



3 May 2017

Synopsis

Scroll to read full summaries with links to news articles.

The head of **Germany's** domestic intelligence agency has warned that the threat of **cyberattacks** facing German companies are not taken seriously. **Mr Maassen** has called for greater powers for Government authorities to tackle cybersecurity threats but that more must be done by the private sector.

Also in **Germany** this week an administrative court has upheld a **ban** on the transfer of data between **WhatsApp** and **Facebook**. The original ban prevented the two companies from exchanging client data without the consent of customers following the acquisition of WhatsApp by Facebook.

The **US** National Security Agency has announced that it will put an end to the upstream practise of **foreign surveillance** in which the **data** of US citizens discussing foreign surveillance targets was recorded.

In an interview with **CBS** show Face the Nation President **Donald Trump** has alleged that **China** could have been responsible for the **hacking** of Democratic officials during last year's Presidential election.

Nine **Republican Senators** have proposed legislation that would prohibit the Federal Communications Commission from reintroducing **net neutrality** in the future.

The **Chinese** internet regulator has updated its regulations to introduce a requirement for all online news broadcasters to first obtain a **government licence**.

A new study by **Symantec** has found that **India** ranks fourth in global online **security breaches**, accounting for 5% of all detected threats.

The **Kenyan** government has rejected a proposal to punish African Governments that shutdown **internet access** for their citizens.

The **World Economic Forum** has announced a new collaboration with the Government of **South Africa** to increase **internet access** in the country as part of an Internet for All project.

The **European Internet Forum** has hosted a debate with two MEPs to discuss the importance of **digital skills** for participation in modern society.

Representatives of **Digital Europe** have attended a **Bruegel** sponsored event on **ePrivacy** in which Senior Policy Manager **Alexander Whalen** highlighted potential limitations in the EU's ePrivacy Directive.

IEEE Global Internet Policy Monitor

3 May 2017

Table of Contents

Synopsis	1
Europe	4
Internet governance	4
Cybersecurity	4
Privacy	5
Internet Inclusion	6
United States of America	6
Internet governance	7
Cybersecurity	7
Privacy	7
Internet Inclusion	9
Pan-Asia	10
Internet governance	10
Cybersecurity	10
Privacy	11
Internet Inclusion	11
Rest of the World	12
Internet governance	12
Cybersecurity	13
Privacy	13
Internet Inclusion	13
Global Institutions	15
Diary Dates	17

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

27.04.17

Daily Mail

[Germany confirms cyber attacks on political party think tanks](#)

German officials have confirmed the claims made by Trend Micro of repeated cyberattacks against foundations linked to current SPD and CDU government parties. The authorities did not go as far as the security firm in identifying the perpetrators of the attack however.

“Germany's top cyber official on Thursday confirmed said his agency was aware of computer attacks on two foundations tied to Germany's ruling coalition parties for some time, and was helping the think tanks analyse what happened.

Arne Schoenbohm, president of the BSI federal cyber security agency, did not comment on security firm Trend Micro's claim that the attacks were carried out by "Pawn Storm," the same Russian hacking group linked to attacks on French presidential candidate Emmanuel Macron or the U.S. election.”

27.04.17

ABC News

[Spy chief urges German firms to take cybersecurity seriously](#)

The head of Germany's domestic intelligence agency has warned that the threat of cyberattacks facing German companies are not taken seriously. Mr Maassen has called for greater powers for Government authorities to tackle cybersecurity threats but that more must be done by the private sector.

“The head of Germany's domestic intelligence agency says companies aren't taking cybersecurity seriously enough at a time when the threat of electronic attacks is rising.

Hans-Georg Maassen says cyberattacks and disinformation campaigns cost German companies up to 50 billion euros (\$55 billion) a year.

Maassen said Thursday at a business seminar in Berlin it would be good if authorities were given the power to stop such attacks, and that may mean acquiring the ability to strike back against computer networks used to launch them.”

27.04.17

Azer News

[Azerbaijan, France mull strengthening cybersecurity](#)

The respective defence ministries of Azerbaijan and France are currently working on strengthening existing cooperation on cybersecurity through a series of meetings currently underway in Baku, Azerbaijan.

“Baku hosts a working meeting of experts on cybersecurity in accordance with the plan of bilateral cooperation for 2017, signed between the Defense Ministries of Azerbaijan and France.

The experts noted the importance of strengthening cybersecurity measures in the nation's critical infrastructure, such as government, communications and financial services, transport as well as in other areas, the Azerbaijani Defense Ministry reported on April 27.”

