
## 8 February 2017

## Synopsis

**Scroll to read full summaries with links to news articles.**

The **EU** has moved closer to allowing cross-border portability for online subscriptions across the European Union. The move is seen as the first step towards the **Digital Single Market** by modernising and harmonising EU **copyright** rules.

A report from **UK** Members of Parliament has heavily criticized the UK's approach to **cybersecurity**, citing an "Alphabet soup" worth of agencies for inconsistencies in the UK's defences.

The **Irish** privacy watchdog is planning to refer **Facebook's** data transfer processes to the EU's top court over concerns they are used to aid **US** spying on **EU** citizens. A final judgement by the European Court of Justice is likely to have a dramatic impact on US-EU data and **privacy** partnerships.

In the **United States**, the Government's Accountability Office has published a report in which it raises concerns about the **National Cybersecurity and Communications Integration Center** within the Department of Homeland Security. The **GAO's** major concern is the lack of a consolidated central reporting system for cyber incidents involving critical infrastructure.

The **House of Representatives** have this week passed a bill that would update the **Email Privacy Act** first introduced in 1986. The new act would require law enforcement to gain a warrant before accessing email accounts and files stored on **cloud systems**.

A bipartisan bill is also currently progressing through the Senate which will call for the Pentagon to track the **cyber skills** of National Guard and Armed Forces reserves, in an attempt to better utilise the cyber skills already present in the **US military**.

In **China** further progress has been made on the Government's proposed **cyber restrictions**, following the publication of draft rules by the country's internet regulator.

**Indonesia** have this week agreed to strengthen their **cybersecurity** collaboration with **Australia**. The further commitment to tackle cyber intrusion and online radicalisation resulted from the third ministerial council meeting on **security and law** held between the two countries.

The **Indian** government has announced that 250,000 gram panchayats (local self governing bodies) will be given greater **access** to the **Internet** by the end of 2018. 100,000 will receive access by March this year as part of a role out of a larger optical fibre cable network.

Consultancy firm **Deloitte** have issued a report in which they expect **Nigeria** to suffer even higher levels of **ransomware** and **cyber attacks** in 2017, compared to 2016. Following the report's publication **Remi Afon**, national president at the Cyber Security Experts Association of Nigeria (**CSEAN**) argued that the Government needs to adopt a more realistic **cybersecurity** strategy.

This week **ICANN** has released its draft report reviewing the body's at-large community. The draft report is available for public comment, though no deadline has been announced.

**ENISA** have this week launched their 2016 Threat Landscape report identifying the leading **cyber threats**. The full report is available here.

**IEEE Global Internet Governance Monitor**

**8 February 2017**

## Table of Contents



Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

# Europe

## Internet governance

**08.02.17**

**Euractiv**
**EU agrees landmark deal on cross-border portability for online subscriptions**

European Union institutions moved a step closer yesterday (7 February) to letting consumers access their online subscriptions for services like Netflix or Sky when they travel across the bloc.

The agreement between the European Parliament and Malta, which acts on behalf of all 28 EU states in its role as the bloc's current holder of the rotating presidency, is another step in an EU drive to knock down barriers in the single market of 500 million people.

It is the first step towards modernising copyright rules in the EU, proposed by the Commission under its Digital Single Market strategy (DSM). Malta has also pledged to prioritise digitalisation during its six months at the helm of the EU presidency.

Maltese Minister for the Economy Chris Cardona said "Europeans travelling within the EU will no longer be cut off from online services such as films, sporting broadcasts, music, e-books or games they have paid for back home."

Letting people take their online subscriptions abroad comes after the bloc has already decided to abolish roaming charges for using mobile phones when travelling within the EU, set to come into force on 15 June.

## Cybersecurity

**02.02.17**

**Euractiv**
**EU tools up for cyber war**

The European Commission was hacked back in November and it took until mid-January for the EU to announce that it wants to invest more in cyber defence.

The attack, carried out on 24 November, involved millions of requests being made to access the executive's website, crippling its servers. It happened in the afternoon and meant many officials were unable to keep working.

But the bloc's plans to counter hacking and government-launched hoaxes have already come in for criticism. German MEP Jan Phillip Abrecht (Greens/EFA)

said that there are so far no tangible measures to protect critical infrastructure or to tackle Fake News. Much is still “under discussion”.

Things have moved on further in the member states though, where military and IT analysts have been working for years on how best to protect themselves from the growing threat of cyber attacks.

**02.02.17**

**SC Magazine**
**Kaspersky: DDoS attacks growing stronger with unsecured IoT**

Kaspersky researchers spotted a record setting 292 hour-long (12.2 day) DDoS attack in Q4 2016, significantly beating the previous quarter's maximum attack, which lasted 184 hours (7.7 days) days. And poorly secured internet of things (IoT) may be to blame.

