IEEE GLOBAL INTERNET POLICY MONITOR

Read summaries of significant recent internet technology policy activities around the world

1 March 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **European Commission** Vice President **Valdis Dombrovskis** has used a recent speech to call for a common approach to **cybersecurity** in the EU's financial sector. A common approach would create cybersecurity consistency within the EU, an issue that has received growing attention in recent weeks.

Following concerns regarding the impact of **President Trump's** executive order on digital privacy for **EU** citizens, the **US Federal Trade Commission** has assured the EU that they will continue to enforce the **Privacy Shield** agreement.

In the **UK**, the Government has produced its **Digital Strategy** that will guide UK policy beyond the upcoming **Brexit** negotiations. The new strategy has placed a greater focus on **skills**, **connectivity** and **cybersecurity** and emphasises greater government cooperation with industry.

In the **United States** a number of State Governors have raised the issue of **cybersecurity** at the annual **National Governors Association** winter meeting. At a side panel of the meeting a bipartisan alliance of Governors heard evidence from representatives of **Google** and **Deloitte**, as well as a former member of the Justice Department's national security division.

Elsewhere a federal judge in Chicago has ruled that the Government has no legal right to force **Apple** device owners to provide **fingerprints** in order to provide **access** to their devices.

The **FCC** has begun to overturn **net neutrality** regulations implemented during the Obama administration, with the suspension of a **transparency** rule for internet service providers. The rule will be suspended for five years, meaning that it could potentially be recalled if a Democrat succeeds in the 2020 Presidential election.

A **cyberattack** on **Singapore's** Ministry of Defence has led to the leaking of the personal information of 850 service members and department staff. The data was stored on a **I-net** system that allowed users to access the internet without having to use the country's defence computer network.

In **India Hewlett Packard** and **Tata Communications** have announced a joint venture to build an **IoT** network across India. Around 400 million people are expected to benefit from the system which will utilise connections already available in smart buildings, education campuses and healthcare services.

Russia has publicly highlighted its cyber strength in an address by Defence Minister **Sergey Shoygu** to the Russian Duma. In the speech Mr Shoygu has revealed the widely held assumption that cyber had become a central part of Russia’s military.

In **Africa** this week **Zambia** and **Nigeria** have connected to new national data centres that will provide **connectivity** with internet exchanges across Africa and **Europe**.

ICANN have announced that **León Felipe Sánchez Ambía** will become the new Board Director following an election by the At-Large Community.

Elsewhere **ENISA** has published a report on the security incident reporting of Trusted Service Providers within the **European Union**. ENISA has also developed a tool alongside the report to improve the ease with which national supervisory bodies can share security incident reports with the EU Commission and ENISA.

IEEE Global Internet Policy Monitor

1 March 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

No new items of relevance

Cybersecurity

27.02.17

SC Magazine

Cooperative development speeds Nato cyber-intelligence-sharing

NATO has agreed with its partner countries to share research and development advances in cybersecurity tools. Included in the project will be the Cyber Information and Incident Coordination System (CIICS) which is currently being trialed by Finland and Ireland following the successful adoption of the tool by Canada, Romania and the Netherlands.

"NATO and partner countries are sharing R&D in the development of cyber-security tools to achieve economies of scale, including the CIICS (Cyber Information and Incident Coordination System) which has just been deployed in the Alliance's 24/7 cyber operations centre.

CIICS was developed by NATO Communications and Information Agency (NCI Agency), NATO's IT and cyber arm, as part of the Multi National Defence Capability Development (MN CD2) project to share intelligence, detect and thwart cyber-threats at a faster pace and across multiple countries, with Finland set to join the coalition within weeks."

28.02.17

Reuters

EU needs common approach on testing banks' cyber-risks - Dombrovskis

The European Commission Vice President Valdis Dombrovskis has used a recent speech to call for a common approach to cybersecurity in the EU's financial sector. A common approach would create cybersecurity consistency within the EU, an issue that has received growing attention in recent weeks.

"European Union countries should test bank defences against cyber-attacks using a common set of requirements, a senior EU official said on Tuesday, as the bloc plans measures to boost the retail market for financial products.

Cyber attacks against banks have increased in numbers and sophistication in recent years, raising questions on lenders' capacity to protect their customers.

