



10 May 2017

Synopsis

Scroll to read full summaries with links to news articles.

Bulgaria have nominated one of the country's MEP's to become the country's new **European Commission** member after the role was vacated in January. **Mariya Gabriel** will likely adopt the same brief as her predecessor and become the EU's Commission on Digital issues, in which she will support Commission Vice President Andrus Ansip in the creation of the **EU Digital Single Market**.

The **European Data Protection Supervisor** has issued its 2016 report in which it sets out the three priorities for the Supervisor's remaining tenure. Amongst the priorities is the recommendation that greater legislative efforts be conducted to improve cross border management of **data protection**.

The **United States National Institute of Standards and Technology** appears set to recommend that password protections be augmented with additional **authentication** methods rather than with more complex passwords in response to the growing complexity of **cyber attacks** which have moved away from brute force attacks.

Ajit Pai the Chairman of the **FCC** has laid out his plans to expand **broadband internet access** across the **USA**, particularly focusing on more rural areas.

The **Securities and Futures Commission** of **Hong Kong** will look to gain market wide consent from the city's financial sector regarding an array of **cybersecurity** proposals designed to tackle the types of **cyberattacks** that have recently plagued Hong Kong's financial services.

A new **Global Digital Transformation Skills Study** by **Brocade** has found that although 91% of global IT leaders believe business growth and innovation is tied to company IT departments, over half believe that companies will struggle to find enough IT talent to react to changing technologies in a positive manner.

The information technology services company **Dimension Data** has found that **cyber attacks** on national government have doubled in the past year with **IoT** devices becoming a greater source and target of cyberattacks.

Experts from across **Canada's** digital sphere have warned that the country's businesses are not prepared for the introduction of the EU's General Data Protection Regulation (**GDPR**) set to be introduced next year.

The **UN's Human Rights Council** has announced that it will review existing **surveillance laws** in **South Africa**, after a consortium of concerned parties raised the lack of privacy protections in the country to the UN.

The **European Commission** has outlined the next steps it will take in the development of the EU's **digital single market**, with the Commission calling on national legislators to adopt the proposals it has previously produced.

IEEE Global Internet Policy Monitor

10 May 2017

Table of Contents

Synopsis	1
Europe	4
Internet governance.....	4
Cybersecurity.....	5
Privacy.....	6
Internet Inclusion.....	7
United States of America	7
Internet governance.....	8
Cybersecurity.....	8
Privacy.....	8
Internet Inclusion.....	10
Pan-Asia	12
Internet governance.....	12
Cybersecurity.....	12
Privacy.....	13
Internet Inclusion.....	13
Rest of the World.....	15
Internet governance.....	15
Cybersecurity.....	15
Privacy.....	15
Internet Inclusion.....	17
Global Institutions.....	19
Diary Dates.....	20

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

Europe

Internet governance

09.05.17

Politico

[Bulgaria to nominate MEP Mariya Gabriel as commissioner](#)

Bulgaria have nominated one of the country's MEP's to become the country's new European Commission member after the role was vacated in January. Mariya Gabriel will likely adopt the same brief as her predecessor and become the EU's Commission on Digital issues, in which she will support Commission Vice President Andrus Ansip in the creation of the EU Digital Single Market.

"Bulgaria is poised to nominate MEP Mariya Gabriel to replace Kristalina Georgieva on the European Commission.

The online edition of Dnevnik [reported the coming nomination Tuesday](#) and a government source confirmed the planned nomination to POLITICO.

Gabriel would say only that there have been no talks with her regarding such a nomination."

10.05.17

Computing

[EU plans more regulation for internet giants](#)

The European Commission has suggested that it will consider further regulation designed to prevent internet giants from mistreating small businesses as part of a current review of the digital single market project.

"The European Union is planning new rules for internet giants operating in the EU that would bar them from offering poorer terms to small businesses that use their platforms to promote their products and services.