The firm also found that 80 countries had their resources targeted, compared to 67 in the previous quarter, with China absorbing 71 percent of these attacks, according to the Q4 Summary report.

The top the 10 most targeted countries accounted for almost 97 percent of all attacks with China leading the pack accounting for nearly 77 percent of all the attacks, a slight uptick from the previous quarter, followed by the U.S. which accounted for almost 13 percent of the attacks.

Researchers also spotted four main trends: the demise of amplification-type attacks, rising popularity of attacks on applications along with their increase in encryption usage, rising popularity in WordPress Pingback attacks and the use of IOT botnets to carry out DDoS attacks.

**02.02.17**

**SC Magazine**
**Dutch revert to an all-paper ballot, fearing election hack**

Concerns over a possible election hack by a nation-state actor, the Dutch government will turn to pen and paper and not use a computer to tally the ballots in its national election next month.

The Dutch are basing their concern on intelligence reports that indicate Russian or other fringe groups may attempt to influence the March 15 vote, USA Today reported.

Dutch voters already use paper ballots that are hand-counted locally, but normally they are then brought to another office where a computer is used to create the final tally.

“No shadow of a doubt can be allowed to hang over the result," said Dutch Interior Minister Ronald Plasterk, according to *USA Today*, adding the move was prompted by fears over computer software "vulnerabilities."

The Netherlands joins a growing list of democracies, including France and South Korea, that are worried over outside forces meddling in upcoming elections.

**03.02.17**

**Reuters**
**'Alphabet soup' of agencies leave UK exposed to cyber attacks: report**

Britain's government has taken too long to coordinate an "alphabet soup" of agencies tasked with protecting the country from an ever-increasing risk of cyber attack, a parliamentary report said on Friday.

The Public Accounts Committee report said that as of last April there were at least 12 separate organizations in Britain responsible for protecting information, with "several lines of accountability with little coherence between them."

Processes for recording breaches of personal data by government departments are inconsistent and chaotic, the report said, adding that the government is struggling to meet a skills gap in the security profession.

The findings come in the wake of a spate of cyber attacks that have targeted banks, businesses and institutions, including Tesco Bank, Lloyd's Bank, Talk-Talk, and the National Health Service.

"The threat of cyber-crime is ever-growing yet evidence shows Britain ranks below Brazil, South Africa and China in keeping phones and laptops secure," said committee chair Meg Hillier.

**06.02.17**

**MIS-Asia**
**UK defence secretary urges NATO to fend off Russian cyberattacks**

The U.K.'s defense secretary is accusing Russia of using cyber attacks to "disable" democratic processes across the West, and he's demanding that NATO fight back.

"NATO must defend itself as effectively in the cyber sphere as it does in the air, on land, and at sea," Defense Secretary Michael Fallon said. "So adversaries know there is a price to pay if they use cyber weapons."

Fallon made the comments in a Thursday speech about the threat of "Russia's military resurgence."

He pointed to the Kremlin's suspected role in influencing last year's presidential election in the U.S., as part of growing number of alleged cyber attacks that have targeted Western governments.

"Russia is clearly testing NATO and the West," he said. "It is seeking to expand its sphere of influence, destabilize countries, and weaken the Alliance."

The suspected Russian cyber attacks on Western governments appear to be ongoing. On Friday, the Norwegian security service reportedly said that nine personal civil servant email accounts were targeted with spear-phishing email attacks from elite Russian cyberspies.

**07.02.17**

**SC Magazine**
**Polish bank regulator used as watering hole site for Polish banks**

Polish banks have reportedly been infected with malware from a Polish financial regulator. Several unnamed banks were infected by as yet unknown viruses from the Polish Financial Supervision Authority (KNF), which ironically enough oversees the information security of Polish banks.

Several banks had complained of attacks over the week of 30 January, noticing suspicious files and encrypted traffic flowing through their networks and to strange IPs. Further investigation revealed malware on servers and workstations. Further investigation led the banks down to the source which, strangely enough, was their own regulator.

Attackers had apparently started using the website as a watering hole website. Attackers had altered a Javascript file on the website, so that when users visited, an iframe would download a file onto their computers which when executed would load a Remote Access Trojan (RAT). While banks have apparently reassured customers that they have not yet detected any unauthorised transactions, they do not yet know what exactly was stolen as the outgoing traffic was encrypted.

**07.02.17**

**Politico**
**U.S. shares election-hacking intel with Europe**

The U.S. intelligence community is working with governments across Europe to ensure they don't fall victim to the same digital meddling campaign that rattled the American presidential election.

