IEEE

GLOBAL INTERNET POLICY MONITOR

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

22 February 2017

Synopsis

Scroll to read full summaries with links to news articles.

In the **EU** this week, **data privacy** watchdogs have been seeking assurances from the **American** Government that the data privacy of European citizens will continue to be respected. The concerns were raised following action by the White House to curb illegal immigration that included the exclusion of non-Americans from the **Privacy Act.**

Earlier this week, members of the **London Internet Exchange** members voted against a proposal that would have allowed the **UK** government to monitor the communications of users without informing the Exchange and its members.

NATO and **Finland** have agreed to strengthen their cooperation on cybersecurity issues, following the resurgence of **Russia** and growing digital threats.

In the **United States** this week Defence Secretary **James Mattis** has called for a review of existing **cyber policy** in the military based on the recommendations of the **National Defence Authorization Act** signed during the Obama administration.

Google have announced that their **Internet access** plans have been reassessed, with a smaller plan now in motion. Initially the programme was designed to spread Wi-Fi emitting balloons across the world to aid internet access, however following the recent announcement Google will now look to cover only those regions in greatest need as its parent **Alphabet Inc.** looks to cut costs.

The **UK** and **China** have agreed to further cooperation on **cybersecurity** issues as part of wider security discussions between senior officials.

The **Japanese** company **NEC Corporation** has been given permission by the Japanese Government to provide **cybersecurity** training to government institutions across the **Association of Southeast Asian Nations.** The training will take place in Japan and will seek to ensure a higher standard in cybersecurity across the region.

Ahead of **cybersecurity** discussions with **Israeli** Prime Minister **Nethanyahu** this week the **Australian** Government has announced a new fund of 1.9 million Australian dollars for **cybersecurity** training in the country's universities.

Elsewhere **ENISA** has published a new report into the security measures needed for **Digital Service Providers (DSPs),** in which it hopes to establish a commons set of **standards** for DSPs.

Finally, **ICANN** have launched a new consultation into the organisations **transparency**, calling upon members to submit their views by 10 April.

IEEE Global Internet Policy Monitor

22 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

20.02.17

EurActiv
Malta’s new draft law raises concerns over internet freedom

Several thousand people took to the streets of Malta on Sunday (19 February) to protest against a new bill that is expected to force online news sites to register with the government.

The protest, organised by Malta’s opposition Nationalist Party (NP), is campaigning against a new proposal, seen as a clampdown on freedom of speech.

The draft bill, proposed last week, seeks to update Malta’s defamation and libel laws, which some say is a way to oblige citizens to register before being able to express views on the Internet.

“This is a restriction on internet freedom and a future nationalist government will repeal it if it gets approved by parliament,” NP leader Simon Busuttil told the rally in Valletta.

The move comes after the Organization for Security and Co-operation in Europe (OSCE) slammed Malta last week for intimidating journalist Daphne Caruana Galizia.

22.02.17

The Register
London Internet Exchange members vote to block UK Snoopers' Charter gagging order

Members of LINX, the London Internet Exchange – the UK's largest net “peering” point - have rejected proposals that would reshape the company’s constitution and could block members from being consulted about government tapping instructions.

The vote, on Tuesday, followed a *Reg* report revealing that members had been given less than two weeks notice of a proposed change which would allow LINX’s chairman to “override” directors’ wishes and prevent members learning about controversial actions, including, according to LINX, “secret orders from the government.”

Directors of the company had urged the 740 members of LINX, mostly Internet providers from overseas, to vote for the plans without any debate or considering alternatives, during a 10-minute “Extraordinary General Meeting” (EGM) held on Tuesday.

The majority of LINX members did not cast votes, *The Reg* has learned. Of those that did vote, 37 per cent rejected the plan and 63 per cent supported it. To comply with British Companies Acts law, 75 per cent of voting members must agree with any “Special Resolution” making major changes. The votes in favour therefore fell significantly short of the level legally required.

Cybersecurity

16.02.17

The Hill
NATO, Finland deepen cooperation on cyber defense

The North Atlantic Treaty Organization (NATO) and Finland are stepping up their cooperation on cyber defense in the face of increased threats in cyberspace and a resurgent Russia.

NATO and Finland on Thursday signed a political framework agreement on cyber defense cooperation that will allow them to better protect and strengthen their networks.

