacted at a time where acquiring cyber security skills is of utmost importance," Malik said. (Information Age)

Five Eyes to tech industry: Make access to online communications possible, or else. The attorneys-general and interior ministers of the Five Eyes nations — Australia, Canada, New Zealand, the UK and the US — have called for ICT service providers "to voluntarily establish lawful access solutions to their products and services that they create or operate in our countries". The 'Statement of Principles on Access to Evidence and Encryption' was one of the outcomes of a five country ministerial meeting held on the Australian Gold Coast on August 28 and 29. (Computer World)

Auditors name cybersecurity as chief concern. Cybersecurity tops the list of concerns for internal audit professionals across Europe, a survey has revealed. More than two-thirds of chief internal auditors from the public and private sectors said they see cybersecurity as the biggest organisational risk for 2019, according to a Chartered Institute of Internal Auditors

poll. Data security and protection (58%) and compliance (58%) were joint second in the list of risks, which was based on responses from more than 300 chief internal auditors. (Public Finance)

LGFL schools to benefit from anti-malware rollout through Malwarebytes deal. The London Grid for Learning (LGfL) believes it is driving what will be the UK's largest rollout of anti-malware software for schools. The not-for-profit trust, led by former Camden Council chief information officer John Jackson, provides high-speed uncontended broadband and associated services to schools. It has now signed a deal with anti-malware provider Malwarebytes which will see all schools on LGfL's nationwide network provided with the software at no additional cost. (Government Computing)

Highlands and Islands Enterprise has launched a series of workshops to help businesses in the north of Scotland create an effective digital strategy. Business leaders will be guided through the different digital channels and shown techniques to achieve their goals, whether that is increasing sales or raising brand awareness. Attendees will also be given an overview of social media platforms, including which ones they should prioritise and ideas for content. (Holyrood)

Meet the common enemy of accountancy bodies: Cybercrime. Some of the biggest names in the accounting sector have come together to tackle their biggest existential online threat. The CCAB (Consultative Committee of Accountancy Bodies) has released its economic crime manifesto which includes a major component aimed at tackling cybercrime in the UK. What does that mean to the wider accounting community and why it was introduced in the first place? (TechRadar)

Most UK businesses are not insured against security breaches and data loss, says study. Nearly half of senior executives not aware of what their company insurance covers them for, according to NTT Security report. With annual losses from cyber crime estimated to be topping $400bn (£291bn), you would think organisations are flocking to insurers. However, NTT Security found that only one-third of senior executives in the UK admit their companies are insured against information security breaches and data loss. This is despite the fact that 81% agree that it is 'vital' their organisation is insured against information security breaches. (Information Age)

Five reasons cyber security is more important than ever. The threat of cybercrime to businesses is rising fast. According to one estimate, by McAfee, the damages associated with cybercrime now stands at over $400 billion, up from $250 billion two years ago, with the costs incurred by UK business also running in the billions. In a bid to stave off e-criminals, organisations are increasingly investing in ramping up their digital frontiers and security protocols, however, many are still put off by the costs. (Consultancy)

Wales awarded first cybersecurity centre of excellence. Cardiff University has been named as an "academic centre of excellence" in cybersecurity research by the UK's National Cyber Security Centre (NCSC), becoming the first institution in Wales to be given this status. The award is in recognition of the internationally excellent research developed at the University over a number of years and will allow academics to feed directly into the UK Government's strategy of making the country more resilient to cyber attacks. (Software Testing News)

Most NHS Trusts Provide No Alternative to Consumer IM. The majority of England's NHS Trusts could be exposing themselves to privacy and compliance risk by using consumer IM tools, a new Freedom of Information request has revealed. Mobile solutions provider CommonTime analyzed responses from 136 of the country's 151 hospital trusts to find that over half (58%) have no policy in place to discourage the use of consumer-grade IM platforms like WhatsApp and iMessage. (Infosecurity Magazine)