Intelligence agencies have shared with several foreign governments the classified version of their deep-dive report on what they believe was a Russian plot to undermine Hillary Clinton and tilt the election toward Donald Trump, according to a senior intelligence official and intelligence-oriented lawmakers.

Such an exchange is vital, insist key U.S. lawmakers who warn Russia is turning its U.S. playbook — hack political enemies, leak salacious information — against Europe in an attempt to remake the international order to its liking.

Russian President Vladimir Putin is "trying to break the competence in democracies" around the globe, said Sen. Lindsey Graham (R-S.C.), who ran for president as a vocal Moscow critic.

## Cyber Privacy

**07.02.17**

**Reuters**
**Ireland challenges Facebook in threat to cross-border data pact**

Ireland's privacy watchdog has launched a bid to refer Facebook's data transfer mechanism to the European Union's top court in a landmark case that could put the shifting of data across the Atlantic under renewed legal threat.

The move is the latest challenge to the various methods by which large tech firms such as Google and Apple move personal data of EU citizens back to the United States.

The issue of data privacy came to the fore after revelations in 2013 from former U.S. intelligence contractor Edward Snowden of mass U.S. surveillance caused political outrage in Europe and stoked mistrust of large technology companies and an overhaul in the way businesses can move personal data - from human resources information to people's browsing histories - so as to protect Europeans' information against U.S. surveillance.

Ireland's data protection commissioner, who has jurisdiction over Facebook as its European headquarters are in Dublin, wants The Court of Justice of the European Union to determine the validity of Facebook's "model contracts" - common legal arrangements used by thousands of firms to transfer personal data outside the 28-nation bloc.

Irish Data Protection Commissioner Helen Dixon has formed the view that some of the complaints against the model contracts are "well founded," Michael Collins, a lawyer for the commissioner told Ireland's High Court on Tuesday.

## Internet Inclusion

**02.02.17**

**Computer Weekly**
**Facebook vows to upskill 10,000 women in 2017**

Facebook has vowed to upskill more than 10,000 women in 2017 by providing events and online courses.

In partnership with members network Enterprise Nation, Facebook has created free online and offline training resources, designed to give women online digital skills.

Mobile tools will also be provided to assist women in developing and growing their own businesses.

The partnership is part of Facebook's #SheMeansBusiness initiative, launched in 2016, which aims to tackle the gender gap in the UK's small business sector. Research has found that of the UK's 5.4 million small businesses, only a fifth were started by women.

Over 40% of women said practical support such as digital skills training would help them to start a business.

# United States of America

## Internet governance

***No new items of relevance***

## Cybersecurity

**02.02.17**

**SC Magazine**
**Kaspersky: DDoS attacks growing stronger with unsecured IoT**

Kaspersky researchers spotted a record setting 292 hour-long (12.2 day) DDoS attack in Q4 2016, significantly beating the previous quarter's maximum attack, which lasted 184 hours (7.7 days) days. And poorly secured internet of things (IoT) may be to blame.

The firm also found that 80 countries had their resources targeted, compared to 67 in the previous quarter, with China absorbing 71 percent of these attacks, according to the Q4 Summary report.

The top the 10 most targeted countries accounted for almost 97 percent of all attacks with China leading the pack accounting for nearly 77 percent of all the attacks, a slight uptick from the previous quarter, followed by the U.S. which accounted for almost 13 percent of the attacks.

Researchers also spotted four main trends: the demise of amplification-type attacks, rising popularity of attacks on applications along with their increase in encryption usage, rising popularity in WordPress Pingback attacks and the use of IOT botnets to carry out DDoS attacks.

**02.02.17**

**SC Magazine**
**Cisco: Data breaches costing some businesses 20 percent of revenue**

The cybercrime landscape underwent several changes in 2016 with malicious actors taking a more “corporate” approach to their craft, which helped lead to even greater losses by business hit with a cyberattack.

The damage inflicted on organizations victimized by data breaches and other cyberattacks last year included losing customers, revenue and potential business opportunities, according to the "Cisco 2017 Annual Cybersecurity Report." This year's version marks the report's 10th anniversary. These incursions were due to a combination of using new methodology, along with bringing back some old favorites like spam.

The report, which is based on a survey of 3,000 chief security officers and security operations leaders from 13 countries, found that 22 percent of breached

organizations lost at least some customers with 40 percent of that group losing at least 20 percent of their customer base.

Another 29 percent said their firms lost revenues due to a cyberattack – with 38 percent of that group saying losses exceeded 20 percent. Although somewhat harder to define, 23 percent reported losing business opportunities.

The Cisco report also found that cybercriminals are acting with a new level of professionalism that, ironically, mirrors the companies they are attacking.

