



8 March 2017

Synopsis

Scroll to read full summaries with links to news articles.

EU Commissioner **Vera Jourova** has this month stated that if the **Trump** administration puts the EU-US **privacy shield** in jeopardy the EU will put an end to the agreement.

In the **UK**, **Facebook** and **BT** have announced plans for a joint technology hub to develop next generation technology and to improve **internet access**.

Following concerns for potential **Russian** interference in their upcoming legislative elections, the **French** government has dropped **electronic voting** for overseas voters. The changes were implemented following a report from the **National Cybersecurity Agency** who highlighted the “extremely high risk” of **cyber attacks** on election systems.

In the **United States**, President Trump’s administration has begun to review the delayed **cybersecurity** executive order. The order was originally meant to be signed in the first weeks of the Trump Presidency, but has now passed to industry experts for their input ahead of an imminently expected publication.

The head lawyer for the **National Security Agency** has called for a single agency to oversee **cybersecurity** for the **USA**. Mr **Glenn Gerstell** also suggested that a single body could be mirrored on the **UK’s National Cyber Security Centre**.

Elsewhere the **US** government has asked that the **Irish High Court** refuse the referral of the **Facebook data privacy** case to the **EU Court of Justice**. The Government’s argument is that the Irish Data Protection Commissioner’s proposal would undermine the future of **US-EU data sharing**.

China has this week published its first **cyberpolicy** paper, which outlines the country’s position on a range of domestic and international **cyber issues**. In the paper the Chinese Government specifically calls for greater cooperation in **internet governance**, though with national sovereignty retained by individual countries.

Singapore has announced this week that a new **Defence Cyber Organisation** will be established to better defend the country's armed forces network. The Government was prompted to establish the new body following a breach of personal details of both civilian and military officials within the Ministry of Defence.

A new report by the **Facebook**-Economist Intelligence Unit has found that **India** ranks 36th out of 75 nations for **internet inclusiveness**. The report ranked countries based on affordability, availability and access policies. The top 5 countries were **Singapore, Sweden, USA, UK** and **Japan**.

Nigeria has this week launched a stakeholder consultation as part of its policy to establish greater **net neutrality** and openness in the country's internet.

Joe Cannataci the **UN's** independent expert on **digital privacy** has submitted a report to the UN's **Human Rights Council**, in which he calls for the creation of an internationally recognised treaty on **cyber surveillance**, that would create universal protections for personal privacy.

Digital Europe have published a new position paper on the **EU's** proposed **Electronic Communications Code**. The paper largely agrees with the EU's plans, though states that consideration has to be paid to the development of technology in the future.

ICANN's system controls of **IANA's** registry management systems and the Domain Name System Security Extensions have been audited by **PricewaterhouseCoopers**, who have validated ICANN's existing protocols.

IEEE Global Internet Policy Monitor

8 March 2017

Table of Contents

Synopsis	1
Europe	4
Internet governance	4
Cybersecurity	4
Privacy	5
Internet Inclusion	7
United States of America	8
Internet governance	8
Cybersecurity	8
Privacy	8
Internet Inclusion	11
Pan-Asia	13
Internet governance	13
Cybersecurity	13
Privacy	14
Internet Inclusion	16
Rest of the World	18
Internet governance	18
Cybersecurity	18
Privacy	18
Internet Inclusion	19
Global Institutions	21
Diary Dates	23

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

06.03.17

The Hill

[British defense officials call for more cooperation between NATO, EU on cyber](#)

The UK's Defence Minister and leading Defence Civil Servant Stephen Lovegrove have both called for greater cybersecurity cooperation between NATO and the EU. Speaking at the Atlantic Council in Washington D.C. Mr Lovegrove warned NATO members not to become complacent on their security.

“Officials with Britain’s Defense Ministry on Monday called for greater cooperation on cybersecurity between NATO and the European Union.

The demands come in the wake of Britain’s vote to leave the EU, which British Defense Secretary Michael Fallon indicated Monday would not affect Britain’s security cooperation with other European nations.

Fallon and Stephen Lovegrove, the Defense Ministry’s permanent secretary, both said in separate remarks on Monday that NATO and EU should strengthen cooperation on cybersecurity.”

06.03.17

Telangana Today

[India, Portugal to collaborate in electronic manufacturing, cyber security](#)

India and Portugal have agreed to a new collaboration on electronic and digital issues. The partnerships will focus on the manufacturing of electronics, as well as collaboration on cybersecurity and e-governance.