Cyber claims being driven by organised criminal gangs – CFC. Malicious malware, such as NotPetya, and nation-state hacking have cast a dark shadow over the cyber insurance landscape, and while the threats are real, that's just the top of the pyramid of what's driving cyber claims. CFC Underwriting's chief innovation officer can count on one hand the number of claims that the insurance company has seen tied to high-profile nation-state attacks. (Insurance Business Magazine)

Government to spend £92m on 'study' for go-it-alone post Brexit Galileo alternative. The government is to invest £92m of public money on a study weighing up how to develop the UK's own satellite navigation system to replicate the EU's Galileo system. It says it has to consider creating the alternative if the European Commission will not let UK industry collaborate with Galileo on an equal basis. A 'go-it-alone' UK –led project has already been estimated as likely to cost at least £3.7bn. (Government Computing)

UK universities recognised for excellence in cyber security research. Three UK universities have been recognised as Academic Centres of Excellence in Cyber Security Research (ACE-CSR), leading the way in cyber security skills. The National Cyber Security Centre (NCSC) and the Engineering and Physical Sciences Research Council (ESPRC) have identified the University of Kent, King's College London, and Cardiff University as having first-rate research with scale and impact. (Advance)

Scottish Parliament

(No significant news this week)

UK Parliament

Security of UK Telecommunications. Telecommunications networks are essential for the day-to-day running of UK businesses and public services, however, concerns have been raised recently over their security. This POSTnote outlines the threats to these networks, the ability of networks to cope with disruption, and possible protective measures. Key points:

- Telecommunications (telecoms) have been recognised by the Government as one of 13 critical national infrastructure sectors – a term signifying infrastructure that is pivotal to the functioning of the UK.
- Concerns have been raised recently about the security of telecoms networks, including undersea cables that transmit an estimated 97% of global communications and $10 trillion of financial transactions every day.
- Threats to telecoms can be classified as physical or cyber, and can be malicious, non-deliberate, or the result of a natural disaster. Examples of threats to telecoms include cable damage, power and system failures, flooding and cyber-attacks.
- The Communications Act 2003 requires telecoms companies to take measures to maintain the security and resilience of their networks. While there is no mandated security and resilience standard for telecoms, Ofcom and others produce guidance on what measures telecoms companies should take in order to meet their obligations under the Communications Act.
- Physical resilience measures include investing in duplicates of infrastructure, installing back-up power supplies, and protecting infrastructure using defences around site premiers. Cyber resilience measures include preparing a data breach plan and using anti-virus software. https://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0584#fullreport

Scottish Government

Investing in Scotland's Digital Future. Businesses in Scotland are to benefit from the most advanced 'Internet of Things' (IoT) network in the UK as part of a £6 million project. The new network, called IoT Scotland, will provide a wireless sensor network for applications and

services to collect data from devices and send that data without the need for 3G/4G or Wi-Fi, supporting businesses develop new and innovative applications, changing the way they work. The network will enable all businesses to have the ability to monitor the efficiency and productivity of their assets, equipment, scheduling maintenance and improving production. For example, IoT Scotland could support wider use of smart bins that wirelessly inform local authorities when they require emptying, ensuring best use of bin lorries but also helping to reduce carbon emissions. Similarly, the network could monitor office environments to lower costs by saving energy, while reducing carbon footprints of buildings. (Scottish Government)

UK Government

New cyber unit to tackle child sex abuse in Kenya. British-built cyber centre in Nairobi will help bring paedophiles, who target and abuse vulnerable children in Kenya, to justice.

- New UK-Kenya security compact builds on our cooperation to tackle shared threats
- Money lost to corruption and hidden in Britain will be returned to the people of Kenya

British paedophiles who target and abuse vulnerable children in Kenya will be brought to justice thanks to a new cyber centre being built by Britain in Nairobi, the Prime Minister will announce today. Online child sex abuse is a global problem with images created and shared across the world, including in Kenya. This new centre will help the Kenyan police stop these images being distributed online to help protect children from being abused. The centre will also tackle a major barrier that prevents these predators being caught and prosecuted. (Prime Minister's Office, 10 Downing Street)