**06.02.17**

**The Hill**
**GAO raises alarm over key cyber office**

A new government report has found numerous problems with a critical Department of Homeland Security office charged with tracking and identifying cyberattacks on government systems and critical infrastructure.

The report from the Government Accountability Office says the National Cybersecurity and Communications Integration Center faces a number of impediments to safeguarding the nation's cybersecurity.

The center does not have a single, consolidated system that tracks cyber incidents, the report said. Instead, it receives reports of cyber intrusions in a variety of ways, including by phone and email, which makes it more difficult for agents to catalogue them in one place.

The GAO said the center does not have contact information for nearly a quarter of representatives of all owners of critical cyber infrastructure that, if attacked, could have "a catastrophic impact on the nation." This makes it more difficult for the center to get in immediate contact with owners of critical assets when necessary.

**07.02.17**

**The Hill**
**Trump official: Election infrastructure should be protected**

President Trump's secretary of Homeland Security indicated Tuesday that he would keep in place the Obama administration's designation of election infrastructure as "critical."

"I believe we should help all of the states to make sure their systems are protected, so I would argue we should keep that in place," Secretary John Kelly said during testimony before the House Homeland Security Committee in response to questioning from Rep. Cedric Richmond (D-La.).

The Obama administration designated the U.S. election infrastructure as "critical" in January, just two weeks before Trump's inauguration.

The move extended to storage facilities, polling places and centralized vote tabulation locations supporting the election process, as well as information and communications technology such as voter registration databases and voting machines.

The decision resulted in these systems being subject to federal protections.

“Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law,” then-Secretary of Homeland Security Jeh Johnson said at the time.

Many state and local election officials opposed the designation, though Johnson stressed that it did not amount to “a federal takeover.”

**07.02.17**

**Politico**
**U.S. shares election-hacking intel with Europe**

The U.S. intelligence community is working with governments across Europe to ensure they don’t fall victim to the same digital meddling campaign that rattled the American presidential election.

Intelligence agencies have shared with several foreign governments the classified version of their deep-dive report on what they believe was a Russian plot to undermine Hillary Clinton and tilt the election toward Donald Trump, according to a senior intelligence official and intelligence-oriented lawmakers.

Such an exchange is vital, insist key U.S. lawmakers who warn Russia is turning its U.S. playbook — hack political enemies, leak salacious information — against Europe in an attempt to remake the international order to its liking.

Russian President Vladimir Putin is “trying to break the competence in democracies” around the globe, said Sen. Lindsey Graham (R-S.C.), who ran for president as a vocal Moscow critic.

**07.02.17**

**Politico**
**Sources: Cyber order could get Trump's signature this week**

A postponed cybersecurity executive order is expected to finally get President Donald Trump's signature sometime this week, several sources familiar with the discussions told POLITICO.

The order, which is intended to make agency heads more accountable for the digital security at their departments, has undergone repeated delays and revisions since Trump entered the White House.

While multiple people expect the finished directive this week, some cautioned that further holdups are possible.

Several people tracking the order say the administration is still tweaking the order's language, which has already changed considerably from an early draft and now stretches more than 2,200 words. And on Capitol Hill, some lawmakers expressed concerns Tuesday that they haven't had enough input.

The new commander in chief was on track to sign the presidential fiat last week, but the signing ceremony was abruptly canceled at the last minute, with the White House citing a scheduling change. According to reports, the White House axed the signing to focus on the pending lawsuits against Trump's recent order to limit immigration.

## Cyber Privacy

**06.02.17**

**SC Magazine**
**Privacy alert: FBI pressing Google to hand over U.S. customer data stashed on foreign servers**

Google is being pressured to hand over data to the FBI that is has stored on a foreign server, according to a Monday report on ZDNet.

The order on Friday from U.S. Judge Thomas Rueter, in Philadelphia, requests that Google comply with FBI search warrants necessitating the retrieval of customer data stashed on servers overseas.

The FBI desires the emails for its investigations into a domestic fraud court case. The judge claimed that the transfer of email files from servers located abroad to U.S. soil inferred "no meaningful interference" with the suspects' "possessory interest." Rather, the judge said the files are needed so they could be examined by FBI agents locally. The move did not qualify as a seizure, he said.

"Though the retrieval of the electronic data by Google from its multiple data centers abroad has the potential for an invasion of privacy, the actual infringement of privacy occurs at the time of disclosure in the United States," Judge Rueter stated in his statement.

**06.02.17**

**The Hill**
**House passes bill requiring warrants for email searches**

A bill aimed at modernizing the United States's aging law covering law enforcement access to emails and other stored files passed the House Monday night.