Seeking to reassure savers and strengthen financial stability, several EU countries are conducting tests on banks' security systems, but EU authorities warned national initiatives may be less effective and more costly than a common EU approach."

01.03.17

SC Magazine

German researchers find flaws in nine major password managers

A team of security researchers has found that nine popular Android based password management applications contain security vulnerabilities. The team found that My Passwords, Informaticore Password Manager, LastPass, Keeper, F-Secure KEY, Dashlane, Hide Pictures Keep Safe Vault, Avast Passwords, and 1Password were all affected, though six of these have now been corrected.

"A group of security researchers called TeamSIK has published a security assessment of nine popular password management applications on Android devices and found them all to contain security vulnerabilities.

The group, who belong to the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt, Germany, said: "The overall results were extremely worrying and revealed that password manager applications, despite their claims, do not provide enough protection mechanisms for the stored passwords and credentials."

Privacy

22.02.17

SC Magazine

Privacy Shield enforcement not affected by Trump EO, FTC acting chair says

Maureen Ohlhausen, the acting Chair of the Federal Trade Commission has assured journalists that the US remains an active partner in the EU-US Privacy Shield. The comments were made following concerns by EU officials that an Executive Order signed by President Trump would remove privacy protections for EU data in the US, a central component of the Privacy Shield.

"The Federal Trade Commission's enforcement of the Privacy Shield should not be impeded by an executive order signed by Donald Trump in January, shortly after he took office, according to Acting FTC Chairwoman Maureen Ohlhausen.

"We will continue to enforce the Privacy Shield protections, and we hope we will move ahead as planned," Ohlhausen said to a group of reporters attending a U.S. Chamber of Commerce event, Morning Consult reported. "In my opinion, nothing has changed."

27.02.17

SC Magazine

The Investigatory Powers Act on hold for now due to EU Court ruling

The UK government has confirmed that it has yet to start using powers for mass information collection provided by the Investigatory Powers Act, following the December ruling by the European Court of Justice that the powers were unlawful. The Government has also been forced to delay a consultation for a communications data code of practice as a result of the ruling.

"Due to a ruling by the European Court of Justice last December, the government is yet to slurp up data under power given to it in the Investigatory Powers Act.

The controversial Act is seen by some to be heralding in a new era of government surveillance of all UK citizens, and has had much opposition while going through both houses of parliament.

December's ruling declared that the Act is unlawful, due to being "general and indiscriminate". Three months later, and the UK government has confirmed that the ruling has meant it has yet to start using its new powers to collect information in bulk."

28.02.17

SC Magazine

French and German MPs ask for encryption backdoors, industry says 'no'

European technology firms have rejected calls by French and German Ministers for backdoors to secure encryption to be incorporated into new and existing technology. The firms were responding to a letter sent by the ministers to security experts in the European Commission as part of a lobbying campaign to increase security service access to encrypted communications.

"Technology firms have responded to a letter written by ministers in the French and German governments – which calls for legislation to mandate secure encryption with backdoors – saying it is impossible.

The ministers who wrote the letter believe that encryption backdoors are essential for counter-terrorism.

The letter, sent by Thomas de Maizière and Bruno Le Roux, respectively the German and French ministers of the interior, was sent to security experts in the European Commission such as Brit Julian King."

Internet Inclusion

01.03.17

Computing

Digital Strategy: Skills, security and connectivity at heart of government's digital push

In the UK, the Government has produced its Digital Strategy that will guide UK policy beyond the upcoming Brexit negotiations. The new strategy has placed a greater focus on skills, connectivity and cybersecurity and emphasises greater government cooperation with industry.

"The government has unveiled its Digital Strategy with skills, connectivity and cyber security at the heart of its plans to ensure the UK can embrace the benefits of digital transformation.

The plan was released by the Department for Culture, Media and Sport (DCMS) and presented by culture secretary Karen Bradley in a speech at the offices of startup hub Entrepreneur First.

"Digital technology is revolutionising all aspects of our lives, whether healthcare, transport, manufacturing, entertainment, or our connections with family and friends," she said."

United States of America

Internet governance

No new items of relevance

Cybersecurity

25.02.17

The Hill

Governors put spotlight on cybersecurity

A number of State Governors have raised the issue of cybersecurity at the annual National Governors Association winter meeting. At a side panel of the meeting a bipartisan alliance of Governors heard evidence from representatives of Google and Deloitte, as well as a former member of the Justice Department's national security division.