Privacy

26.04.17

Info World

[German court upholds WhatsApp-Facebook data transfer ban](#)

A German administrative court has upheld a ban on the transfer of data between WhatsApp and Facebook. The original ban prevented the two companies from exchanging client data without the consent of customers following the acquisition of WhatsApp by Facebook.

“Facebook must obtain the permission of German users of WhatsApp before processing their personal data, a German court confirmed on Tuesday.

Last August, Facebook subsidiary WhatsApp changed its privacy policy to allow the transfer of its users' personal information to Facebook for processing. That angered the Hamburg Commissioner for Data Protection and Freedom of Information, which in September [ordered the companies to stop the transfer](#) until they had obtained users' consent, and to delete any data they had already transferred.”

Internet Inclusion

No new items of relevance

United States of America

Internet governance

No new items of relevance

Cybersecurity

28.04.17

Techworld

[U.S. military wants white-hat hackers to target its cyber security systems](#)

The US military has continued to support bug bounty programmes, following successful experiences with the Army and Pentagon. The newest bug bounty programme will test specific sections of the Air Force's public website and will use a team of international hackers rather than American.

"The U.S. military, which continues its interest in bug bounty programs as a way to improve cybersecurity, is launching a new contest next month.

Called "Hack the Air Force," the new program will put certain of the branch's Web sites up as targets for a set of international hackers who have been vetted by [HackerOne](#), which is running the program."

01.05.17

Reuters

[Trump says China could have hacked Democratic emails](#)

In an interview with CBS show Face the Nation President Donald Trump has alleged that China could have been responsible for the hacking of Democratic officials during last year's Presidential election.

"President Donald Trump said China may have hacked the emails of Democratic officials to meddle with the 2016 presidential election, countering the view of U.S. intelligence officials who have said Moscow orchestrated the hacks.

In an interview transcript published on Sunday, Trump gave no evidence backing his allegation, first made on the eve of the Nov. 8 presidential election, that China could have hacked the emails of his rivals."

Privacy

30.04.17

Ars Technica

[NSA ends spying on messages Americans send about foreign surveillance targets](#)

The US National Security Agency has announced that it will put an end to the upstream practise of foreign surveillance in which the data of US citizens discussing foreign surveillance targets was recorded.

“Today, a spokesperson for the National Security Agency announced that the agency would end the practice of “upstream” collection of messages sent by American citizens—messages that were not directed to targets of NSA intelligence collection but referred to “selectors” for those targets in the body of the communications. According to [the statement](#), the NSA has put an end to that practice, which has been authorized since 2008 under the agency’s interpretation of Section 702 of the Foreign Intelligence Surveillance Act (FISA).”

02.05.17

Reuters

[Privacy group sues NYPD for release of facial-recognition documents](#)

The Center for Privacy and Technology at Georgetown University Law School has filled a suit against the New York Police Department this week to force the disclosure of documents relating to the Department’s use of facial-recognition technology.

“A privacy group sued the New York Police Department on Tuesday to demand the release of documents related to its use of facial-recognition technology, which rights groups have criticized as discriminatory and lacking in proper oversight.

The lawsuit is the latest attempt to compel U.S. law enforcement agencies to disclose more about how they rely on searchable facial-recognition databases in criminal investigations.”

Internet Inclusion

02.05.17

Ars Technica

[GOP's "Internet Freedom Act" permanently guts net neutrality authority](#)

Nine Republican Senators have proposed legislation that would prohibit the Federal Communications Commission from reintroducing net neutrality in the future. The legislation would prevent the FCC from classifying Internet Service Providers as common carriers over which the FCC has authority.

"Nine Republican US senators yesterday submitted legislation that would prohibit the Federal Communications Commission from ever again using the regulatory authority that allowed the commission to impose net neutrality rules. The ["Restoring Internet Freedom Act"](#) would prohibit the FCC from classifying ISPs as common carriers under Title II of the Communications Act and "from imposing certain regulations on providers of such service."

The Internet "is threatened by the Federal Communications Commission's 2015 Open Internet Order, which would put federal bureaucrats in charge of engineering the Internet's infrastructure," Sen. Mike Lee (R-Utah). said in an [announcement](#) yesterday. "That is why I am introducing the Restoring Internet Freedom Act, which would nullify [the] Open Internet Order and prohibit the FCC from issuing a similar rule in the future."