The current law, known as the Electronic Communications Privacy Act, allows law enforcement to access any stored files without a warrant if such material is left on a third-party server for more than 180 days. But that law was passed in 1986 — three years before the invention of the internet — when computer

owners did not have the same systems as modern users, such as cloud hosting, webmail and online photo galleries.

The Email Privacy Act, which passed under suspension of the rules Monday, alters the previous rule to universally require warrants for such information. The same bill cleared the House in 2016 on an overwhelming 419-0 vote, but it stalled in the Senate.

## Internet Inclusion

**07.02.17**

**Ars Technica**
**FCC chair stuns consumer advocates with move that could hurt poor people**

It's no surprise that US Federal Communications Commission Chairman Ajit Pai rolled back some of the changes made by former Chair Tom Wheeler. After Donald Trump's election ensured that the FCC would switch to Republican control, Pai warned Wheeler against "midnight regulations" that can "quickly be undone" by new leadership. On Friday last week, Pai undid a few Wheeler-era decisions while saying that actions no longer supported by the commission's majority "should not bind us going forward."

But one decision in particular is galling to advocates for low-income Americans who can't afford broadband Internet service. As we reported, the FCC on Friday told nine companies that they can no longer provide subsidized broadband to customers who qualify for the Lifeline program. This 32-year-old program gives poor people $9.25 a month toward communications services, and it was changed last year to support broadband in addition to phone service.

FCC procedures make it easy to overturn any recent action, and these nine companies gained their Lifeline broadband approvals late in Wheeler's tenure. Pai's FCC says the commission wants to implement new measures to combat fraud and waste in the Lifeline program and that revoking the Lifeline designations will provide additional time to achieve that. But none of the nine providers was accused of fraud, and the FCC already has the power to investigate and punish any provider that defrauds the program. Pai could have let these companies continue selling subsidized broadband to poor people as long as they committed no fraud, but he chose not to.

**07.02.17**

**The Hill**
**Bipartisan bill asks Pentagon to track cyber skills in National Guard, Reserve**

A bipartisan team of senators introduced new legislation Monday requiring the Department of Defense (DOD) to track cybersecurity skills in the National Guard and Reserve.

The DOD Emergency Response Capabilities Database Enhancement Act of 2017 would add a cybersecurity category to an already existing database that tracks the capabilities of National Guard and Reserve forces.

The bill was introduced by Sens. Joni Ernst (R-Iowa), Deb Fischer (R-Neb.) and Kirsten Gillibrand (D-N.Y.) — all of whom serve on the Senate Armed Services Committee — as well as Sen. Chris Coons (D-Del.).

“The reality is that cyber warfare is an emerging and ever-evolving battlefield, and we must use all available tools to protect our nation’s security, including those that already exist in our National Guard units,” said Ernst, who chairs the Emerging Threats and Capabilities Subcommittee.

“Many of our guardsmen work in the cyber and IT field in their civilian careers, and we must present more opportunities to harness their skillset to advance our nation’s cyber initiatives,” she added in a statement.

# Pan-Asia

## Internet governance

**06.02.17**

**Reuters**
**China proposes further tightening of internet oversight**

China is proposing a further tightening of controls over the internet with the possible establishment of a new commission to vet internet services and hardware, Beijing's internet regulator has said.

China adopted a controversial cyber security law in November to counter what Beijing says are growing threats such as hacking and terrorism, but the law triggered concerns among foreign business and rights groups.

Overseas critics of the law say it threatens to shut foreign technology companies out of various sectors, and includes contentious requirements for security reviews and for data to be stored on servers in China.

New draft rules, released by China's internet regulator at the weekend, propose setting up an intra-departmental body to examine and coordinate policies nationwide.

The commission would consider risks to national security and stop Communist Party and government departments from buying online products and services that have not been approved.

## Cybersecurity

**02.02.17**

**SC Magazine**
**Kaspersky: DDoS attacks growing stronger with unsecured IoT**

Kaspersky researchers spotted a record setting 292 hour-long (12.2 day) DDoS attack in Q4 2016, significantly beating the previous quarter's maximum attack, which lasted 184 hours (7.7 days) days. And poorly secured internet of things (IoT) may be to blame.

The firm also found that 80 countries had their resources targeted, compared to 67 in the previous quarter, with China absorbing 71 percent of these attacks, according to the Q4 Summary report.

The top the 10 most targeted countries accounted for almost 97 percent of all attacks with China leading the pack accounting for nearly 77 percent of all the attacks, a slight uptick from the previous quarter, followed by the U.S. which accounted for almost 13 percent of the attacks.