The ideas have been put forward as the European Commission goes into its mid-term review of the ongoing Digital Single Market project, the EU's effort to streamline the pan-European marketplace across its 28 members, supposedly to facilitate cross-border online trade."

Cybersecurity

09.05.17

Ars Technica

[Russia behind hack of new French president Macron, evidence suggests](#)

Metadata from leaked documents originally from the computers of French President Elect Emmanuel Macron's campaign appear to implicate a Russian company called Evrika ZAO, a systems integrator with acknowledged ties to Russian intelligence service the FSB.

"Late on May 5 as the two final candidates for the French presidency were about to enter a press blackout in advance of the May 7 election, nine gigabytes of data allegedly from the campaign of Emmanuel Macron were posted on the Internet in torrents and archives. The files, which were initially distributed via links posted on 4Chan and then by WikiLeaks, had forensic metadata suggesting that Russians were behind the breach—and that a Russian government contract employee may have falsified some of the dumped documents.

Even WikiLeaks, which initially publicized the breach and defended its integrity on the organization's Twitter account, has since acknowledged that some of the metadata pointed directly to a Russian company with ties to the government"

10.05.17

Cybersecurity NZ

[Cyber attacks on govt double; IoT becomes threat and source of attack](#)

The information technology services company Dimension Data has found that cyber attacks on national government have doubled in the past year with IoT devices becoming a greater source and target of cyberattacks.

"Cyber attacks on the government sector doubled last year, pushing it into a first place tie with the finance sector for most targeted market according to new research which also highlights the threat of IoT.

Dimension Data says cyber attacks on government agencies accounted for 14% of all cybersecurity attacks in 2016, up from 7% a year earlier, with the finance sector also seeing a dramatic increase, from 3% in 2015 to 14% in 2016."

Privacy

05.05.17

New Europe

[Europe's Data Protection Supervisor issues 2016 annual report](#)

The European Data Protection Supervisor has issued its 2016 report in which it sets out the three priorities for the Supervisor's remaining tenure. Amongst the priorities is the recommendation that greater legislative efforts be conducted to improve cross border management of data protection.

"Europe's Data Protection Supervisor (EDPS) presented on May 4 its annual report on May 4. The document outlines three main goals for the second half of its remaining current mandate.

The European Data Protection Supervisor Giovanni Buttarelli, underlined that the remaining half of his five-year mandate will focus on solidifying the data protection strategy within the EU institutions and bodies.

"Data protection and privacy continue being on the top of the political agenda," said Buttarelli, as 121 countries are now on horizontal data protection and privacy legislation."

05.05.17

IT World Canada

[Experts worry Canadian firms won't be ready for new European privacy rule](#)

Experts from across Canada's digital sphere have warned that the country's businesses are not prepared for the introduction of the EU's General Data Protection Regulation (GDPR) set to be introduced next year.

"The deadline for enterprises to comply with the European Union's tough new personal data privacy regulations is just over 12 months away, but experts still worry many companies here that fall under its umbrella will be penalized because they won't be prepared in time.

"A lot of folks in North America haven't realized the impact it will potentially have," says John Proctor, vice-president of the global cyber security practice at Montreal-based solutions provider CGI."

05.05.17

Politico

UK intelligence asks for 'real time' data from telecoms

The British government is considering implementing rules to ensure espionage services like GCHQ (the UK equivalent of the NSA) and other agencies can have real time access to telecom company data, including electronic communications.

"A [draft proposal](#) of the British government shows the U.K. security services would be granted the power to surveil citizens in "near real time."

The paper, [leaked](#) to digital activists at Open Rights Group but not confirmed by the U.K. Home Office, explains how telecoms and postal services would have to assist security services in intercepting electronic communications.

The paper also mentions that telecoms companies should provide data "in an intelligible form" without "electronic protection," which would undermine encryption technologies used to protect user data, including personal data, that is gathered and stored by these companies."

