
## 26 April 2017

# Synopsis

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

**NATO** members and allies are currently conducting the largest global **cyber defence** exercise in **Estonia**. The participants are responding to a scenario in which the military resources of a fictitious country are subjected to a cyber attack.

In the **UK** the national data protection watchdog has raised concerns that not enough clarity currently exists regardint the EU's concept of **consent** in the incoming **General Data Protection Regulation**.

The Dutch courts have overturned a ruling by the **Dutch Telecommunicaitons** regulator that had found **T-Mobile** in violation of Dutch **net neutrality** legislation, stating that EU rules on zero-rating allowed T-Mobile to continue the practise even if it was banned in the Netherlands.

The White House's Office of **American** Innovation led by **Jared Kushner** has announced that the administration's top Cyber Czar will participate in activities to ensure that all new government tools consider **cybersecurity** from the outset.

**FCC** Chairman **Ajit Pai** has made clear his intention to begin expected reforms to Obama-era **net neutrality** rules. Sources close to Mr Pai have suggested that reforms could be conducted quickly, with the Fall an anticipated final date for completion.

The **Indian** government have implemented a **gag** on **internet access** in the Kashmir valley region, restricting the use of 3G and 4G services by student protestors to post videos of demonstrations against the Government.

**China's** national **CERT** team has reported that the country is facing increasing **cyber threats** from **IoT** devices and networked industrial systems. Elsewhere the Chinese Government have agreed to a new **cybersecurity** partnership with **Australia**, in which shared norms for digital usage will be adopted to prevent **cybercrime** and theft between the two countries.

The Government of **Cameroon** has returned **internet access** to the Anglophone regions in the South and Northwest of the country. The **ban** had been imposed in response to anti-government protests, in which the Government alleged social media had been used to spread false information.

**ITU** has announced that **Argentina** has formally agreed to hold the **2017 World Telecommunication Development Conference**, set to be held in Buenos Aires in October.

**IEEE Global Internet Policy Monitor**

**26 April 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

**24.04.17**

**SC Magazine**

**New cyber-security research centre launches at Cardiff University**

The first European centre of excellence for cybersecurity research has opened at Cardiff University. The centre will look at cutting edge techniques for the detection of cyber attacks, as well as the development of academic programmes to address the UK's cybersecurity skills gap.

*"As the first centre of its kind in Europe, the Centre of Excellence in Cyber-Security Analytics will be located at Cardiff University's School of Computer Science and Informatics.*

*"Cyber-security research is of critical importance in our digital society so it's extremely important that we find innovative, real-world solutions to help detect, and protect against, dangerous cyber-attacks," said Professor Colin Riordan, vice-chancellor at Cardiff University."*

**24.04.17**

**The Hill**

**EU member of parliament: Nationalism at odds with international cybersecurity**

Dutch MEP Marietje Schaake has criticised protectionist measures to close borders, stating that it could have a significant impact on the security of digital borders and wider cyberspace. Ms Schaake also argued that such actions did not support the ideal of free internet.

*"A member of the European Union's Parliament described the rising tide of nationalism in the United States and Europe as antithetical to cybersecurity and the free internet at a conference featuring a number of world cybersecurity policy leaders Monday at Georgetown University.*

*MEP Marietje Schaake (Netherlands) said that closing borders to try to regain control over diminishing power could have dire consequence on the online landscape."*

**25.04.17**

**The Hill**

**DNC hackers targeted French presidential candidate Macron: researchers**

Trend Micro has reported that the same hackers that targeted the Democratic party during the US Presidential election have targeted Emmanuel Macron, France's leading candidate in this year's Presidential election.

*"The hackers behind the Democratic National Committee (DNC) email breach appear to have made similar attacks against Emmanuel Macron, a French candidate for president, as well as groups associated with German political parties, according to a new report.*

*The security firm Trend Micro reports that the hacking groups known as Fancy Bear, APT 28 and Pawn Storm attacked the French and German targets using similar phishing schemes to the one that caught the DNC. U.S. intelligence, as well as the bulk of experts, believe Fancy Bear is a Russian espionage operation."*

**25.04.17**

**Yahoo**

**Cyber spies target German party think-tanks ahead of election**

Trend Micro have also reported that two German think tanks connected to the CDU and SPD parties have been targeted in the same cyber attacks that have affected the French Presidential candidate Emmanuel Macron and are believed to have originated from the same group that target the Democratic Party in the 2016 US Presidential Election.