Researchers also spotted four main trends: the demise of amplification-type attacks, rising popularity of attacks on applications along with their increase in encryption usage, rising popularity in WordPress Pingback attacks and the use of IOT botnets to carry out DDoS attacks.

**03.02.17**

**The Jakarta Post**
**Indonesia, Australia strengthen cyber-security ties**

Australia and Indonesia agreed on Thursday to focus on cyber security in their fight against terrorism and transnational crimes after a meeting in Jakarta.

The agreement was reached at the third ministerial council meeting on security and law despite the ongoing suspension of military cooperation between the two countries.

The meeting highlighted an array of issues related to counterterrorism, such as deradicalization, cyber intrusion, as well as tracing and stopping those funding terrorism online.

Coordinating Political, Legal and Security Affairs Minister Wiranto, who led the Indonesian delegation, noted that both countries had openly exchanged views on the development of regional security dynamics and the importance of maintaining stability in the region.

“The meeting today [Thursday] was held in an open, constructive and friendly atmosphere, so we expect that it will result in tighter and stronger cooperation in law and security,” Wiranto said in a press conference at the conclusion of the meeting.

**07.02.17**

**MIS Asia**
**Only 45 percent of APAC enterprises proactively conduct cyber risk assessments**

Majority of organisations (80 percent) in the Asia Pacific (APAC) region are confident that their corporate data has not been compromised, and 50 percent believe it will not be compromised within the next 12 months.

This is according to a survey commissioned by security intelligence company, LogRhythm, titled "Exploring Cyber Security Maturity in Asia: A study of Enterprise Corporate Executives, IT Executives & IT Practitioners' Perceptions towards Cyber Security Readiness in Asia Pacific".

The survey conducted by Frost & Sullivan polled 400 IT decision makers in Australia, Hong Kong, Malaysia, and Singapore to better understand the cyber resilience of organisations in the region and how they can adopt an integrated approach on cybersecurity.

It was found that even though organisations are confident of their cyber resilience, more than half of them (55 percent) do not conduct a risk assessment study or will only do so if there is a breach or a suspected breach.

"It is encouraging to hear that APAC enterprises are confident about their resilience against cyberthreats. However, these enterprises must ensure that their sense of confidence is not misplaced by proactively conducting cyber risk assessment within their organisation," said Bill Taylor-Mountford, Vice President APAC and Japan for LogRhythm, in a press release.

**08.02.17**

**MIS-Asia**
**Cybersecurity chief releases digital forensic tools in Malaysia**

CyberSecurity Malaysia's chief executive officer Dato' Dr. Haji Amirudin Abdul Wahab has made available two digital forensics tools.

During the recent launch, Dr Amirudin said the tools have been made released under the national infosecurity specialist agency's xForensik R&D and commercialisation initiatives.

While showing the products, called 'Kloner' and 'Pendua,' he said they are the agency's first "innovation attempt to provide local ICT industries, law enforcement agencies and tertiary education institutions with affordable digital forensics tools and software.

Dr Amirudin went on to say that these tools are suitable for both operational and educational purposes especially in the light of an increasingly complex threatscape.

He said the first product 'Kloner' has been designed as a light weight portable external storage duplicator equipped with forensic data preservation functions. "It is designed and developed for investigator inclusive first responders at a crime scene."

The second tool, Pendua, is a portable digital document in a USB thumb-drive, which contains forensics duplicator software to copy data evidence from a suspect's computer at a crime scene.

## Cyber Privacy

***No new items of relevance***

## Internet Inclusion

**07.02.17**

**Security Brief Asia**
**Japan cybersecurity skills shortage in a 'state of urgency' before 2020 Olympics**

A new cybersecurity training and simulation center will be coming to Japan to address the country's growing skills shortage, all to prepare for the onslaught of attacks expected at the Japan 2020 Olympic and Paralympic Games.

The new center will be built in Toranomon, Tokyo, by Cyberbit and Ni Cybersecurity, which will embark on a joint effort to provide hands-on training for cybersecurity professionals.

The center will speed up cybersecurity certification and provide upskilling for existing staff, particularly for those in the government and finance industries.

Japan's cybersecurity skills shortage is expected to from 100,000 to almost 200,000 in the next three years, according to the Japanese Ministry of Economy, Trade and Industry.

Further statistics from the Information-technology Promotion Agency (IPA) show that out of the 265 information security personnel, 160,000 do not have the required skills for their jobs.

**08.02.17**

**Economic Times India**
**Internet to be available in all gram panchayats by next year: Govt**

Internet services are expected to be provided to all the 2.5 lakh (250,000) gram panchayats by the end of next year, government told Lok Sabha today, adding that the net connectivity is being strengthened to promote "less cash economy".