Internet Inclusion

08.05.17

Networks Asia

More than half of IT teams will struggle due to a lack of the 'right' skills

A new Global Digital Transformation Skills Study by Brocade has found that although 91% of global IT leaders believe business growth and innovation is tied to company IT departments, over half believe that companies will struggle to find enough IT talent to react to changing technologies in a positive manner.

"An encouraging 91 percent of global IT leaders acknowledge that IT departments are currently recognized as very important or critical to innovation and business growth, according to a new [Global Digital Transformation Skills Study](#) released by Brocade.

However, over half (54 percent) predict they will struggle with a lack of IT talent in 12 months. Contributing factors identified from the research include skills shortages, prevalence of outdated skills, lack of commitment to training at the corporate board level, and the rapidly changing technology environment."

United States of America

Internet governance

No new items of relevance

Cybersecurity

03.05.17

SC Magazine

[FBI: Many companies ignore cybercrime warnings from government](#)

A former director of the FBI's National Cyber Investigative Joint Task Force has stated that over a third of companies notified of digital threats to their networks and personnel ignore the warnings.

"Over a third of companies officially notified by U.S. federal authorities that their networks and personnel are being targeted by nation-state hackers or cybercriminal groups fail to act on this intelligence, according to Donald Freese, former director of the FBI's National Cyber Investigative Joint Task Force, now with the agency's Information Technology Branch.

Too often after issuing companies an official "targeted identity notification," warning them that their systems are being targeted, "we will approximately 72 hours to a week later see malware now beaconing from that same system," said Freese, speaking today at SC Media's RiskSec NY 2017 conference."

05.05.17

Info World

[NIST to security admins: You've made passwords too hard](#)

The United States National Institute of Standards and Technology appears set to recommend that password protections be augmented with additional authentication methods rather than with more complex passwords in response to the growing complexity of cyber attacks which have moved away from brute force attacks.

"Despite the fact that cybercriminals stole more than [3 billion user credentials in 2016](#), users don't seem to be getting savvier about their password usage. The good news is that how we think about password security is changing as other authentication methods become more popular.

Password security remains a Hydra-esque challenge for enterprises. Require users to change their passwords frequently, and they wind up selecting easy-to-remember passwords. Force users to use numbers and special characters to select a strong password and they come back with passwords like [Pa\\$\\$w0rd](#).”

08.05.17

Reuters

[FCC website hit by attacks after 'net neutrality' proposal](#)

The Federal Communications Commission has stated that the regulators website was affected by a DDOS attack following criticism of planned proposals to repeal net neutrality regulations by HBO “Last Week Tonight” host John Oliver.

“The U.S. Federal Communications Commission said Monday that its website was hit by deliberate denial of service attacks after the telecommunications regulator was criticized by comedian John Oliver for its plan to reverse “net neutrality” rules.

The attacks came soon after Oliver on Sunday urged viewers to file electronic comments with the FCC opposing the plan unveiled by FCC Chairman Ajit Pai to reverse rules implemented under President Barack Obama that boosted government regulatory powers over internet service providers.”

10.05.17

Ars Technica

[US military needs cyberwarriors so badly it may let skilled bods skip boot camp](#)

The US Military’s commander of CYBERCOM has acknowledged that the armed services face a shortage of skilled personnel. Various branches of the military have announced that they may forgo traditional boot camps for new recruits in order to quickly bring in new cyber focused troops.

“The US military is having a hard time getting people with essential information technology and information security skill sets as the services struggle to build a force of “cyber-warriors.” During a [Senate Armed Services Committee hearing today](#), senators focused in part on how the work force problem is affecting the US Cyber Command’s (US CYBERCOM’s) ability to deal with the demands of information warfare and threats both to the Defense Department’s networks and those of other agencies and industry.