*"Two foundations tied to Germany's ruling coalition parties were attacked by the same cyber spy group that targeted the campaign of French presidential favourite Emmanuel Macron, a leading cyber security expert said on Tuesday.*

*The group, dubbed "Pawn Storm" by security firm Trend Micro, used email phishing tricks and attempted to install malware at think tanks tied to Chancellor Angela Merkel's Christian Democratic Union (CDU) party and coalition partner, the Social Democratic Party (SPD), Feike Hacquebord said."*

**26.04.17**

**NATO**

**[World's largest cyber defence exercise takes place in Estonia]**

NATO members and allies are currently conducting the largest global cyber defence exercise in Estonia. The participants are responding to a scenario in which the miliarty resources of a fictitious country are subjected to a cyber attack.

*"Locked Shields 2017, the largest and most advanced cyber defence exercise in the world, is taking place this week. It is organized by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.*

*The exercise involves around 800 participants from 25 nations. Participants include security experts who protect national IT systems, policy officers and legal advisors from NATO Allies and Partners. According to the exercise scenario, experts will have to defend the services and networks of a military air base of a fictitious country, against cyber-attacks targeting the base's electric power grid system, drones, military command and control systems and other infrastructure. More than 2500 cyber-attacks will be simulated. While IT experts will train to defend computer networks and handle legal and forensic challenges, policy officers will exercise their decision-making procedures."*

## Privacy

**20.04.17**

**SC Magazine**

**[Information Commissioner notes confusion over 'Consent' in GDPR]**

The national data protection watchdog in the UK has raised concerns that not enough clarity currently exists regardint the EU's concept of consent in the incoming General Data Protection Regulation.

*"The UK's data protection watchdog has noted a great deal of confusion around the concept of 'Consent' drawn out in landmark European regulation set to hit Britain's shores next year.*

*Issues around consent are increasingly troubling the minds of data protection professionals according to a new blogpost from the Information Commissioner's Office (ICO)."*

## Internet Inclusion

**21.04.17**

**GTB**

**T-Mobile Netherlands wins "breakthrough" net neutrality ruling**

The Dutch courts have overturned a ruling by the Dutch Telecommunicaitons regulator that had found T-Mobile in violation of Dutch net neutrality legislation, stating that EU rules on zero-rating allowed T-Mobile to continue the practise even if it was banned in the Netherlands.

*"Deutsche Telekom's Dutch operation has been given permission to continue a free music package, after it won a net neutrality dispute in a court in Rotterdam.*

*The Dutch Authority for Consumer and Market had ordered T-Mobile Netherlands to suspend its Datavrije Muziek service in December, claiming it was in breach of Dutch net neutrality laws because it was detrimental to competition with internet services."*

# United States of America

## Internet governance

***No new items of relevance***

## Cybersecurity

**24.04.17**

**Next Gov**

**White House Cyber Czar to play role in Kushner Innovation Office**

The White House's Office of American Innovation led by Jared Kushner has announced that the administration's top Cyber Czar will participate in activities to ensure that all new government tools consider cybersecurity from the outset.

*"President Donald Trump's top cybersecurity advisor will be pitching in on a government modernization program led by the president's son-in-law Jared Kushner to ensure security is built into any new government tools from the beginning, he said Monday.*

*Kushner's Office of American Innovation has numerous tasks including combating opioid addiction and improving services to veterans but the president put a premium on the office's government modernization role in early comments."*

## Privacy

***No new items of relevance***

## Internet Inclusion

**24.04.17**

**Politico**

**FCC chief to launch net neutrality rewrite this week, sources say**

FCC Chairman Ajit Pai has made clear his intention to begin expected reforms to Obama-era net neutrality rules. Sources close to Mr Pai have suggested that reforms could be conducted quickly, with the Fall an anticipated final date for completion.

*“FCC Chairman Ajit Pai intends to launch his reworking of the Obama-era net neutrality rules, according to sources familiar with the plan, setting up a showdown on an issue that has long pitted tech companies against internet providers.*

*In a speech in Washington on Wednesday, Pai plans to discuss his vision for net neutrality — keeping open internet principles but getting rid of the utility-style regulatory framework approved by the agency's previous Democratic majority. And he could circulate a notice of proposed rulemaking on the plan to his fellow commissioners on Thursday, sources said. That would set up a vote on the issue at the FCC's May 18 meeting. One industry source said the chairman's goal is to finish the proceeding by this fall.”*

# Pan-Asia

## Internet governance

**23.04.17**

**The Tribune (India)**

**Internet gag continues for sixth day**

The Indian government have implemented a gag on internet access in the Kashmir valley region, restricting the use of 3G and 4G services by student protestors to post videos of demonstrations against the Government.

*"An Internet gag, ordered at the beginning of this week, has now entered its sixth day in the Kashmir valley as the authorities remain tight-lipped about restoring the communication services in the region.*

*The high-speed 3G and 4G Internet services have remained affected by the gag, which was ordered in the region in the aftermath of protests by students."*

## Cybersecurity

**21.04.17**

**Ars Technica**

**Researchers claim China trying to hack South Korea missile defense efforts**

The information security firm FireEye have reported an increase in cyber attacks from China directed at South Korea since February when the country announced it would introduce the US THAAD system to protect the country from potential attacks from North Korea.