"Governors from states across the country put the spotlight on cybersecurity at an annual gathering in Washington on Saturday.

Virginia Gov. Terry McAuliffe (D) hosted a session at the National Governors Association winter meeting to discuss the "serious cybersecurity issues" facing the nation and how states need to improve their defenses against cyber threats.

"Cybersecurity is critical to each and every governor," said McAuliffe, who noted that Virginia was targeted by 86 million cyberattacks last year. "We have a wealth of information that every single day people are trying to get in and get our information through cyber threats and cyber criminals."

25.02.17

The Hill

NSA head Rogers pushes to loosen reins on cyberweapons

Admiral Michael Rogers, head of the NSA and Cyber Command has pushed for a greater role for private sector firms in the development of offensive cyberweapons. The Admiral's argument is that the US will be unable to sustain longterm development without the use of the private sector, much in the way conventional weapons are developed.

"Adm. Michael Rogers — both head of the National Security Agency (NSA) and Cyber Command — is pushing for widespread changes to the U.S.'s treatment of cyber weaponry, including contracting private sector firms to develop arms.

"In the application of kinetic functionality — weapons — we go to the private sector and say, 'Build this thing we call a [joint directed-attack munition], a [Tomahawk land-attack munition].' Fill in the blank," he said at a conference in San Diego, as quoted by the Department of Defense."

27.02.17

SC Magazine

Cooperative development speeds Nato cyber-intelligence-sharing

NATO has agreed with its partner countries to share research and development advances in cybersecurity tools. Included in the project will be the Cyber Information and Incident Coordination System (CIICS) which is currently being trialed by Finland and Ireland following the successful adoption of the tool by Canada, Romania and the Netherlands.

"NATO and partner countries are sharing R&D in the development of cyber-security tools to achieve economies of scale, including the CIICS (Cyber Information and Incident Coordination System) which has just been deployed in the Alliance's 24/7 cyber operations centre.

CIICS was developed by NATO Communications and Information Agency (NCI Agency), NATO's IT and cyber arm, as part of the Multi National Defence Capability Development (MN CD2) project to share intelligence, detect and thwart cyber-threats at a faster pace and across multiple countries, with Finland set to join the coalition within weeks."

Privacy

22.02.17

SC Magazine

Privacy Shield enforcement not affected by Trump EO, FTC acting chair says

Maureen Ohlhausen, the acting Chair of the Federal Trade Commission has assured journalists that the US remains an active partner in the EU-US Privacy Shield. The comments were made following concerns by EU officials that an Executive Order signed by President Trump would remove privacy protections for EU data in the US, a central component of the Privacy Shield.

"The Federal Trade Commission's enforcement of the Privacy Shield should not be impeded by an executive order signed by Donald Trump in January, shortly after he took office, according to Acting FTC Chairwoman Maureen Ohlhausen.

"We will continue to enforce the Privacy Shield protections, and we hope we will move ahead as planned," Ohlhausen said to a group of reporters attending a U.S. Chamber of Commerce event, Morning Consult reported. "In my opinion, nothing has changed."

23.02.17

SC Magazine

Fingerprints to unlock iPhone? Judge says no.

Law enforcement have been told that they have no legal right to force suspects to open their Apple devices with their fingerprints, after a federal judge in Chicago ruled that it constituted an unreasonable search.

"A federal judge in Chicago issued an opinion on February 16 that would deny the government's attempt to force Apple device owners from providing a fingerprint to unlock their device.

The 14-page opinion and order, part of a child porn case, adds to the growing debate around individual rights to privacy and the needs of law enforcement to get past encryption technologies to further their investigations.

It boils down to Fourth Amendment protections against unreasonable search and seizure as well as the Fifth Amendment right to avoid self-incrimination."

Internet Inclusion

24.02.17

Info World

FCC rolls back net neutrality ISP transparency rules

The Federal Communications Commission has suspended transparency rules for Internet Service Providers for a period of five years, for services with less than 250,000 subscribers. The five year freeze may become more permanent if the now Republican led FCC is successful in overturning net neutrality regulations adopted during the Obama administration.