Admiral Michael Rogers, appearing in his capacity as commander of US CYBERCOM (a role he holds as well as that of director of the National Security Agency), told the committee that he was confident that CYBERCOM would meet

a 2018 deadline for the command to reach full operational capability. But he acknowledged that there was still a shortage of service members throughout the military required to sustain CYBERCOM long-term.”

10.05.17

Cybersecurity NZ

Cyber attacks on govt double; IoT becomes threat and source of attack

The information technology services company Dimension Data has found that cyber attacks on national government have doubled in the past year with IoT devices becoming a greater source and target of cyberattacks.

“Cyber attacks on the government sector doubled last year, pushing it into a first place tie with the finance sector for most targeted market according to new research which also highlights the threat of IoT.

Dimension Data says cyber attacks on government agencies accounted for 14% of all cybersecurity attacks in 2016, up from 7% a year earlier, with the finance sector also seeing a dramatic increase, from 3% in 2015 to 14% in 2016.”

Privacy

No new items of relevance

Internet Inclusion

08.06.17

Yahoo

Trump's FCC chief looks to expand broadband internet access

Ajit Pai the Chairman of the FCC has laid out his plans to expand broadband internet access across the USA, particularly focusing on more rural areas.

“Federal Communications Commission chairman Ajit Pai sounded like a different person while speaking [at the American Enterprise Institute](#) on Friday from the one who delivered [a blistering attack on open internet regulations at the Newseum](#) just two weeks ago.

Pai, who glossed over [his plan to scrap rules banning internet providers from discriminating against or in favor of legal sites](#), never mentioned his opposition

to [now-dead privacy regulations](#) that would have barred ISPs from selling your browsing history to advertisers without your permission.”

08.05.17

Networks Asia

[More than half of IT teams will struggle due to a lack of the 'right' skills](#)

A new Global Digital Transformation Skills Study by Brocade has found that although 91% of global IT leaders believe business growth and innovation is tied to company IT departments, over half believe that companies will struggle to find enough IT talent to react to changing technologies in a positive manner.

“An encouraging 91 percent of global IT leaders acknowledge that IT departments are currently recognized as very important or critical to innovation and business growth, according to a new [Global Digital Transformation Skills Study](#) released by Brocade.

However, over half (54 percent) predict they will struggle with a lack of IT talent in 12 months. Contributing factors identified from the research include skills shortages, prevalence of outdated skills, lack of commitment to training at the corporate board level, and the rapidly changing technology environment.”

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

04.05.17

MIS Asia

[CSA hosts Cybersecurity Challenge to increase Singapore's cybersecurity talent pool](#)

Singapore's Cyber Security Agency (CSA) has announced a new cybersecurity competition to foster the country's cybersecurity talents. The competition will use Cyber Security Challenge UK's CyPhinx a virtual reality skyscraper used to host cybersecurity games.

"To spur more talents to join the cybersecurity field, the Cyber Security Agency of Singapore (CSA) will be organising the Cybersecurity Challenge Singapore.

One component of the challenge is CyPhinx, a virtual three-dimensional skyscraper that is developed by Cyber Security Challenge UK, a UK Government-backed organisation, in 2015.

CyPhinx allows players to create avatars, access cybersecurity game challenges, interact with like-minded cyber enthusiasts, as well as demonstrate their skills to fellow players and potential employers."

08.05.17

South China Morning Post

[Hong Kong regulator SFC seeks input on tighter cybersecurity measures](#)

Hong Kong's Securities and Futures Commission will look to gain market wide consent from the city's financial sector regarding an array of cybersecurity proposals designed to tackle the types of cyberattacks that have recently plagued Hong Kong's financial services.

"The Securities and Futures Commission has proposed a range of measures to tighten cybersecurity for all of the 500 Hong Kong stockbrokers and fund

managers in the city, according to a consultation paper that seeks to collect views from the market over the next two months.