Tackling child sexual exploitation online. Home Secretary Sajid Javid says all technology companies must step up their efforts to tackle online child sexual exploitation. Today (Monday 3 September), the Home Secretary set out the scale of online child sexual exploitation (CSE), with a 700% increase in child abuse images being referred to the National Crime Agency (NCA) in the last five years, up to 80,000 people in the UK presenting some kind of sexual threat to children online and material increasingly featuring younger and younger children. In a speech at the headquarters of the National Society for the Prevention of Cruelty to Children (NSPCC) the Home Secretary vowed to lead the cross-Government effort in the response to the evolving threat of online CSE, including funding for law enforcement, intelligence agencies and a new prevention drive. He called on the technology industry to work in partnership with each other and with government to stop online child sexual abuse, sharing solutions and best practice to improve the response. (Home Office)

Facebook removes VPN app due to privacy concerns. Following discussions with Apple, Facebook's Onavo Mobile VPN app has been withdrawn from the iOS app store, with reports alleging this is due to possible policy violations on personal data collection. According to marketing information, the app promised to "keep you and your data safe when you browse and share information on the web." However, allegations have suggested that Facebook may be using the app to identify how users were using other third-party applications, even if the user believed the app was private. (NCSC)

Guidance for Data Breaches. More high profile data breaches have come to light recently, affecting the UK's Superdrug high street store and mobile phone provider T-Mobile. In a statement to customers, Superdrug explained how, on the 20th August 2018, they received a ransom demand believed to be from cyber criminals, claiming they had obtained customer information. Superdrug stated that they could not find any evidence of a data breach but now believe that the cyber criminals accessed their customer accounts using credentials from other websites. Superdrug believed that customer dates of birth, phone numbers and loyalty scheme details were accessed and advised customers to reset their passwords. (NCSC)

Variant of the Mirai botnet returns. In 2016, a Mirai botnet DDoS attack crippled the French telecoms provider OVH. Internet access was slowed or prevented for parts of the USA when a service provider, Dyn came under attack. One attack maxed out at 620Gbps, one of the

largest the internet has ever witnessed. Mirai worked by enslaving IoT devices. Now, the source code of a thought to be abandoned variant of the Mirai botnet has been compiled using an open source tool, Aboriginal Linux, which generates binaries for a considerable number of platforms. (NCSC)

Report on the security of UK Telecommunications by the Parliamentary Office of Science & Technology. The Parliamentary Office of Science & Technology (POST) have released a paper on the Security of UK Telecommunications which covers both the physical and cyber threats facing telecommunications networks. The paper expands on POST's May 2017 paper Cyber Security of UK Infrastructure which identifies the cyber attack threats on critical national infrastructure. The NCSC, along with many other agencies, organisations, individuals and academic institutions have worked with POST on these papers. (NCSC)

Data can save lives, but we must protect it. We're on the cusp of a digital health revolution that could see healthcare providers make better use of data to intervene earlier, provide more personalised treatment and, ultimately, reduce the cost of running our healthcare system. But patients, who are already taking a more hands-on approach to managing their own health, rightfully expect highly personal data about their bodies to remain secure. This means that unlocking the opportunities hinges on having great cybersecurity solutions – plus a collaborative effort to navigate the logistical, administrative, ethical and technical hurdles in front of us. (LORCA)

Most security awareness training gets filed away and forgotten. Here's what we think works. People are often described as being the weakest link in cybersecurity defence. But here at ThinkCyber we believe that people can (and should) be turned into one of the strongest. There's certainly enough data supporting the argument that people's lack of cyber awareness is at the heart of many breaches. For example, in 2017 IBM found that two thirds of recorded cyber attacks resulted from accidental or inadvertent user activities, while data from insurance brokers Willis Towers Watson has shown that approximately 90% of all cyber insurance claims are the result of some type of human error or behaviour. (LORCA)