"The U.S. Federal Communications Commission has voted to roll back some net neutrality regulations that require broadband providers to inform customers about their network management practices.

The Republican-controlled FCC on Thursday suspended the net neutrality transparency requirements for broadband providers with fewer than 250,000 subscribers. Critics called the decision anticonsumer.

The transparency rule, waived for five years in a [2-1 party-line vote]() Thursday, requires broadband providers to explain to customers their pricing models and fees as well as their network management practices and the impact on broadband service."

28.02.17

Reuters

[New FCC chair vows 'light-touch' approach to regulation]()

Ajit Pai, the new chairman of the Federal Communications Commission has promised to use a less restrictive regulatory approach during his tenure. Speaking at the Mobile World Congress in Barcelona Mr Pai highlighted his opposition to using public utility regulations to limit digital technologies.

"The new Republican head of the U.S. Federal Communications Commission promised "light-touch" regulation of areas such as the internet, a dramatic shift away from the Obama administration's approach to telecommunications oversight.

Ajit Pai, whom President Donald Trump named in January to chair the FCC, said at the Mobile World Congress in Barcelona that the agency made a "mistake" in 2015 when it adopted landmark "net neutrality rules" reclassifying internet service like a public utility."

Pan-Asia

Internet governance

01.03.17

Channel News Asia

China warns against cyber "battlefield" in internet strategy

The Chinese Government have warned against the militarisation of the internet in a new call for greater cooperation in internet governance that respects national cyber sovereignty. The Foreign Ministry and Cyberspace Administration also expressed the importance of using cyberdefences to modernise the Chinese military as part of the cooperation strategy document.

"The strengthening of cyber capabilities is an important part of China's military modernisation, the government said on Wednesday, warning that the internet should not become "a new battlefield".

China, home to the largest number of internet users, has long called for greater cooperation among nations in developing and governing the internet, while reiterating the need to respect "cyber sovereignty".

But Beijing, which operates the world's most sophisticated online censorship mechanism known elsewhere as the "Great Firewall", has also signalled that it wants to rectify "imbalances" in the way standards across cyberspace are set."

Cybersecurity

27.02.17

SC Magazine

Government-backed malware campaign targets South Korean public sector

A cyber attack on the South Korean public sector has been blamed on a foreign government. The attack was based in a malicious Hangul Word Processor document, which experts have noted have a higher chance of bypassing security scans due to their low sophistication.

"Attacks on these individuals could be an attempt to gain a foothold into assets that can be deemed extremely valuable.

Cisco Talos discovered the campaign was active between November 2016 and January 2017, targeting a limited number of people.

The malicious document in question, which is written in Korean, is a Hangul Word Processor (HWP), a popular alternative to Microsoft Office in South Korea.

Cisco Talos reported that "many security devices are not equipped to process HWP files. This can allow an attacker a vector with a much lower risk of detection by any security scanning devices."

28.02.17

SC Magazine

Singapore MoD computer breached, 850 lose PII

The Ministry of Defence in Singapore has been effected by a security breach to its I-net computer system, which allows military and civilian officials to access the internet securely. Whilst the personal information of 850 staff were released the attack is not believed to have affected the country's defence computer system.

"The personally identifiable information of 850 Singapore military service members and Ministry of Defense staffers was compromised in what is being called a targeted and carefully planned attack on the MOD's I-net computer system.

The I-net breach was discovered earlier this month, but ministry officials reported no sensitive information was leaked, according to the Singapore Straits Times. The I-net system is used by troops and civilian MoD workers to access the internet for personal reasons and is not connected to the countries defense computer network."

01.03.17

Phnom Penh Post

Cyber security training now underway in Japan

Japan's International Cooperation Agency has begun training for six ASEAN countries in a bid to improve their cybersecurity. Cambodia, Laos, Indonesia, Myanmar, Vietnam and the Phillipines will receive training for three years with representatives from each government receiving training on how to enhance security.

"Japan has launched a new effort to boost the cyber defence capabilities of six ASEAN members, including Cambodia, though some experts wondered if the arrangement was a good fit for either party.

Officials from Cambodia's Ministry of Posts and Telecommunications are participating in a training session from February 20 to March 3, representatives of the Japan International Cooperation Agency (JICA) confirmed."