The regulator's action came after 27 hacking attacks on 12 licensed financial firms in the 18 months to the end of March led to investor losses totalling HK\$110 million (US\$14.2 million), the commission said in a statement on Monday."

10.05.17

Cybersecurity NZ

Cyber attacks on govt double; IoT becomes threat and source of attack

The information technology services company Dimension Data has found that cyber attacks on national government have doubled in the past year with IoT devices becoming a greater source and target of cyberattacks.

"Cyber attacks on the government sector doubled last year, pushing it into a first place tie with the finance sector for most targeted market according to new research which also highlights the threat of IoT.

Dimension Data says cyber attacks on government agencies accounted for 14% of all cybersecurity attacks in 2016, up from 7% a year earlier, with the finance sector also seeing a dramatic increase, from 3% in 2015 to 14% in 2016."

Privacy

No new items of relevance

Internet Inclusion

08.05.17

Networks Asia

More than half of IT teams will struggle due to a lack of the 'right' skills

A new Global Digital Transformation Skills Study by Brocade has found that although 91% of global IT leaders believe business growth and innovation is tied to company IT departments, over half believe that companies will struggle to find enough IT talent to react to changing technologies in a positive manner.

"An encouraging 91 percent of global IT leaders acknowledge that IT departments are currently recognized as very important or critical to innovation

and business growth, according to a new [Global Digital Transformation Skills Study](#) released by Brocade.

However, over half (54 percent) predict they will struggle with a lack of IT talent in 12 months. Contributing factors identified from the research include skills shortages, prevalence of outdated skills, lack of commitment to training at the corporate board level, and the rapidly changing technology environment.”

Rest of the World

Internet governance

04.05.17

IT Web Africa

[Zambia to force ISPs to help with cybercrime](#)

The Zambian government will introduce legislation to tackle cybercrime and other digital security threats. Amongst the proposed bills is a new requirement for ISPs to support the Government's actions in investigating and preventing cybercrime.

"Zambia's government has tabled several Bills it says are aimed at curbing cybercrime and strengthening digital security within the telecom sector. However, a source within the Ministry of Communications and Transport has said the data protection Bill will be used to force ISPs to help authorities."

The Bills cover cybercrime, data protection, e-transmissions and eGovernment and according to Minister of Communications and Transport Brian Mushimba said the pending legislation is aimed at improving security and making the sector more attractive for investment."

Cybersecurity

10.05.17

IT Web Africa

[Hackers invited to disrupt Botswana's electronic voting machines](#)

The Independent Electoral Commission of Botswana has invited hackers to test the country's proposed electronic voting machine before it is introduced for the 2019 election.

"Independent Electoral Commission (IEC) officials have invited hackers to prove whether or not the country's proposed electronic voting machine (EVM) system can be manipulated."

The new voting system is expected to be used for the country's next general election in 2019."

10.05.17

Cybersecurity NZ

[Cyber attacks on govt double; IoT becomes threat and source of attack](#)

The information technology services company Dimension Data has found that cyber attacks on national government have doubled in the past year with IoT devices becoming a greater source and target of cyberattacks.

“Cyber attacks on the government sector doubled last year, pushing it into a first place tie with the finance sector for most targeted market according to new research which also highlights the threat of IoT.”

Dimension Data says cyber attacks on government agencies accounted for 14% of all cybersecurity attacks in 2016, up from 7% a year earlier, with the finance sector also seeing a dramatic increase, from 3% in 2015 to 14% in 2016.”

Privacy

05.05.17

IT World Canada

[Experts worry Canadian firms won't be ready for new European privacy rule](#)

Experts from across Canada's digital sphere have warned that the country's businesses are not prepared for the introduction of the EU's General Data Protection Regulation (GDPR) set to be introduced next year.

“The deadline for enterprises to comply with the European Union's tough new personal data privacy regulations is just over 12 months away, but experts still worry many companies here that fall under its umbrella will be penalized because they won't be prepared in time.”