01.05.17

Info World

[Appeals court won't rehear a challenge to net neutrality rules](#)

The US D.C. Circuit Court of Appeals will not hear a case brought by broadband trade groups relating to a previous decision to uphold the FCC's net neutrality rules. The court's justification for the decision is the announcement by FCC Chairman Ajit Pai that the agency will seek to repeal its own rules voluntarily.

"A U.S. appeals court has denied a request by broadband trade groups to rehear its decision [last June](#) to uphold the Federal Communications Commission's controversial 2015 net neutrality rules.

The court's decision on Monday is a hollow victory for net neutrality supporters. Just last Wednesday, new FCC Chairman Ajit Pai [announced plans](#) to repeal the rules at the agency, without a court ordering him to do so."

Pan-Asia

Internet governance

23.04.17

South China Morning Post

[China updates internet regulations to tighten control over online news](#)

The Chinese internet regulator has updated its regulations to introduce a requirement for all online news broadcasters to first obtain a government licence. The changes are the first comprehensive revision since 2005 and will come into effect on Thursday 1 June.

“China’s internet regulator has updated its rules on internet and social media news, requiring all online news broadcasters to obtain government licences.

It is the first comprehensive revision of the regulations in 12 years.

It incorporates a collection of piecemeal documents and groups them together to provide a clearer scope of the restrictions.”

Cybersecurity

28.04.17

Times of India

[India ranks 4th in online security breaches](#)

A new study by Symantec has found that India ranks fourth in global online security breaches, accounting for 5% of all detected threats. The survey also finds that India has suffered an increasing number of cyber attacks since 2015.

“As the risk of cyber threats looms over enterprises going digital, a Symantec study reveals that India ranks fourth when it comes to online security breaches, accounting for over 5% of global threat detections. The US and China occupy the top two slots and together make for almost 34%, followed by Brazil and then India.

The year 2016 saw a resurgence of the email as an attack channel, multi-million-dollar virtual bank heists, ransomware and new frontiers like IoT and cloud getting exposed to threats. While China has managed to bring down hacks from nearly 24% in 2015 to under 10% in 2016, India saw instances of fraud increase from 3.4% in 2015 to 5.1% in 2016.”

01.05.17

Reuters

[Trump says China could have hacked Democratic emails](#)

In an interview with CBS show Face the Nation President Donald Trump has alleged that China could have been responsible for the hacking of Democratic officials during last year's Presidential election.

"President Donald Trump said China may have hacked the emails of Democratic officials to meddle with the 2016 presidential election, countering the view of U.S. intelligence officials who have said Moscow orchestrated the hacks.

In an interview transcript published on Sunday, Trump gave no evidence backing his allegation, first made on the eve of the Nov. 8 presidential election, that China could have hacked the emails of his rivals."

Privacy

No new items of relevance

Internet Inclusion

02.05.17

BGR

[India to have 420 million mobile internet users by June 2017: IAMAI](#)

A new report by the Internet and Mobile Association of India (IAMAI) and the research consultancy IMRB has found that India's mobile internet population will have grown to 420 million by June of this year. The study finds that whilst growth in urban centres has reached around 9% compared to last year, the greatest growth in the number of mobile internet users in India is in rural areas has reached 26%.

"Rural India is growing at a much higher rate — around 26 percent — as compared to the urban areas in terms of mobile [internet](#) users, a joint study said. There has been a year-on-year growth of 15 per cent in mobile internet users between October 2015-2016, said the report by the Internet and Mobile Association of India (IAMAI) and IMRB."

Rest of the World

Internet governance

29.04.17

The Independent

[Turkey blocks Wikipedia without court order or explanation](#)

The Turkish government's Information and Communication Technology Authority has blocked access to Wikipedia to all citizens. Normally a restriction of the internet is accompanied with a court order to support the provisional administrative measure, however this has yet to emerge.

"Access to Wikipedia, a free online encyclopedia, has been blocked in Turkey, according to an internet censorship-monitoring network.

Turkey Blocks, which calls itself an independent "digital transparency project" said users in Turkey have been unable to access all language editions of Wikipedia since yesterday morning. "The loss of availability is consistent with internet filters used to censor content in the country," the monitor said."

29.04.17

Daily Nation

[Kenya rejects bid to punish States for internet shutdown](#)

The Kenyan government has rejected a proposal to punish African Governments that shutdown internet access for their citizens. The suggested proposal would have introduced a 12 month ban on the distribution of IP addresses to Governments that shut down their citizens' access to the internet.

"Kenya has rejected a recently published proposal that recommends the disabling of online platforms run by governments as punishment to African states that shut down the internet on their citizens.