Agencies & Responders

Police, RBS and Scottish Government unite to fight fraud. In a step to stop scammers in their tracks and keep the public's money safe, senior politicians, security specialists and Police Scotland joined Royal Bank CEO Ross McEwan in Edinburgh to present a united front in helping to keep Scotland safe from the growing impact of fraud and cybercrime. Mr McEwan held an event this morning (Wednesday) at Royal Bank of Scotland's flagship branch at St Andrew's Square alongside Finance, Economy and Fair Work Secretary Derek MacKay, the SBRC's Mandy Haeburn-Little and Police Scotland Chief Superintendent John McKenzie to discuss steps that could be taken to stop fraudsters in their tracks. The meeting coincided with the launch of the Royal Bank of Scotland's Little Book of Big Scams, which has been developed with support and input from some of the parties at the meeting. (Police Scotland)

NCA and police arrest 130 suspects for child sexual abuse and exploitation in just one week. More than 130 suspects – including a former police officer and five teachers – were arrested in a crackdown on online child sex offenders – as UK law enforcement today asks the tech industry to increase their help eradicating preventable offending. The suspects were arrested in a joint operation by the National Crime Agency (NCA) and forces in England, Wales, Scotland and Northern Ireland. During the recent week of action, 225 warrants were executed, 164 children safeguarded, and 131 arrests made for offences relating to indecent images of children. Of the arrests, 13 were registered sex offenders and 19 held positions of trust, with a children's entertainer, an ex-police officer and two special constables arrested. (NCA)

Drone technology: security threats and benefits for police focus of INTERPOL forum. The drone whizzed over the heads of the crowd seated in the auditorium of the INTERPOL

Global Complex for Innovation (IGCI) in Singapore, performing aerial manoeuvres displaying its ability to operate in enclosed indoor spaces. A second demonstration showcased drones designed for use in outdoor spaces, highlighting the benefits and also challenges of deploying such technology in public areas. Drone technology was front and centre at the IGCI this week during the Drone Expert Forum, a three-day (28 – 30 August) conference which brought together nearly 100 experts from law enforcement, academia and private industry to demonstrate how drones can at the same time be a threat, particularly for critical infrastructure, a tool and source of evidence for police worldwide. (INTERPOL)

International Bodies

Council of Europe: Cybercrime News. The Associated Chambers of Commerce and Industry (ASSOCHAM) held the 11th Cyber Security today in cooperation with the Council of Europe. ASSOCHAM Secretary General Shri Uday Kumar Varma underlined the need for resilient cooperative partnerships to address challenges in cyberspace. Dr. Gulshan Rai, National Cyber Security Coordinator of the Government of India, pointed at the complex international environment and expressed concerns about claims of extra-territorial jurisdiction with regard to access to data and data protection. The Council of Europe representative, Alexander Seger, encouraged India to consider joining the Budapest Convention as well as the Data Protection Convention 108 and to participate in the further development of these tools as this would help address some of these concerns. (Council of Europe)

Industry & Technology

BAE Systems appoints cyber security forum committee. BAE Systems has appointed ten senior business figures to the steering committee for its new cyber security forum and lobbying group. The Intelligence Network was launched in July to address the lack of collaboration between companies in tackling cyber crime, as criminals begin to develop similar capabilities to hostile nation states. It followed a government announcement in April that criminals were launching more online attacks against British businesses than ever before, and called for more collaboration to thwart this. The new forum will be spearheaded by senior figures from organisations which produce hundreds of billions of dollars of revenue and are being threatened by cyber attacks. (Sky News)

Windows utility used by malware in new information theft campaigns. WMIC-based payloads highlight how attackers are turning to innocuous system processes to compromise Windows machines. Researchers have uncovered a new attack chain which exploits little-known Microsoft Windows utilities and innocuous software to fly under the radar in the quest to steal data. According to Symantec, the new malware campaign is a prime example of what the company calls "living off the land." In other words, attackers are now turning to the resources already available on target machines -- including legitimate tools and processes -- as well as running simple scripts and shellcode in memory and performing fileless attacks. (ZDNet)

Do mining companies need to wake up to the cyber threat? Cybersecurity is paramount for companies in all industries, with global breaches predicted to cost $6tn by 2023, more than double the figure in 2015. But despite the importance of effective cybersecurity for the mining and mineral sectors, the industry has been slow to react, instead taking an “ad hoc” approach, according to a new study by EY. The report, entitled *Does cyber risk only become a priority once you’ve been attacked?*, examines the stance that mining companies take on cybersecurity and asks whether more should be done. (Mining Technologies)