*"Chinese government officials have been very vocal in their opposition to the deployment of the Terminal High-Altitude Air Defense (THAAD) system in South Korea, raising concerns that the anti-ballistic missile system's sensitive radar sensors could be used for espionage. And according to researchers at the information security firm FireEye, Chinese hackers have transformed objection to action by targeting South Korean military, government, and defense industry networks with an increasing number of cyberattacks. Those attacks included a denial of service attack against the website of South Korea's Ministry of Foreign Affairs, which the South Korean government says originated from China."*

**23.04.17**

**OpenGov Asia**

**China CERT report highlights rise in cyberthreats associated with IoT devices and networked industrial systems**

China's national CERT team has reported that the country is facing increasing cyber threats from IoT devices and networked industrial systems, based on analysis of incidents in 2016 and before.

*"A report released by the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT) on April 19, summarising the Internet Security situation in 2016, highlighted security risks associated with Internet-of-things (IoT) devices and networked industrial systems.*

*The CNCERT report says that as the country's industries adopt and integrate digital technologies into their systems, with progress in the Make in China 20205 initiative, it will create vulnerabilities and bring new cyberthreats."*

**24.04.17**

**SC Magazine**

**Asian Interpol operation finds nearly 9,000 CnC servers**

Interpol have reported that it has identified around 8,800 command and control servers in the ASEAN region, as part of an operation to identify cybersecurity threats in Asia. Of the websites compromised the investigation has found that a number of government portals have been affected, potentially leading to the leak of personal data.

*"Investigators from seven Southeast Asian nations collaborated on a joint Interpol operation that identified approximately 8,800 command-and-control servers in eight countries and nearly 270 compromised websites, including government portals that may have contained personal data on citizens.*

*According to an Interpol press release, the exposed threats included malware attacks against banks and other institutions, ransomware, distribute denial of service attacks, and spam campaigns. The operation, which focused specifically on the ASEAN (Association of Southeast Asian Nations) region, also uncovered several phishing website operators, "including one with links to Nigeria, with further investigations into other suspects still ongoing," the press release announced."*

**24.04.17**

**ZDnet**

**Australia to work with China on cybersecurity**

The Chinese Government have agreed to a new cybersecurity partnership with Australia, in which shared norms for digital usage will be adopted to prevent cybercrime and theft between the two countries.

*"The federal government has announced it has agreed to enhanced cybersecurity cooperation with China, following discussions between Prime Minister Malcolm Turnbull, Foreign Minister Julie Bishop, and Secretary of the Chinese Communist Party's Central Commission for Political and Legal Affairs Meng Jianzhu.*

*During the discussions held last week in Sydney, Australia and China agreed that neither country would conduct or support cyber-enabled theft of intellectual property, trade secrets, or confidential business information with the intent of obtaining competitive advantage."*

## Privacy

***No new items of relevance***

## Internet Inclusion

***No new items of relevance***

# Rest of the World

## Internet governance

***No new items of relevance***

## Cybersecurity

**21.04.17**

**SC Magazine**

**Kenya set to pass cybercrime bill as east Africa seeks legal harmony**

A further step towards legal harmonisation on cybercrime in East Africa is nearing completion after the Kenyan Government announced its intentions to introduce a new Computer and Cybercrime Bill, that will be expected to pass into law by the end of 2017.

*"The Kenya government is set to pass the Computer and Cybercrime Bill into law after its approval by cabinet as east African countries push for regional harmonisation of cyber-crime laws.*

*The bill is set to be tabled in parliament for debate and then go to a vote within the next few weeks. After that, it is expected to be signed by the president before the end of the year."*

**24.04.17**

**ZDnet**

**Australia to work with China on cybersecurity**

The Chinese Government have agreed to a new cybersecurity partnership with Australia, in which shared norms for digital usage will be adopted to prevent cybercrime and theft between the two countries.

*"The federal government has announced it has agreed to enhanced cybersecurity cooperation with China, following discussions between Prime Minister Malcolm Turnbull, Foreign Minister Julie Bishop, and Secretary of the Chinese Communist Party's Central Commission for Political and Legal Affairs Meng Jianzhu.*

*During the discussions held last week in Sydney, Australia and China agreed that neither country would conduct or support cyber-enabled theft of intellectual*

*property, trade secrets, or confidential business information with the intent of obtaining competitive advantage."*

**24.04.17**

**All Africa**

**Rwanda: Parliament Passes Cyber Security Bill**

The lower chamber of the Rwandan Parliament have passed a draft law that will establish a National Cyber Security Authority in Rwanda. Last year the draft law was returned to the Parliament for approval after President Paul Kagame asked for further discussion of national security powers in the bill.