“[India](#) and [Portugal](#) on Monday agreed to set up an institutional mechanism to collaborate in areas of electronic manufacturing, ITeS, start-ups, cyber security and e-governance, an official said.

“We had a very good discussion and have agreed to collaborate in the areas of electronic manufacturing, ITeS, cyber security, e-governance and capacity building. We will support the Portugal team in scaling up their initiatives — Simplex and Portuguese Citizen Shops, which are like our MyGov and Common Service Centre initiatives,” [IT Minister Ravi Shankar Prasad](#) said.”

06.03.17

Reuters

[France drops electronic voting for citizens abroad over cybersecurity fears](#)

Following concerns for potential Russian interference in their upcoming legislative elections, the French government has dropped electronic voting for citizens overseas. The changes were implemented following a report from the National Cybersecurity Agency who'd highlighted the “extremely high risk” of cyber attacks on election mechanisms.

“France's government has dropped plans to let its citizens abroad vote electronically in legislative elections in June because of concern about the risk of cyber attacks, the Foreign Ministry said on Monday.

The National Cybersecurity Agency believed there was an "extremely high risk" of cyber attacks. "In that light, it was decided that it would be better to take no risk that might jeopardize the legislative vote for French citizens residing abroad," the ministry said in a statement.

Concern about foreign interference in western elections has surged amid allegations of Russian hacking - which Moscow denies - in the U.S. presidential ballot.”

[Privacy](#)

02.03.17

Bloomberg

[If Trump Spoils Privacy Pact, We'll Pull It, EU Official Warns](#)

EU Commissioner Vera Jourova has this month stated that if the Trump administration puts the EU-US privacy shield in jeopardy the EU will put an end to the agreement. The move came after recent concerns emerged for the security of EU citizen data, following a change in US policy as a result of an Executive Order.

“Vera Jourova spent months working with the Obama administration on a deal to protect Europeans from digital surveillance by U.S. spies. With a new occupant

now in the White House, the EU's privacy czar says she's prepared to rip up the pact if the Americans don't adhere to its terms.

"If there is a significant change, we will suspend" the accord, Jourova, the European Union's justice commissioner, said in a Bloomberg interview. "I will not hesitate to do it. There's too much at stake."

02.03.17

Irish Times

[US government asks High Court to refuse Facebook case referral](#)

Lawyers for the US government have called on the Irish High Court to reject a motion to move the data privacy case against Facebook to the EU's Court of Justice. The motion was filed by the Irish Data Protection Commissioner, but US lawyers have criticized her decision suggesting it places EU-US data cooperation in jeopardy.

"The US government has urged the [High Court](#) to refuse the Data Protection Commissioner's bid to have the Court of Justice of the EU (CJEU) decide issues with potentially enormous consequences for EU-US data transfers.

Eileen Barrington SC, for the US, said the commissioner's "unique", "unusual" and "unprecedented" application for a reference to the CJEU was based on the commissioner's "fatally flawed" draft finding concerning adequacy of remedies available in the US for breach of data privacy rights of EU citizens.

This application was of "critical significance" to the US for legal and commercial reasons and should be dismissed for reasons including that it had been "entirely overtaken by events", particularly the 2016 agreement between the [European Commission](#) and US on the Privacy Shield framework for EU-US data transfers."

08.03.17

Channel News Asia

[UN expert urges states to work towards cyber surveillance treaty](#)

The UN's privacy expert Joe Cannataci has produced a report calling for an international agreement on cyber surveillance, claiming that current standards are outdated in the digital age. The report also calls for the creation of an international warrant for data access, to reduce reliance on US legal safeguards and practices.

"The world needs an international treaty to protect people's privacy from unfettered cybersurveillance, which is being pushed by populist politicians preying on fear of terrorism, according to a U.N. report debated on Wednesday.

The report, submitted to the U.N. Human Rights Council by the U.N. independent expert on privacy, Joe Cannataci, said traditional privacy safeguards such as rules on phone tapping were outdated in the digital age.

"It's time to start reclaiming cyberspace from the menace of over-surveillance," Cannataci told the Council."

Internet Inclusion

08.03.17

The Telegraph

Facebook and BT open 'acceleration centres' to improve internet access

Facebook and UK telecoms company BT have agreed to open a UK hub for next generation technology. The plans will also fit into Facebook's aim of expanding internet access worldwide. The centres in London and Ipswich will use technology developed by UK startups to apply solutions to existing networks.