“We look forward to enhancing our situational awareness and exchanging best practices with Finland, including through dedicated points of contact for rapid information exchange on early warning information and lessons learned,” Ambassador Sorin Ducaru, NATO’s assistant secretary general for emerging security challenges, said.

Jukka Juusti, permanent secretary of Finland’s defense ministry, indicated that the country also wants to boost cooperation with the alliance by holding more joint cyber training and exercises. Finland already participates in the alliance’s Cyber Coalition, an annual cyber defense exercise.

17.02.17

SC Magazine
UK and China agree coordination on cyber-security issues

The UK and China have, “agreed to regular coordination on cyber-security related issues in order to prevent cyber-commercial espionage and related transnational criminal activity. I welcomed China's openness to signing-up to the WeProtect global alliance on preventing child sexual exploitation online,” said Sir Mark Lyall Grant, the UK's national security adviser.

He was hosting Wang Yongqing, secretary-general of the Central Commission for Politics and Law, for the second UK-China High Level Security Dialogue.

The dialogue focused on cooperation on cyber-security, counter-terrorism and countering violent extremism, and organised crime.

During the dialogue, the National Security Adviser and Secretary-General Wang agreed various measures aimed at strengthening UK and China security cooperation.

17.02.17

BBC
German parents told to destroy Cayla dolls over hacking fears

An official watchdog in Germany has told parents to destroy a talking doll called Cayla because its smart technology can reveal personal data.

The warning was issued by the Federal Network Agency (Bundesnetzagentur), which oversees telecommunications.

Researchers say hackers can use an unsecure bluetooth device embedded in the toy to listen and talk to the child playing with it.

But the UK Toy Retailers Association said Cayla “offers no special risk”.

In a statement sent to the BBC, the TRA also said, “there is no reason for alarm”.

The Vivid Toy group, which distributes My Friend Cayla, has previously said that examples of hacking were isolated and carried out by specialists. However, it said the company would take the information on board, as it was able to upgrade the app used with the doll.

20.02.17

Public Technology
TechUK calls for G20 focus on digital

The representative body for the tech industry in the UK, TechUK, has released a position paper with a number of global technology bodies and associations, which sets out seven priorities for the governments making up the G20.

It said: “The G20 is a critically important setting for the world’s leading governments to outline approaches to managing 21st century ICT policy challenges, combating protectionism, achieving the UN Sustainable Development Goals, and growing the global economy in ways that benefit all countries and people.”

Among the areas is a call for governments to make sure that any data protection policies promote innovation and international interoperability, while saying that governments must “acknowledge that privacy is a fundamental right”.

The document also calls for governments to make sure that cyber security measures ”avoid prescribed technology standards” and incorporate “meaningful” consultation with the private sector.

This latter point is also picked up separately, with the tech associations saying that governments should be more transparent with industry and other stakeholders, for instance through advanced notice of - and opportunity to comment on - draft laws, regulations and other measures affecting ICT.

Privacy

16.02.17

Reuters
EU privacy watchdogs seek assurances on U.S. data transfer pact

European Union data privacy watchdogs will seek assurances from U.S. authorities that a move by U.S. President Donald Trump to crack down on illegal immigration will not undermine a transatlantic pact protecting the privacy of Europeans' data.

European concerns have been raised by an executive order signed by Trump on Jan. 25 aiming to toughen enforcement of U.S. immigration law.

The order directs U.S. agencies to “exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.”

The exemption of foreigners from the U.S. law governing how federal agencies collect and use information about people has stoked worries across the Atlantic about the new administration's approach to privacy and its impact on cross-border data flows.

21.02.17

EurActiv
EU privacy watchdogs reiterate warning about Windows 10

European Union data protection watchdogs said on Monday they were still concerned about the privacy settings of Microsoft’s Windows 10 operating system despite the US company announcing changes to the installation process.

The watchdogs, a group made up of the EU’s 28 authorities responsible for enforcing data protection law, wrote to Microsoft last year expressing concerns about the default installation settings of Windows 10 and users’ apparent lack of control over the company’s processing of their data.

The group – referred to as the Article 29 Working Party – asked for more explanation of Microsoft's processing of personal data for various purposes, including advertising.

"In light of the above, which are separate to the results of ongoing inquiries at a national level, even considering the proposed changes to Windows 10, the Working Party remains concerned about the level of protection of users' personal data," the group said in a statement which also acknowledged Microsoft's willingness to cooperate.