Privacy

No new items of relevance

Internet Inclusion

28.02.17

Network Asia

IoT network in S'pore achieves 95% outdoor coverage

UnaBiz, ENGIE, and Sigfox have announced that a significant milestone in the deployment of the first Internet of Things network in Singapore. The network now has 95% coverage across the island and is the first such IoT network of its kind in Southeast Asia.

"At UnaBiz's inaugural UnaDay, ENGIE, Sigfox and UnaBiz jointly announced that they have reached an important milestone in the deployment of the first Internet of Things (IoT) network in Singapore, achieving 95 percent outdoor coverage across the island. This network, which is the first of its kind in Southeast Asia, will help improve energy efficiency, facility management and customer-centred solutions for businesses in the region with the capacity to support over 100 million connected devices while maintaining high network reliability and security."

28.02.17

Network Asia

Demand for Malaysian IT and tech talent to rise: report

A new report by the Monster Employment Index has found a 36% year on year growth in demand for Malaysian online talent. This growth has also been found in other ASEAN countries with the Phillipines also reporting a 19% growth in demand.

"Malaysia's upbeat economic outlook despite significant headwinds has led to an uptick in online hiring sentiment, especially for roles across the IT, Telecom/ ISP and BPO/ ITES sectors. It reported a strong 36% growth year-on-year, as reported by the Monster Employment Index (MEI).

The MEI is a monthly gauge of online job hiring activity by Monster.com, which records the industries and occupations that show the highest and lowest growth in e-recruitment, including statistics from the IT/Telecom sector."

01.03.17

MIS Asia

HPE and Tata Communications will jointly build IoT network in India

A new partnership has been announced by Hewlett Packard Enterprise and Tata Communications at the Mobile World Congress. The two companies will collaborate to build an Internet of Things network in India. The project will develop existing connections and is expected to benefit over 400 million people.

"Hewlett Packard Enterprise (HPE) and Tata Communications are working together to roll out a low power wide area (LoRa)-based network in India.

HPE announced the collaboration on Monday (27 February 2017) at the Mobile World Congress in Barcelona, Spain.

The joint project will connect devices, applications, and other Internet of Things (IoT) solutions over the LoRa network in smart buildings, campus, utilities, fleet management, security, and healthcare services in nearly 2,000 communities in India. More than 400 million people are expected to benefit from the project."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

24.02.17

SC Magazine

No secret anymore: Russia touts cyber force

Sergey Shoygu the Russian Minister of Defence has publicly admitted that the Russian military has developed a permanent force developed for cyber attacks. The revelation is the first time that a member of the Russian Government has admitted to the existence of cyberforces, believed by intelligence agencies in the US to have played a significant role in November's Presidential election.

"Russia has a cyber army. The announcement was made by Sergey Shoygu, minister of defense, while addressing the Duma, the nation's lower house of parliament, and reported in Tass, the Russian state news agency.

"The information operations forces have been established, that are expected to be a far more effective tool than all we used before for counter-propaganda purposes," Shoigu said. "Propaganda should be smart, competent and effective."

26.02.17

Digital Trends

Microsoft looks to fight cybercrime in Latin America with new facility in Mexico

Microsoft has launched a new cybersecurity engagement centre in Mexico designed to counteract cybercrime in Latin America. The centre will also look to support digital transformation efforts in the region.

"Microsoft is taking the fight against cybercrime global with a new cybersecurity center in Mexico.

Not all heroes wear capes — in fact, some of them wear glasses and sit on the IT team at Microsoft. On Friday, the technology company announced the launch *of a new Cybersecurity Engagement Center in Mexico as part of its global initiative to bolster IT security."*

27.02.17

SC Magazine

Cooperative development speeds Nato cyber-intelligence-sharing

NATO has agreed with its partner countries to share research and development advances in cybersecurity tools. Included in the project will be the Cyber Information and Incident Coordination System (CIICS) which is currently being trialed by Finland and Ireland following the successful adoption of the tool by Canada, Romania and the Netherlands.

"NATO and partner countries are sharing R&D in the development of cyber-security tools to achieve economies of scale, including the CIICS (Cyber Information and Incident Coordination System) which has just been deployed in the Alliance's 24/7 cyber operations centre.