One lakh gram panchayats are to be connected by underground Optical Fibre Cable (OFC) by March this year under the first phase of BharatNet project, Minister P P Chaudhary said while replying to questions on behalf of Minister of State for Communications Manoj Sinha who was not present in the House.

Under the second phase of BharatNet project, remaining 1.5 lakh gram panchayats are to be provided connectivity by December 2018, Chaudhary said. This would be done through a mix of underground fibre cables, fibre over power lines, radio and satellite media.

# Rest of the World

**03.02.17**

**The Guardian (Nigeria)**
**NITDA seeks curriculum review for national ict development**

National Information Technology Development Agency (NITDA) has commenced process of engaging the National Universities Commission (NUC), the National Board for Technical Education (NBTE) and other relevant Agencies for a review of the national (educational) curriculum to incorporate courses on information and communication technologies.

The Control Objectives for Information and Related Technology (COBIT 5) National Implementation Committee inaugurated in Abuja recently is believed to be the vehicle to push for the curriculum review.

Members of the committee were drawn from various MDAs comprising of Central Bank of Nigeria (CBN), National University Commission (NUC), National Agency for Food and Drug Administration and Control (NAFDAC), Security and Exchange Commission (SEC), Nigeria Maritime Administration and Safety Agency (NIMASA), Nigeria Communication Commission (NCC), Nigeria Electricity Regulation Commission (NERC), National Environmental Standards and Regulations Enforcement Agency (NESREA).

Nigeria CommunicationsWeek learnt NITDA's interest in the curriculum review is primarily to include courses that will spur knowledge-based economy and local content development (LCD).

**03.02.17**

**The Jakarta Post**
**Indonesia, Australia strengthen cyber-security ties**

Australia and Indonesia agreed on Thursday to focus on cyber security in their fight against terrorism and transnational crimes after a meeting in Jakarta.

The agreement was reached at the third ministerial council meeting on security and law despite the ongoing suspension of military cooperation between the two countries.

The meeting highlighted an array of issues related to counterterrorism, such as deradicalization, cyber intrusion, as well as tracing and stopping those funding terrorism online.

Coordinating Political, Legal and Security Affairs Minister Wiranto, who led the Indonesian delegation, noted that both countries had openly exchanged views on the development of regional security dynamics and the importance of maintaining stability in the region.

"The meeting today [Thursday] was held in an open, constructive and friendly atmosphere, so we expect that it will result in tighter and stronger cooperation in law and security," Wiranto said in a press conference at the conclusion of the meeting.

**04.02.17**

**Washington Post**
**In Israel, teaching kids cyber skills is a national mission**

In some Israeli schools, fourth-graders learn computer programming while gifted 10th-graders take after-school classes in encryption tactics, coding and how to stop malicious hacking. The country even has two new kindergartens that teach computer skills and robotics.

The training programs — something of a boot camp for cyber defense — are part of Israel's quest to become a world leader in cybersecurity and cyber technology by placing its hopes in the country's youth.

To that end, Israel announced this week the establishment of a national center for cyber education, meant to increase the talent pool for military intelligence units and prepare children for eventual careers in defense agencies, the high-tech industry and academia.

"You students need to strengthen us with your curiosity," Prime Minister Benjamin Netanyahu told an Israeli cyber technologies expo, sitting next to high school students in a training program overseen by the defense establishment. "Your years in the security services will be golden years for the security of the nation."

**06.02.17**

**MIS-Asia**
**Australian government calls on white hat hackers**

The Australian Government is urging white hat hackers to enter a 24-hour cyber security competition.

Student teams of four are being invited to enter the fifth Cyber Security Challenge Australia (CySCA), which was last held in 2015.

CySCA is open to full-time Australian university undergraduates and undergraduate-equivalent TAFE students based in Australia.

The best performing team will win a trip to DEFCON 2017 in Las Vegas and the top team of first year students will be taken to RUXCON 2017 in Melbourne.

The competition, which will be held in May, is a "24-hour virtual game that tests cyber penetration and forensic analysis skills", the government said.

**07.02.17**

**SC Magazine**
**Deloitte Nigeria: expect more ransomware and cloud attacks in 2017**

Nigeria will experience evolving ransomware and cloud-based attacks this year as more organisations migrate from their infrastructures and platforms to the cloud, said Tope Aladenusi, head of cyber-risk services at Deloitte Nigeria.

According to Nigeria's 2017 Cybersecurity Outlook by Deloitte, Nigeria will face increased cases of ransomware attacks targeting fast growing SMEs, and more cyber-criminals are likely to shift their focus from individual organisations to cloud service providers.

“This puts a huge burden on organisations as there would be difficulty in monitoring an organisation's perimeter as their security administrators may have limited control over issues from the cloud,” Aladenusi told SC Media UK.