Internet Inclusion

15.02.17

SC Magazine
UK approaching skills 'cliff edge' as cyber workforce ages - report

The global IT security industry will face a shortfall of 1.8 million workers by 2022, according to a new study, while the UK faces the prospect of its workforce actually shrinking.

The Center for Cyber Safety and Education surveyed 19,000 cyber-security professionals for its eighth bi-annual Global Information Security Workforce Study (GISWS), sponsored by non-profit professionals' association (ISC)².

It found that the perceived shortfall in cyber-security experts had risen 20 percent, up from 1.5 million, the figure it published in its previous survey in 2015.

The UK government's recent Cyber Security Strategy called Britain's cyber-security skills gap a "national vulnerability that must be resolved".

The survey found that two-thirds of firms in the UK don't have enough infosecurity personnel to meet their needs, and it is impacting economic security. Around 47 percent claimed the reason behind this was an absence of qualified candidates.

16.02.17

Bloomberg
Alphabet Scraps Plan to Blanket Globe With Internet Balloons

In 2013, Google ran its first tests for Project Loon, an ambitious effort to circulate broadband-emitting balloons across the globe. On Thursday, the company said that's not necessary anymore.

Executives at the project said they have found ways to run the program with fewer balloons. Rather than building a worldwide network, the team will now launch a small number of balloons into particular regions that need internet access. That will accelerate the project's path toward becoming an actual commercial operation, the Loon team said. The announcement is consistent with moves across Google parent Alphabet Inc. to curb costs at its riskier, expensive projects.

“We can now run an experiment with 10 or 20 or 30 balloons,” said Astro Teller, the head of X, the Alphabet division that houses Project Loon. “The service has a much better chance of ultimately being profitable.”

Teller said the team will be testing with telecommunications providers “in the coming months.”

United States of America

Internet governance

No new items of relevance

Cybersecurity

16.02.17

The Hill
NATO, Finland deepen cooperation on cyber defense

The North Atlantic Treaty Organization (NATO) and Finland are stepping up their cooperation on cyber defense in the face of increased threats in cyberspace and a resurgent Russia.

NATO and Finland on Thursday signed a political framework agreement on cyber defense cooperation that will allow them to better protect and strengthen their networks.

“We look forward to enhancing our situational awareness and exchanging best practices with Finland, including through dedicated points of contact for rapid information exchange on early warning information and lessons learned,” Ambassador Sorin Ducaru, NATO’s assistant secretary general for emerging security challenges, said.

Jukka Juusti, permanent secretary of Finland’s defense ministry, indicated that the country also wants to boost cooperation with the alliance by holding more joint cyber training and exercises. Finland already participates in the alliance’s Cyber Coalition, an annual cyber defense exercise.

19.02.17

The Hill
Ex-House intel chairman: US 'not necessarily winning' the cyber war

Former House Intelligence Committee Chairman Mike Rogers (R-Mich.) raised concerns Sunday about U.S. cybersecurity, warning that the country is “not necessarily winning.”

“We are in a cyber war in this country, and most Americans don't know it. And we are not necessarily winning,” he said in an interview with John Catsimatidis that aired on AM 970 in New York.

“We have got huge challenges when it comes to cybersecurity … Hackers have been able to get into the uplinks and downlinks of our satellite systems, which means your GPS could go out and not come back on. They have been able to get into remote ... driverless cars and slam on the brakes when they are going 55 to 60 mph," the former lawmaker added.

Rogers pointed out various cyber threats that the U.S. is currently facing, including from nation-states and international hacking organizations.

21.02.17

The Hill
Defense chief asks for plan on cyber reform

Defense Secretary James Mattis is asking Pentagon leaders to develop a plan to improve support of cyber operations and information management.

Mattis issued a memo on organizational and structural reforms to his deputy and other officials last week, moving forward on reforms spelled out in an annual defense policy bill.

The guidance instructs officials to address several reforms put forth in the fiscal year 2017 National Defense Authorization Act (NDAA) signed by then-President Obama in December, including plans to boost the military's cyber operations.

"Develop an initial plan … for more optimized organizational structure and processes to support information management and cyber operations, considering the impact of the provisions in the NDAA for 2017 concerning the establishment of U.S. Cyber Command, and other relevant laws," Mattis wrote in the memo, which was highlighted by the Pentagon on Tuesday.