*"Members of the Lower Chamber of Parliament have passed the draft law establishing the National Cyber Security Authority (NCSA) and determining its responsibilities, organisation and functioning.*

*The Bill establishing NSCA was initially passed by parliament last October to safeguard private and government information and infrastructure against online crimes and cyber-attacks."*

**26.04.17**

**ZDnet**

**NTT Security finds 86 percent of Australia's attacks come from within**

The security firm NTT Security has found in its 2017 Global Threat Intelligence Report that 86% of cyberattacks in Australia originate domestically, with 10% of attacks originating from Australia's allies the USA and Germany.

*"86 percent of the total attacks experienced by Australia during a 12-month period originated from within the country's borders, a report from NTT Security has found.*

*The United States was the source of 9 percent of the total attacks, while Germany accounted for 1 percent."*

## Privacy

***No new items of relevance***

## Internet Inclusion

**25.04.17**

**Newsweek**

**Residents of English-speaking Cameroon have access to Internet resored as Government lifts ban**

The Government of Cameroon has returned internet access to the Anglophone regions in the South and Northwest of the country. The ban had been imposed in response to anti-government protests, in which the Government alleged social media had been used to spread false information.

*"Residents of Cameroon's English-speaking regions have welcomed the lifting of an internet ban implemented in response to fierce anti-government protests. Authorities imposed the ban in January, claiming people were using social media to spread false information.*

*Lawyers, teachers and students have led protests in the south- and northwestern provinces of the country since October 2016. At the heart of the dispute is the use of French in courts and schools. Elsewhere, the employment of court workers who do not understand British common law also sparked protests."*

# Global Institutions

**20.04.17**

**ICANN**

**ICANN Holds First Capacity Development Workshop for Pacific GAC Members**

ICANN has announced that at the end of April it will hold a capacity development workshop with members of the Pacific Governmental Advisory Committee for the first time.

*"The Internet Corporation for Assigned Names and Numbers (ICANN) in cooperation with the ICANNGovernmental Advisory Committee (GAC) Under-served Regions Working Group will hold the first capacity development workshop for Pacific GAC members and representatives from 28 – 29 April 2017 in Nadi, Fiji.*

*The workshop, themed "Harnessing the Potential of the Pacific GAC Representatives for Better Participation in ICANN", will focus on raising awareness and assist in building capacity of Pacific GACrepresentatives and governments on how best to effectively participate and contribute to policy making at ICANN. It is supported by the Fiji Government's Department of Communications."*

**21.04.17**

**ITU**

**Communiqué: ITU and Argentina sign Host Country Agreement...**

ITU has announced that Argentina has formally agreed to hold the 2017 World Telecommunication Development Conference, set to be held in Buenos Aires in October.

*"The International Telecommunication Union (ITU) and the Government of Argentina have signed a Host Country Agreement to formalize arrangements for the World Telecommunication Development Conference (WTDC-17), to be held 9-20 October 2017 in Buenos Aires, Argentina, following the invitation of the Government of Argentina.*

*The agreement was signed by ITU Secretary-General Houlin Zhao and Mr Héctor Marcelo Cima, Ambassador Extraordinary and Plenipotentiary, on behalf of the Government of Argentina."*

**26.04.17**

**NATO**

## World's largest cyber defence exercise takes place in Estonia

NATO members and allies are currently conducting the largest global cyber defence exercise in Estonia. The participants are responding to a scenario in which the miliarty resources of a fictitious country are subjected to a cyber attack.

*"Locked Shields 2017, the largest and most advanced cyber defence exercise in the world, is taking place this week. It is organized by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.*

*The exercise involves around 800 participants from 25 nations. Participants include security experts who protect national IT systems, policy officers and legal advisors from NATO Allies and Partners. According to the exercise scenario, experts will have to defend the services and networks of a military air base of a fictitious country, against cyber-attacks targeting the base's electric power grid system, drones, military command and control systems and other infrastructure. More than 2500 cyber-attacks will be simulated. While IT experts will train to defend computer networks and handle legal and forensic challenges, policy officers will exercise their decision-making procedures."*

# Diary Dates

**ITU Council 2017 – 15.05.17 – 25.05.17**

Geneva, Switzerland

**Africa Internet Summit (AIS) 2017 – 29.05.17 – 02.06.17**

Nairobi, Kenya

**European Dialogue on Internet Governance – 06.06.17-07.06.17**

Tallinn, Estonia

**World Summit on the Information Society Forum (WSIS) 2017 – 12.06.17 – 16.06.17**

Geneva, Switzerland

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

Dublin, Ireland

**ITU WTDC-17 – 09.10.17 – 20.10.17**

Buenos Aires, Argentina

**IGF 2017 – 18.12.17 – 21.10.17**

Geneva, Switzerland