“A lot of folks in North America haven't realized the impact it will potentially have,” says John Proctor, vice-president of the global cyber security practice at Montreal-based solutions provider CGI.”

08.05.17

IT Web Africa

Kenyan patient records vulnerable to breaches

An audit of Kenya's digital security by Privacy International has raised concerns for medical records in the country, specifically highlighting the absence of digital privacy laws in the country.

"Absence of laws to govern the management of digital medical records encourages service providers to innovate."

"There is no law that prescribes how to digitally handle patient data and this leaves patients vulnerable to a potential breach of privacy, according to Nicky Nyamasyo, Head of IT at e-health company ION Kenya."

10.05.17

Business Tech (South Africa)

SA's spying laws are being reviewed by the UN Human Rights Council

The UN's Human Rights Council has announced that it will review existing surveillance laws in South Africa, after a consortium of concerned parties raised the lack of privacy protections in the country to the UN.

"The United Nations Human Rights Council will on Wednesday review South Africa's current surveillance policies, following a formal submission by Right 2 Know (R2K), Privacy International and the Media Policy and Democracy Project (MPDP)."

"The consortium have raised concerns over state spying and lack of privacy protections in South Africa."

Internet Inclusion

08.05.17

Networks Asia

More than half of IT teams will struggle due to a lack of the 'right' skills

A new Global Digital Transformation Skills Study by Brocade has found that although 91% of global IT leaders believe business growth and innovation is tied to company IT departments, over half believe that companies will struggle to find enough IT talent to react to changing technologies in a positive manner.

“An encouraging 91 percent of global IT leaders acknowledge that IT departments are currently recognized as very important or critical to innovation and business growth, according to a new [Global Digital Transformation Skills Study](#) released by Brocade.

However, over half (54 percent) predict they will struggle with a lack of IT talent in 12 months. Contributing factors identified from the research include skills shortages, prevalence of outdated skills, lack of commitment to training at the corporate board level, and the rapidly changing technology environment.”

Global Institutions

04.05.17

ICANN

[Independent Examiner Issues Final Report on Review of the At-Large Organization](#)

ICANN has announced that the Independent Examiner ITEMS International has now published the final report relating to the review of the ICANN at-large organization. The report is largely positive but includes a call for reforms to the at-large community to ensure that end-user interests are better recognised in policy advice.

“After extensive consultation with the At-Large and the broader ICANN community, including a formal [public comment process](#), and ongoing engagement and participation of the [At-Large Review Working Party](#), ITEMS International, the independent examiner for the review of the At-Large organization, has issued its [final report](#) [PDF, 4.08 MB]. This marks an important milestone in ICANN's commitment to continuous improvement, accountability and transparency.”

10.05.17

European Commission

[Digital Single Market: Commission calls for swift adoption of key proposals and maps out challenges ahead](#)

The European Commission has outlined the next steps it will take in the development of the EU's digital single market, with the Commission calling on national legislators to adopt the proposals it has previously produced.

“It takes stock of the progress made, calls on co-legislators to swiftly act on all proposals already presented, and outlines further actions on online platforms, data economy and cybersecurity.

Since May 2015, the European Commission has delivered 35 legislative proposals and policy initiatives as announced in its [Digital Single Market strategy](#). The focus is now on obtaining [political agreement](#) with the European Parliament and the Council on all proposals, above all the [updated EU telecoms rules](#) which will boost investments in high-speed and quality networks, which are critical for the full deployment of the digital economy and society.”

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

[2017 European Security Conference](#) – 05.06.17-06.06.17

Lisbon, Portugal

[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

[China Cyber Security Conference & Exposition 2017](#) – 13.06.17

Beijing, China

[ICANN 59](#) – 26.06.17-29.06.17

Johannesburg, South Africa

[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

[ICANN 60](#) – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

[IGF 2017](#) – 18.12.17 – 21.10.17

Geneva, Switzerland