Congress aimed to strengthen cybersecurity with the defense legislation by elevating the U.S. Cyber Command — previously under the authority of the U.S. Strategic Command — to a unified command. It also put a hold on separating the dual-hat authority over the Cyber Command and National Security Agency, pending an assessment by the Pentagon.

21.02.17

The Hill
Cyberattacks a top concern of businesses worldwide, survey finds

Nearly nine in 10 businesses worldwide are worried about the threat of cyberattacks, according to a new survey.

Cyberattacks, followed by data breaches and unplanned IT and telecom outages are the leading causes of concern regarding operations among businesses globally, according to a study from the Business Continuity Institute and British Standards Institute.

Eighty-eight percent of businesses report being concerned or extremely concerned about the threat of cyberattacks, including malware and distributed denial of service attacks. Cyberattacks have topped the list of perceived threats for three straight years in the annual study, which surveyed more than 700 organizations in 79 different countries this year.

Cyberattacks and intrusions have attracted increased attention in the wake of the election-related hacks of systems used by the Democratic National Committee and former Clinton campaign chairman John Podesta and massive data breaches disclosed by Yahoo.

By one estimate, cyberattacks cost businesses a total $400 billion annually, a figure that is expected to rise in coming years.

The pair of Yahoo data breaches—which were announced last year within months of one another—resulted in Verizon Communications acquiring the company at a $350 million discount in a revised deal announced Tuesday.

Privacy

16.02.17

Reuters
EU privacy watchdogs seek assurances on U.S. data transfer pact

European Union data privacy watchdogs will seek assurances from U.S. authorities that a move by U.S. President Donald Trump to crack down on illegal immigration will not undermine a transatlantic pact protecting the privacy of Europeans' data.

European concerns have been raised by an executive order signed by Trump on Jan. 25 aiming to toughen enforcement of U.S. immigration law.

The order directs U.S. agencies to “exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.”

The exemption of foreigners from the U.S. law governing how federal agencies collect and use information about people has stoked worries across the Atlantic about the new administration's approach to privacy and its impact on cross-border data flows.

Internet Inclusion

16.02.17

Bloomberg
Alphabet Scraps Plan to Blanket Globe With Internet Balloons

In 2013, Google ran its first tests for Project Loon, an ambitious effort to circulate broadband-emitting balloons across the globe. On Thursday, the company said that’s not necessary anymore.

Executives at the project said they have found ways to run the program with fewer balloons. Rather than building a worldwide network, the team will now launch a small number of balloons into particular regions that need internet access. That will accelerate the project’s path toward becoming an actual commercial operation, the Loon team said. The announcement is consistent with moves across Google parent Alphabet Inc. to curb costs at its riskier, expensive projects.

“We can now run an experiment with 10 or 20 or 30 balloons,” said Astro Teller, the head of X, the Alphabet division that houses Project Loon. “The service has a much better chance of ultimately being profitable.”

Teller said the team would be testing with telecommunications providers “in the coming months.”

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

16.02.17

MIS Asia
No consensus in approach to defending cyber threats in Singapore

Boardroom executives and IT Decision Makers (ITDMs) are at odds in their approach to defending against cyber threats, according to a new research published by cyber defence experts, BAE Systems.

The 30 board directors and 120 IT leaders polled in Singapore believed that the other party is responsible for managing the response to a cyber-attack.

Two-thirds of C-Suite respondents say their IT teams and staff more broadly are responsible in the event of a breach, whereas 39 percent of ITDMs think this is the case.

Meanwhile, 57 percent of ITDMs think senior management and leaders should shoulder the blame of a breach, as compared to less than a quarter (24 percent) of C-Suite respondents.

The research also indicated that the board level directors' estimated cost of a successful attack was S16.5 million lower than that of their IT colleagues.

17.02.17

SC Magazine
UK and China agree coordination on cyber-security issues

The UK and China have, “agreed to regular coordination on cyber-security related issues in order to prevent cyber-commercial espionage and related transnational criminal activity. I welcomed China's openness to signing-up to the WeProtect global alliance on preventing child sexual exploitation online,” said Sir Mark Lyall Grant, the UK's national security adviser.

He was hosting Wang Yongqing, secretary-general of the Central Commission for Politics and Law, for the second UK-China High Level Security Dialogue.

The dialogue focused on cooperation on cyber-security, counter-terrorism and countering violent extremism, and organised crime.

During the dialogue, the National Security Adviser and Secretary-General Wang agreed various measures aimed at strengthening UK and China security cooperation.