The proposal, now with a Mauritius-based agency responsible for assigning Internet Protocol (IP) addresses throughout Africa, suggests that any government which wilfully disrupts internet access should be denied IP addresses for 12 months."

Cybersecurity

27.04.17

Azer News

[Azerbaijan, France mull strengthening cybersecurity](#)

The respective defence ministries of Azerbaijan and France are currently working on strengthening existing cooperation on cybersecurity through a series of meetings currently underway in Baku, Azerbaijan.

“Baku hosts a working meeting of experts on cybersecurity in accordance with the plan of bilateral cooperation for 2017, signed between the Defense Ministries of Azerbaijan and France.

The experts noted the importance of strengthening cybersecurity measures in the nation's critical infrastructure, such as government, communications and financial services, transport as well as in other areas, the Azerbaijani Defense Ministry reported on April 27.”

Privacy

No new items of relevance

Internet Inclusion

03.05.17

India Blooms

[World Economic Forum, South African Government launch push to Bridge Digital Divide](#)

The World Economic Forum has announced a new collaboration with the Government of South Africa to increase internet access in the country as part of an Internet for All project.

“The World Economic Forum, in partnership with the Government of South Africa, will this week announce the launch of a new platform project called South Africa Internet for All, which aims to bring millions of South Africans, including those in rural areas, onto the internet for the first time through new models of public-private collaboration. Currently, according to the International Telecommunications Union, 52% of South Africans use the internet.

The project, which is aligned to the Government's National Development and South Africa Connect plans, will address the barriers that prevent universal



internet access: infrastructure connectivity, affordability, skills and awareness, and relevant content; and also explore how Internet for All can better support the development of e-government services and SMEs.”

Global Institutions

29.04.17

EIF

Digital skills of tomorrow

The European Internet Forum has hosted a debate with two MEPs to discuss the importance of digital skills for participation in modern society.

“On 29 March, EIF and MEPs Brando Benifei and Victor Negrescu hosted a debate to discuss the growing need for digital skills to participate in modern society.

In his opening remarks, MEP Brando Benifei stressed the importance of basic digital skills to participate in modern society. Investing resources in education and training will be key to creating a more innovative and cohesive society where no one is left behind.”

01.05.17

ITU

ITU Telecom World 2017 takes a look into our smart future

The 2017 ITU Telecom World conference in September will focus on the theme of smart digital transformation. The conference will include attendees from small and medium enterprises and initiatives particularly from emerging markets in Africa and Asia.

“Leading names from government and industry from across the world of digital technology will convene for the International Telecommunication Union (ITU) [Telecom World 2017](#) from 25-28 September in Busan, Republic of Korea, itself one of the most technologically advanced nations on earth and top of [ITU's ICT development index in 2016](#). Together they will debate, showcase, network and more under the theme of smart digital transformation, global opportunity.

As the global tech event for corporates, governments and small- and medium-sized enterprises (SMEs), ITU Telecom World 2017 comprises an [exhibition](#) for digital solutions, [forum](#) for debate and sharing knowledge, a [networking](#) hub connecting nations, individuals and organizations, and an [awards](#) programme recognizing innovative information and communications technology (ICT) solutions with social impact.”

02.05.17

ICANN

[Date Change for ICANN62 in June 2018 to be held in Panama](#)

ICANN have announced that the date for the June 2018 public meeting in Panama has been changed in order to respect the Muslim Holiday celebration of Eid al-Fitr.

“The ICANN Board has approved Panama as the location in Latin America to host ICANN’s 62nd public meeting. Previously scheduled for the week of 18 June, this Policy Forum has been moved to 25-28 June to respect the Muslim Eid al-Fitr holiday celebration.”

02.05.17

Digital Europe

[DIGITALEUROPE speaks at Bruegel ePrivacy event](#)

Representatives of Digital Europe have attended a Bruegel sponsored event on ePrivacy in which Senior Policy Manager Alexander Whalen highlighted potential limitations in the EU’s ePrivacy Directive. Mr Whalen also drew attention to the focus of debate on cookies and the need to extend discussion to additional topics such as virtual personal assistants, translation services and text-to-speech.

“On 25 April, DIGITALEUROPE spoke at the “Protecting the Privacy of Electronic Communications: Getting the Next Steps Right” event in Brussels, Belgium. The event, organised by Bruegel, aimed to examine whether the draft ePrivacy Regulation strikes the right balance between protecting the fundamental rights of citizens and allowing industry to innovate.”

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