Cybersecurity researchers double SCADA vulnerability finds. Independent cybersecurity researchers found nearly double the number of vulnerabilities in supervisory control and data acquisition (SCADA) systems in the first six months of 2018 as they did in the first half of 2017, according to a new report by Japanese multinational Trend Micro, amid rising concerns about infrastructure security. The 202 holes spotted in such industrial control systems are not necessarily a bad thing – they are being disclosed because vendors are engaging in bug

bounty programmes, which pay out to security researchers who can find flaws in their software or hardware potentially exploitable by a malicious hacker. (World Pipelines)

Cobalt cyber heist group mounts new campaign. Security researchers discover new campaign using two malicious links to double the chances of infection, which is believed to be linked to a notorious cyber crime group. Researchers at security firm Netscout have discovered a financially motivated cyber attack campaign that could be linked to the Cobalt Group, which is believed to be responsible for cyber heists costing millions. Similarities in phishing emails used in the new ongoing campaign targeting financial institutions in Eastern Europe and Russia led researchers to suspect a link to the Cobalt group, which has targeted mainly financial organisations in the past, often by using automatic teller machine (ATM) malware. (Computer Weekly)

Free, easy to use, and available to anyone: The powerful malware hiding in plain sight on the open web. "When the Russian military is using free stuff, you know how good that stuff is." When people hear about a cyber attack or hacking campaign, they may picture a well-oiled machine that's taken time, skills and resources to build. They imagine underground forums on the dark web, where attackers can buy powerful malware and unleash it on their target of choice. But what if having access to the funding and contacts necessary to deliver attacks with the power of state-backed campaigns wasn't required? In some cases, tools which can be used to conduct malicious cyber operations, ranging from espionage to taking down infrastructure, are freely available on the open web. (ZDNet)

Simple but extremely effective: Inside the world's most prolific mobile banking malware. Asacub trojan has quietly been going about its business for years, stealing funds from hundreds of thousands of victims - but it can also be easily avoided. Asacub is one of the world's most successful mobile banking trojans, responsible for stealing funds from hundreds of thousands of users worldwide. But how did this unremarkable piece of malware become so prolific? While Asacub initially started life as a form of spyware in the first half of 2015, by the start of the following year, the malware had shifted to stealing funds and banking information -- and has kept that focus ever since. (ZDNet)

Cyber attackers switching to covert tactics. Cyber criminals are moving away from mass, high-profile attacks to ones that are stealthy and more subtle – as well as attacks targeting systems typically used in critical infrastructure, researchers say. Cyber criminals are moving away from attention-grabbing ransomware attacks to more covert methods intended to steal money and valuable computing resources, a report reveals. Illicit cryptocurrency mining, also known as cryptojacking, is having the biggest impact so far this year, according to the latest mid-year security roundup report from security firm Trend Micro. The report reveals a 96% increase in cryptojacking detections in the first half of the year compared with the whole of 2017, and a 956% increase in detections compared with the first six months of 2017. (Computer Weekly)

Collaboration essential in combatting cyber security threats. The concept of sharing information with your closest rivals can seem alien to many companies, and understandably so. In such a competitive industry many players, both big and small, may be somewhat resistant to an idea that could dull a company's own competitive edge. However, this is exactly the mindset that the Auto-ISAC is trying to iron out. When 14 automakers came together back in 2015 to form this information sharing community, a precedent was set for the industry, one which arguably provides the strongest defence against the new concept of hackable vehicles – and it is one that has flourished since the tactical information sharing process began in 2016, as the Auto-ISAC's Executive Director, Faye Francy, explained to Automotive World. (Automotive World)