21.02.17

Network Asia
NEC to provide cyber-attack defense training for ASEAN countries

NEC Corporation says it has received an order from the Japan International Cooperation Agency (JICA) to provided cyber-attack defense for officials from governmental institutions responsible for cyber security in six members of the Association of Southeast Asian Nations (ASEAN) (Cambodia, Indonesia, Laos, Myanmar, the Philippines and Vietnam).

The first round of the training is scheduled from February 20 to March 3, 2017.

Damage due to cyber-attacks has recently been spreading globally. Given the increasingly serious damage attributable to such targeted attacks on governmental organizations and critical infrastructure, there is a growing necessity to take measures to improve cyber security capabilities.

This defense training, which will take place in Japan over a three year period, aims to improve incident response, including the early discovery and detection of damage, as well as the implementation of countermeasures to targeted cyber-attacks on ASEAN countries.

Training sessions feature lectures on the latest threats and security measures, as well as drills similar to the Cyber Defense Exercise with Recurrence (CYDER), which are practical cyber-attack defense drills that have been conducted by the Ministry of Internal Affairs and Communications in Japan since 2013.

21.02.17

ZD Net
Singapore opens $5.9M cybersecurity lab in local university

Singapore has opened a cybersecurity facility to support research efforts between academia and industry players and provide a testbed for product development.

Located at the National University of Singapore (NUS), the S$8.4 million (US$5.93 million) site would provide a “realistic environment” for cybersecurity research and testing, according to a joint statement Tuesday by the university and Singapore's National Research Foundation (NRF).

It can simulate more than 1,000 computers to perform various tasks to create cybersecurity incidents, such as large-scale malicious cyber attacks. It also has a large database of malware that can be tapped for research and education purposes. These capabilities were expected to be further expanded three-fold by year-end.

The new facility is an initiative of the country's cybersecurity R&D programme, which is supported by various government ministries and agencies, including NRF, Cyber Security Agency, Ministry of Home Affairs, and Ministry of Defence, as well as academia, research institutes, and enterprises. The national scheme focuses on driving research efforts and capabilities in cybersecurity as well as beefing up digital infrastructures, specifically, in terms of security, reliability and resiliency. NRF is parked under the Prime Minister's Office.

22.02.17

Economic Times
India's cyberspace intelligence agency to be functional from June

In wake of the unprecedented rise in the digital transactions in the country, the government is fast-tracking its efforts to build a robust cyber security ecosystem. The country’s apex cyberspace intelligence agency, the National Cybersecurity Coordination Centre (NCCC), will become functional in June this year while sector specific computer emergency response teams (CERT) for industries such as power, communications etc., will also be created, Ravi Shankar Prasad, Union Minister for Electronics and IT said on Tuesday.

Prasad was speaking at the launch of the Botnet Cleaning and Malware Analysis Centre called the Cyber Swachhta Kendra, which will help individuals and organisations in analysing malware and botnets that affect networks and systems.

Prasad said that India is on the path of becoming one trillion dollar digital economy over the coming years and will need to have strong cybersecurity to facilitate it. Prasad said that while the ministry has already launched a division for digital payments under CERT and a financial CERT is also being set up, states will be encouraged to set up their own CERTs.

Privacy

21.02.17

The Australian
India leads the way in biometrics with huge database

India is leapfrogging into the digital future by offering the world’s largest biometric-identity database for use by tech firms, healthcare providers and novice app developers — an opportunity that excites fans of cyber transactions but worries privacy advocates.

The Indian government has gathered digital-identification records, including fingerprint impressions and eye scans, of nearly all of its 1.2 billion citizens.

Now a government-backed initiative known as “India Stack” aims to standardise ways to exchange the data digitally to facilitate the transfer of signatures and official documents that citizens need to get jobs, make financial transactions or access government services.

By allowing developers to incorporate use of government identification records in their commercial websites and apps, the initiative envisages Indians — with mobile phones in hand — using iris and fingerprint scans to sign up for insurance, invest in mutual funds, receive health subsidies and verify their identity for school examinations.

Internet Inclusion

16.02.17

Bloomberg
Alphabet Scraps Plan to Blanket Globe With Internet Balloons

In 2013, Google ran its first tests for Project Loon, an ambitious effort to circulate broadband-emitting balloons across the globe. On Thursday, the company said that’s not necessary anymore.