CIICS was developed by NATO Communications and Information Agency (NCI Agency), NATO's IT and cyber arm, as part of the Multi National Defence Capability Development (MN CD2) project to share intelligence, detect and thwart cyber-threats at a faster pace and across multiple countries, with Finland set to join the coalition within weeks."

Privacy

24.02.17

The Sydney Morning Herald

Data breach notification laws sharpen security focus

Following the passing of mandatory notification laws by the federal parliament, the Australian technology sector has begun to focus on the issue in greater detail. The law has also seen increased adoption of mature security responses to ensure greater cybersecurity in both the public and private sector.

"Australians now have some comfort they will at least be notified if their online personal data is compromised and many companies are expected to ramp up cyber security after federal parliament passed mandatory breach reporting laws.

The legislation requires government agencies and businesses covered by the Privacy Act to notify any individuals affected by a data breach that's likely to result in serious harm."

Internet Inclusion

24.02.17

IT Web Africa

Zambia smartens up with new national data centre

The first national data centre has been unveiled in Zambia by Huawei Technology Zambia. Plans are now underway to implement the next phase of the project, with the establishment of two further national data centres. Chinese firm Huawei will also develop a national broadband system for public service delivery.

“Huawei Technology Zambia has finally unveiled Zambia's first national data centre constructed as part of the Smart Zambia project.

The data centre, under the Smart Zambia phase 1 project, is being implemented via the Zambia Information and Communication Technology Authority (ZICTA) and funded by the Chinese government through a concessional loan.

Following the completion of the data centre, the government says plans are already underway to implement phase 2 and 3 of the Smart Zambia project that will see the establishment of two additional national data centres and a computer assembly plant in Lusaka.”

26.02.17

Data Economy

Nigeria’s Internet Exchange Signs Into Regional Data Centre In Services Boost

Nigeria’s internet exchange has signed into the MDXI data centre in Lekki for the first time. The data centre will further connect Nigeria to internet exchanges in European and across West Africa.

“The Nigerian Internet Exchange (IXPN) has singed into the MainData Nigeria (MDXi) Lekki data centre as the amount of traffic passing to the IX grows.

MDXi’s data centre connects to a number of IP transit and Content Delivery networks in West Africa.”

Global Institutions

23.02.17

ITU

ITU agrees on key 5G performance requirements for IMT-2020

At a working group meeting in Geneva earlier this week the ITU and its membership agreed on the fundamental performance requirements of 5G. These requirements will form part of the bodies IMT-2020 report which will seek to outline the future for broadband and IoT technologies.

"Membership of ITU including key industry players, industry forums, national and regional standards development organizations, regulators, network operators, equipment manufacturers as well as academia and research institutions together with Member States, gathered in Geneva today, as the working group responsible for IMT systems, and completed a cycle of studies on the key performance requirements of 5G technologies for IMT-2020.

Draft New Report ITU-R M.[IMT-2020.TECH PERF REQ] is expected to be finally approved by ITU-R Study Group 5 at its next meeting in November 2017."

24.02.17

ITU

Paraguay hosts regional preparatory meeting for ITU's World Telecommunication Development Conference 2017

ITU has conducted a regional prepatory meeting in Paraguay ahead of the body's 2017 World Telecommunication Development Conference. The Minister of Finance for Paraguay, Mr Santiago Peña highlighted the importance of using technology to connect citizens across the country.

"The Regional Preparatory Meeting (RPM) for the Americas was held from 22 to 24 February in Asunción, Paraguay. Participants at the meeting assessed the ongoing implementation of the Dubai Action Plan adopted at ITU's last World Telecommunication Development Conference (WTDC-14) and identified priority areas for information and communication technology (ICT) development strategies in the Americas."

27.02.17

SC Magazine

[Cooperative development speeds Nato cyber-intelligence-sharing]

NATO has agreed with its partner countries to share research and development advances in cybersecurity tools. Included in the project will be the Cyber Information and Incident Coordination System (CIICS) which is currently being trialed by Finland and Ireland following the successful adoption of the tool by Canada, Romania and the Netherlands.

"NATO and partner countries are sharing R&D in the development of cyber-security tools to achieve economies of scale, including the CIICS (Cyber Information and Incident Coordination System) which has just been deployed in the Alliance's 24/7 cyber operations centre.