Government is not prepared for constantly changing cyber-crime as it lacks a realistic strategy, said Remi Afon, national president at the Cyber Security Experts Association of Nigeria (CSEAN).

# Global Institutions

**02.02.17**

**ICANN**
**At-Large Draft Report for Public Comment: Announcement**

Provide your public comment [PDF, 1.43 MB] on the Draft Report [PDF, 2.3 MB] issued by ITEMS International (ITEMS) on the Review of the At-Large.

The At-Large is the community of individual internet users who participate in the policy development work of ICANN and provide policy advice to the ICANN Board. Currently, more than 160 groups representing the views of individual Internet users are active throughout the world. At-Large Advisory Committee(ALAC) is responsible for considering and providing advice on the activities of ICANN.

The criteria for the Review was developed in collaboration with the At-Large Review Working Party and focuses on At-Large Community components (ALAC, RALOs and ALSes) to assess the following:

Fulfilment of mission; adherence to Policies and Procedures, and organizational support; accountability and transparency to the public; membership processes and participation; communication; governance and management, effectiveness of execution; evaluation and measurement of outcomes; effectiveness of implementation of prior review recommendations.

**06.02.17**

**ENISA**
**Challenges of security certification in emerging ICT environments**

ENISA issues today its report on the Challenges of security certification in emerging ICT environments. The report is targeted at EU Member States (MS), the Commission, certification bodies and the private sector, and provides a thorough description of the cyber security certification status concerning the most critical equipment in various critical business sectors.

The study contains information on the certification of devices in five business sectors namely, electricity, healthcare, information and communication technology, railway and water transport. It describes the situation in the EU, and discusses the advantages and challenges towards a more harmonised certification practice.

The key finding of the report, is that every sector has its own functional and security challenges, which makes the target of a common certification framework a challenge in itself. Based on desk research and expert validation, an analysis is done to study the existing frameworks and standards, and to identify certification drivers, best practices and candidate products for certification of the

five selected sectors. Finally an aggregated table is provided, which shortly reflects the certification drivers, the market situation and the recommendation for certification for each identified device.

**07.02.17**

**ICANN**
**ICANN Releases Identifier Systems SSR Activities Report**

As part of our continuing commitment to transparency and accountability, ICANN's Identifier Systems Security, Stability and Resiliency (OCTO SSR) department is pleased to publish its activities report for calendar year 2016. You can find the 2016 report here [PDF, 261 KB].

This reports describe the activities that are performed to maintain the security, stability, and resiliency of the Internet's global identifier systems. These activities include collaboration with, global security and operations groups and public safety communities where ICANN staff serves in several roles.

Depending on the engagement or request, our staff:

- offers security or DNS subject matter expertise;
- facilitates cooperative action among ICANN and other communities to maintain Identifier System Security, Stability, and Resiliency;
- conducts research;
- engages with public and private sector actors in capability building related to Identifier Systems SSR;
- supports the daily efforts of security or operations communities to mitigate the misuse or harmful use of the Identifier Systems (in particular, DNS or domain name registration services).

**08.02.17**

**ENISA**
**ENISA Threat Landscape 2016 report: cyber-threats becoming top priority**

This year is characterised by numerous serious cyber-incidents which have dominated the news. Main objectives of malicious activities detected was monetization and political impact.

ETL 2016 is streamlined towards the top cyber-threats, providing information on threat agents and attack vectors including all the remarkable developments, trends and issues. Moreover, it reports about threat agents their motivations, and how their practices, tools and techniques have advanced. Though the defenders have made significant progress in disrupting cyber-threats and in the attribution of incidents, adversaries continue to advance their tactics and techniques.

The emerging challenges originating from cyber-threats and the assessed trends are presented in this report. ENISA's work in the area of threat analysis also includes:

- Threat assessments for two emerging technology areas i) hardware, and ii) ad-hoc and sensor networking for Mobile to Mobile communications (M2M), and an update on the cyber-threat taxonomy.

# Diary Dates

**ENISA evaluation and review**

Open from 18 January to 12 April 2017.

**3rd International Conference on Information Systems Security and Privacy – ICISSP 2017**

**19.02.17-21.02.17**
Porto, Portugal

**European Information Security Summit 2017 (TEISS)**

**21.02.17-22.02.17**
London, UK

**Singapore Cyber Security R&D Conference (SG-CRC 2017)**

**21.02.17-22.02.17**
Singapore

**Emerging issues in building the European data economy**

Foreseen for 1st quarter of 2017

**European Dialogue on Internet Governance**

**06.06.17-07.06.17**
Tallinn, Estonia