Executives at the project said they have found ways to run the program with fewer balloons. Rather than building a worldwide network, the team will now launch a small number of balloons into particular regions that need internet access. That will accelerate the project’s path toward becoming an actual commercial operation, the Loon team said. The announcement is consistent with moves across Google parent Alphabet Inc. to curb costs at its riskier, expensive projects.

“We can now run an experiment with 10 or 20 or 30 balloons,” said Astro Teller, the head of X, the Alphabet division that houses Project Loon. “The service has a much better chance of ultimately being profitable.”

Teller said the team will be testing with telecommunications providers “in the coming months.”

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

16.02.17

SC Magazine
Uganda and Malawi sign pact to fight cybercrime and build capabilities

Uganda signed a memorandum of Understanding with the government of Malawi aimed at increasing collaboration to fight cyber-crime, Uganda's minister for ICT Frank Tumwebaze told SCMedia UK in an exclusive interview.

According to the minister, the memorandum of understanding will allow the two countries collaborate in areas of cyber-security, policy formation, regulation and research among others. The two countries will also collaborate in policy implementation and capacity-building through training their respective departments.

“This is a confidence-building measure for us which helps us to validate what we have been trying out in terms of policy and programmes,” Tumwebaze said.

“The government is committed to building the country's cyber-security capacity to enable growth of the ICT sector as well as assure safety and security of the government's online data," he added.

Benchmarking the ICT sector in the Republic of Uganda has enabled them learn a lot which they intend to implement in their own country, the ICT minister for Malawi Nicholas Ndausi, said.

22.02.17

ZD Net
Australian government pledges AU$1.9m to beef up cybersecurity skills

The Australian government has promised AU$1.9 million to universities that deliver specialised cybersecurity training in a bid to combat the skills shortage in cyber-related fields.

“Cybersecurity skills are fundamental to the success and growth of Australia's digital economy, but like many other nations, Australia is suffering from a skills shortage in this field,” Minister Assisting the Prime Minister on Cyber Security Dan Tehan said in a statement on Wednesday.

Under the program, universities can apply to be recognised as Academic Centres of Cyber Security.

The government hopes the funding injection will help attract more Australians to cybersecurity jobs and increase the number of skilled graduates needed to help protect businesses and government from emerging threats.

“The new centres will help build Australia's capability by leading the way as cybersecurity training facilities,” Tehan added.

The Australian government launched its Cyber Security Growth Centre in December. Based in Melbourne, the centre now operates as a not-for-profit company under the new name of the Australian Cyber Security Growth Network Ltd.

Privacy

No new items of relevance

Internet Inclusion

16.02.17

Bloomberg
Alphabet Scraps Plan to Blanket Globe With Internet Balloons

In 2013, Google ran its first tests for Project Loon, an ambitious effort to circulate broadband-emitting balloons across the globe. On Thursday, the company said that’s not necessary anymore.

Executives at the project said they have found ways to run the program with fewer balloons. Rather than building a worldwide network, the team will now launch a small number of balloons into particular regions that need internet access. That will accelerate the project’s path toward becoming an actual commercial operation, the Loon team said. The announcement is consistent with moves across Google parent Alphabet Inc. to curb costs at its riskier, expensive projects.

“We can now run an experiment with 10 or 20 or 30 balloons,” said Astro Teller, the head of X, the Alphabet division that houses Project Loon. “The service has a much better chance of ultimately being profitable.”

Teller said the team will be testing with telecommunications providers “in the coming months.”

Global Institutions

16.02.17

The Hill
NATO, Finland deepen cooperation on cyber defense

The North Atlantic Treaty Organization (NATO) and Finland are stepping up their cooperation on cyber defense in the face of increased threats in cyberspace and a resurgent Russia.

NATO and Finland on Thursday signed a political framework agreement on cyber defense cooperation that will allow them to better protect and strengthen their networks.

“We look forward to enhancing our situational awareness and exchanging best practices with Finland, including through dedicated points of contact for rapid information exchange on early warning information and lessons learned,” Ambassador Sorin Ducaru, NATO’s assistant secretary general for emerging security challenges, said.

Jukka Juusti, permanent secretary of Finland’s defense ministry, indicated that the country also wants to boost cooperation with the alliance by holding more joint cyber training and exercises. Finland already participates in the alliance’s Cyber Coalition, an annual cyber defense exercise.