CIICS was developed by NATO Communications and Information Agency (NCI Agency), NATO's IT and cyber arm, as part of the Multi National Defence Capability Development (MN CD2) project to share intelligence, detect and thwart cyber-threats at a faster pace and across multiple countries, with Finland set to join the coalition within weeks."

27.02.17

ICANN

León Felipe Sánchez Ambía Selected by At-Large Community as Next ICANNBoard Director

ICANN have announced the results of their most recent election to the ICANN board. León Felipe Sánchez Ambía has been chosen by the At-Large community to succeed Rinalia Abdul Rahim as a board director.

"On behalf of Tijani Ben Jemaa, Chair of the Board Member Selection Process Committee (BMSPC), we are announcing the final result of the ICANN Board Director seat (#15) election, which was selected by the At-Large Community.

The At-Large Community's ICANN Board Director selection process was a six-month effort, and officially ended on 27 February 2017. León Felipe Sánchez Ambía has been selected by At-Large as the successor of Rinalia Abdul Rahim, and will begin his three-year term as an ICANN Board Director at the end of ICANN60 (3 November 2017)."

28.02.17

APEC

APEC Mobilizes to Avert Employment Crisis as Big Data Booms

APEC has announced a new initiative with the private sector to resolve the growing gap between digital skills and requirements in the region.

*"Labor officials from **APEC member economies** are partnering with the private sector to fight the rapidly widening gap between skill levels and employer demand in the Asia-Pacific, prompted by the threat it poses to employment and growth in the digital era. Focus is on mitigating the shortage of personnel equipped to analyze customer, product and other big data vital to business decision-making.*

Officials announced the launch of a collaborative data skills enhancement initiative during a slate of policy development meetings in Nha Trang to strengthen labor and social protection in the region. It includes the commissioning of an impact assessment and formation of a corporate backed panel to guide academic institutions and governments on relevant, employer compatible curricula design—affecting industries ranging from auto production to e-commerce to healthcare."

28.02.17

ENISA

Guidelines on Incident Notification for Digital Service Providers

ENISA has published a new set of guidelines for digital service providers to support them in conforming to the new EU wide directive that mandates incident notification. The full report is available here

"The EU's first DSP mandatory incident notification requirements as part of the first EU-wide set of rules on cyber-security, are a major step towards achieving a common level of cyber-security across the Union. ENISA's comprehensive technical guideline supports stakeholders in addressing mandatory incident notification for Digital Service Providers (DSPs) in the context of the NIS Directive."

01.03.17

ICANN

Inaugural ICANN DNS Symposium to be Held in Madrid

ICANN have announced that its first symposium on Domain Name Systems will be held in Madrid, Spain. The event will take place on Saturday 13 May 2017.

“The Internet Corporation for Assigned Names and Numbers (ICANN) today announced a new event that will be held in Madrid, Spain, on Saturday, 13 May 2017. The ICANN DNS Symposium is intended to provide a technical forum for individuals to discuss topics related to all aspects of the Domain Name System (DNS).

Attendees should have a foundational understanding of the DNS. Topics for the initial event will focus on DNS-related activities within ICANN, including research, security, root server operations, IANA functions and more. To learn more about the symposium or to register for the event, please visit https://www.icann.org/ids.”

01.03.17

ENISA

ENISA and national supervisory bodies agree reporting scheme on security incidents for European TSPs

ENISA has published a framework for security incident reporting for Trusted Service Providers, in collaboration with the European Commission and national supervisory bodies. The full report is available here.

“ENISA publishes its security incident reporting framework for TSPs (Trusted Service Providers) in the context of the new European eIDAS regulation.

ENISA supports supervisory bodies with the implementation of national incident notification schemes. The objective of this proposal is to support efficient and harmonized incident notification schemes across the European Union.”

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

World Cyber Security Congress 2017 – 07.03.17-08.03.17

London, UK

Australian Cyber Security Centre (ACSC) Conference 2017 – 14.03.17-16.03.17

Canberra, Australia

Cyber Intelligence Asia 2017 – 14.03.17-16.03.17

Kuala Lumpur, Malaysia

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

16th European Conference on Cyber Warfare and Security ECCWS – 29.06.17-30.06.17

Dublin, Ireland