RansomWarrior defeated with decryption tool. Security researchers have managed to crack new ransomware purporting to come from India, providing a decryption tool and usage guide for victims. RansomWarrior was discovered by Check Point's Malware Hunter Team in early August. Alongside instructions on how to pay using Bitcoin, a lock screen presents

victims with a list of "bonus tips." These include suggestions for older users to ask a younger relative for help if they are confused about the process, and not to report the incident to police because it will cost valuable time and "they can't help you anyways." (Infosecurity Magazine)

International News

EUROPE

Germany, seeking independence from U.S., pushes cyber security research. Germany announced a new agency on Wednesday to fund research on cyber security and to end its reliance on digital technologies from the United States, China and other countries. Interior Minister Horst Seehofer told reporters that Germany needed new tools to become a top player in cyber security and shore up European security and independence. (Reuters)

Cyber threat against Danish banks 'very high': agency. The cyber threat against Denmark's financial sector is considered to be very high, according to a report by the Centre for Cyber Security (Center for Cybersikkerhed). The centre, which is a department of military security agency FET, assesses cyber threats against Denmark and Danish businesses. "The threat posed to the Danish financial sector by cyber crime is very high," the centre writes in the report. (The Local)

Bank of Spain's website hit by cyber attack. The Bank of Spain's website has been hit since Sunday by a cyber attack which has temporarily disrupted access to the site, a spokesman for the central bank said on Monday. The spokesman said that the attack has not had any effect on the bank's services or its communications with the European Central Bank or other institutions and that there was no risk of a data breach. (Reuters)

Polish parliament enacts national cybersecurity system. The system classifies security incidents and splits national incident response into three separate teams. The Parliament of Poland today passed into law a new act that will fully implement the NIS Directive, the European Union's directive on security of network and information systems. Poland's goal for its new national cybersecurity system is to ensure security for information systems throughout the country. (Dark Reading)

AMERICAS

DARPA seeks transparency in cyber battle. The US Defense Advanced Research Projects Agency (DARPA) is in the final year of a project that aims to root out cyber attacks by improving operators' visibility of their computing systems. Modern computing systems are essentially black boxes that accept inputs and generate outputs, but provide little-to-no visibility of their inner workings, according to DARPA. (Jane's)

Subex partners with Arizona town to boost cybersecurity. The services of analytics solution provider Subex have been acquired by the Town of Florence in Arizona, USA. The partnership between the Arizona town and the Bangalore-based business support firm will see Subex focus its operations on strengthening the security of Florence's public infrastructure as the town aims to become a smart city. Based within the Phoenix metropolitan area, the town is one of the first in the United States to acquire Subex's cybersecurity services. (Information Age)

Won't patch systems? Never run malware scans? Welcome to the US State Department! A branch of the US State Department charged with detecting visa fraud was found to be ignoring basic information security practices. As pointed out by NextGov, a recent audit conducted by the Office of the Inspector General for the State Department found that its Bureau of Consular Affairs Office of Fraud Prevention was neglecting to perform basic tasks on its systems such as checking for updates and running malware scans. (The Register)

President Trump is wrong about the way Chinese hackers target Americans. President Trump again scrambled debate yesterday about foreign cyberthreats with his unfounded claim — refuted by his own FBI — that China hacked Hillary Clinton's emails while she was secretary of state. This is an ongoing pattern for Trump. The president is quick to point the finger at Beijing when it comes to malicious activities in cyberspace, even as he refuses to consistently embrace his intelligence community's findings on Russian election interference in 2016. (Washington Post)

MIDDLE EAST

UAE used Israeli spyware to hack Saudi, Qatari and Lebanese rivals. The United Arab Emirates had asked an Israeli spyware company it had contracted to surveil dissidents to tap the phone calls of the prime minister of Lebanon and other Arab officials, it emerged Friday. The Emirati government reportedly asked the NSO Group how best to hack the phones of various politicians, with the Arab nation's leaders particularly interested in spying on a Saudi prince — though it was not clear whether those officials were actually hacked. (Telegraph)

The rise of the cyber-mercenaries. What happens when private firms have cyberweapons as powerful as those owned by governments? The first text message showed up on Ahmed Mansoor's phone at 9:38 on a sweltering August morning in 2016. "New secrets about torture of Emiratis in state prisons," it read, somewhat cryptically, in Arabic. A hyperlink followed the words. Something about the number and the message, and a similar one he received the next day, seemed off to Mansoor, a well-known human rights activist in the United Arab Emirates. (Foreign Policy)