16.02.17

ENISA
Security Measures for Digital Service Providers

ENISA issues this report to assist Member States and DSPs in providing a common approach on the security measures for DSPs. The study describes the high-level security objectives by providing security measures and examples of implementation concerning DSPs and in particular:

- Cloud computing service providers
- Online marketplaces
- Online search engines

With this study ENISA tries to:

- Define common baseline security objectives for Digital Service Providers (DSPs).
- Describe different levels of sophistication of security measures which fulfil the abovementioned security objectives

- Map the security objectives against well-known industry standards, national frameworks and certification schemes.

The report together with other relevant technical standards have been used as input to the discussions on the implementation of article 16(1) of the NIS Directive concerning the security measures of the DSPs.

The NIS Directive aims to develop cybersecurity capabilities across EU Member States. Commonly defined security measures can support harmonised security practices across Member States and potentially enhance the overall level of NIS in the EU.

Full report available online.

20.02.17

European Internet Forum
Free Movement of data in the EU

On 8 February, EIF and EIF Chair Pilar del Castillo MEP hosted a debate to discuss the best approach to enable data flows within EU in order to future-proof the EU Digital Single Market.

In her opening remarks, Ms. del Castillo stressed the new opportunities presented by the growth of the data economy and the importance of what needs to be done to realize its full potential for Europe.

Krzysztof Szubert, Plenipotentiary Minister of Digital Affairs for International Affairs (Poland), likewise addressed the importance of the free flow of data for the creation of the Digital Single Market, and cited as one of the biggest challenges striking the right balance between data flows and data privacy.

Pearse O'Donohue, acting Director for Future Networks at DG CONNECT, presented the European Commission’s view on the free data flow in the EU and noted the current public consultation on the Commission’s Communication and working document on the European data economy

Hosuk Lee-Makiyama, Director of European Centre for International Political Economy (ECIPE), spoke about the economic consequences of failing to ensure the free data movement in Europe.

Archie Ravishankar, CEO of Cogni, presented the view of the start-up community.

Dr. Klaus Mittelbach, CEO of ZVEI (German Electrical and Electronic Manufacturers' Association), spoke on behalf of the manufacturing industry on the importance of the free movement of data.

20.02.17

European Internet Forum
E Privacy

On 8 February, EIF member MEPs Axel Voss and Michal Boni hosted a debate to explore whether a revised e-privacy directive is necessary in addition to the General Data Protection Regulation (GDPR), or whether it would create unnecessary overlap and legal uncertainty.

In his opening remarks, Mr. Voss questioned the need for a new e-privacy directive and asked whether the GDPR should not be sufficient to ensure the desired level of privacy protection.

Dr. Claus-Dieter Ulmer, Senior Vice President, Global Data Privacy Officer at Deutsche Telekom, endorsed the GDPR and questioned the need for anything more.

Wojciech Wiewiórowski, Assistant Supervisor at the European Data Protection Supervisor, stressed the need to have efficient protection of data privacy and addressed the complementarity between these different legal acts.

Cornelia Kutterer, Microsoft's EU Government Affairs & Digital Policy Director, stressed the importance of considering how means of communications will evolve in coming years when considering new privacy regulations.

David Martin, Senior Legal Officer at BEUC, cited Eurobarometer indications of citizens privacy concerns and expectations, and argued that an e-privacy directive and the GDPR are necessary to meet them and can coexist while overlap can be avoided. He also expressed a concern that the principles of privacy by default and privacy by design were ignored in the latest proposal.

21.02.17

ICANN
Recommendations to Improve ICANN's Transparency

This Public Comment seeks community input on the CCWG-Accountability Work Stream 2 draft recommendations to improve ICANN's transparency. These draft recommendations were developed by the CCWG-Accountability as required by Annex 12 of the final report of the Cross Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability, Work Stream 1).

The CCWG-Accountability reviewed these draft recommendations at its 8 February 2017 plenary meeting and approved their publication to gather public comments.

Following the public comment period the inputs will be analyzed by the CCWG-Accountability WS2 who will consider amending its recommendations in light of the comments received and will publish a report on the results of the public consultation. If significant changes are required as a result of the public consultation the CCWG-Accountability WS2 may opt to have a second public consultation on the amended recommendations. If there are no significant changes required, the CCWG-Accountability WS2 will forward the final recommendations on improving ICANN's Transparency to its Chartering Organizations for approval and then to the ICANN Board for consideration and adoption.

The Public Comment will run from 21 February 2017 to 10 April 2017.

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