What went wrong with Israel's cybersecurity agency. More than three years after it was established, former key officials and other sources describe a government body has lost its focus. When Israel's cabinet approved a plan, strongly backed by Prime Minister Benjamin Netanyahu, to form a Nation Cyber Defense Authority in 2015, the idea was first and foremost to help businesses that didn't have the financial and human resources to protect themselves. (Haaretz)

AFRICA

UK to build new cyber centre to tackle sex abuse in Kenya. No current way for US tech companies to report abusive material online. Britain will establish a cyber centre in Nairobi, Kenya, that will work in collaboration with Kenyan authorities to bring British and other paedophiles preying on children in the country to justice, the government announced today. Kenyan officials do not currently receive any reporting from US-based tech companies when they discover materials that contain the sexual abuse of children, as the secure channels for reporting such material are not in place. (CBR Online)

Cybercrime losses surge above Sh20 billion. Overconfidence by users and lack of smart cybersecurity strategies are exposing many Kenyans to cybercrimes, reveals a *NationNewsplex*review of cybersecurity data. Kenya lost Sh21.1 billion to cybercrime in 2017, a 40 per cent increase from Sh15.1 billion in 2015, according to the *2017 Kenya Cybersecurity Report* by Serianu, an information technology services consultancy firm. (Daily Nation)

State must help us fight cybercrime. Cyber criminals are extremely active across the globe - and very successful. In Africa, too, businesses are losing billions to cybercrime. A quick internet search shows that governments in the Southern African Development Community still aren't prioritising cybersecurity. Botswana doesn't name cyber- security as one of its national priorities. Nor does Mozambique. Zambia's 2018 budget doesn't mention it; nor does Namibia's. (Independent)

ASIA

Can India take the pole position in global cyber governance? As the newest global commons, cyberspace is anarchic in nature, with no formal comprehensive governance framework. The interconnectedness of cyberspace, the low cost of launching a cyber attack, and the invisibility of cyber, makes it difficult to pinpoint the perpetrator with certainty. This is currently the great challenge to the global security establishment's traditional notions of deterrence. (Quartz)

Cybercrime surges above $120-mn in Southeast Asia. The rapid growth of Bitcoin-related scams and other cybercrimes has prompted the United Nations to urge member countries, including Thailand, to step up their legal safeguards against potential economic losses. Cybercrime-related losses worldwide top US$600 billion (Bt19.6 trillion), said Julien Garsany, deputy regional representative of the UN Office on Drugs and Crime (UNODC). (Nation Multimedia)

OCEANIA

Seven Australian universities targeted in global hacking campaign. At least seven Australian universities have been attacked by cyber criminals in a global action targeting researchers. The attack was discovered by Secureworks' Counter Threat Unit (CTU), which said is similar to previous cyber operations by Cobalt Dickens — a threat group associated with the Iranian Government. Secureworks, which is part of the Dell Technologies group, first found a URL spoofing a login page for one university. (ARN Net)

The Cyber Weekly for Scotland has been produced by the Napier Meridian research team and is for the attention of the agreed licensees only. We ask you not to forward the document to any other recipient either electronically or in hard copy without contacting us first.

Napier Meridian

Napier Meridian is an independent consultancy specialising in security strategy. Its expert Staff and Associates have been contributing to the Information Assurance agenda since the 1990s.

Napier Meridian sets out to resolve complexity in organisation and process through provision of clear strategic advice on policy, and clarification of the mechanics of the current cybersecurity response. This insight enables Napier Meridian's clients to manoeuvre within the ever-changing cyber-security domain with accuracy and confidence, rather than be driven by anecdote or speculation, or by simple (and inappropriate) extension of legacy information security processes.

To enquire about Napier Meridian's full set of consultancy services in the National Security, Resilience, Cyber and Specialist Law Enforcement fields, please contact us at: enquiries@napiermeridian.com