"Facebook and BT have announced plans to open a UK hub for developing next-generation telecoms technology, part of the social media giant's efforts to expand global internet access.

The "ecosystem acceleration centres" will host start-ups backed by a \$170m (£135m) London investment fund announced by Facebook's Telecom Infra Project (TIP).

Facebook, which needs to expand internet access to the developing world to continue its rapid growth, leads the TIP consortium of telecoms groups, hoping to shake up mobile networks by building equipment that can boost speeds and coverage."

United States of America

Internet governance

06.03.17

Nextgov

[Trump team is floating cyber Executive Order to industry](#)

President Trump's administration has begun to review the delayed cybersecurity executive order. The order was originally meant to be signed in the first weeks of the Trump Presidency, but has now passed to industry experts for their input ahead of an imminently expected publication.

"Industry officials are reviewing a long-delayed Trump administration cybersecurity executive order, one official said Monday, a sign the order may be released soon.

President Donald Trump was scheduled to sign the order more than a month ago, but abruptly canceled the signing without explanation.

A [revised draft of the order](#) leaked several days later, but the administration has been tight-lipped about how the order has been updated since early February or when it might be released."

Cybersecurity

02.03.17

The Hill

[Lawmakers unveil bill to help state, local governments with cybersecurity](#)

A bill to bolster the cyber protections of State and Local Governments has been reintroduced to the Senate by a bipartisan alliance. The bill comes at a time of heightened anxiety for cybersecurity in the US and would require the Department of Homeland Security's National Cybersecurity and Communications Integration Center to provide assistance and training to governments below the federal level.

"A bipartisan pair of senators has introduced a bill that would require the federal government to do more to help state and local officials combat cyber threats.

Sens. Gary Peters (D-Mich.) and David Perdue (R-Ga.) on Thursday announced that they have reintroduced the State and Local Cyber Protection Act, which

would bolster cybersecurity cooperation between the Department of Homeland Security and state and local governments.”

03.03.17

The Hill

[NSA lawyer advocates for one agency to handle cyber](#)

Glenn Gerstell the National Security Agency’s leading lawyer has suggested in a recent speech that the government consolidate its cybersecurity efforts into a single agency. Mr Gerstell also suggested that the agency be modelled on the UK’s National Cyber Security Centre.

“The National Security Agency’s (NSA) lead lawyer in a recent speech made the case for creating one federal agency to spearhead the government’s cybersecurity efforts.

Glenn Gerstell, the NSA’s general counsel, proposed that federal cybersecurity activities be unified under one roof instead of dispersed across the departments of Defense, Homeland Security and other agencies during [remarks](#) at Duke Law School over the weekend that were released by the NSA on Thursday.

While Gerstell acknowledged progress made on cybersecurity by the George W. Bush and Obama administrations, he said that “glaring gaps remain in our nation’s cybersecurity posture.”

05.03.17

Times of India

[India, US set to bolster security ties, focus on cyber, maritime security](#)

The US and Indian Governments have announced further cooperation on security issues. The bilateral alliance will further strengthen training and exchange programs covering issues from cybersecurity to hostage negotiation.

“India and the US are set to further strengthen their bilateral security ties under the [Trump](#) administration with the two countries deciding to continue exchange programmes on hostage crisis, terror crime scene probe and cybercrime.

A delegation of officials from the US met their counterparts in the home ministry last week and discussed ways to streamline the training programmes being conducted under the [Anti-Terrorism Assistance](#) (ATA) pact.

Indian police officers will undergo training programmes in the US training institutes on negotiations in hostage situations, terror crime scene investigations, besides on two new courses relating to cyber crime and maritime security.”

06.03.17

The Hill

[British defense officials call for more cooperation between NATO, EU on cyber](#)

The UK's Defence Minister and leading Defence Civil Servant Stephen Lovegrove have both called for greater cybersecurity cooperation between NATO and the EU. Speaking at the Atlantic Council in Washington D.C. Mr Lovegrove warned NATO members not to become complacent on their security.

"Officials with Britain's Defense Ministry on Monday called for greater cooperation on cybersecurity between NATO and the European Union.

The demands come in the wake of Britain's vote to leave the EU, which British Defense Secretary Michael Fallon indicated Monday would not affect Britain's security cooperation with other European nations.

Fallon and Stephen Lovegrove, the Defense Ministry's permanent secretary, both said in separate remarks on Monday that NATO and EU should strengthen cooperation on cybersecurity."

07.03.17

Politico

[WikiLeaks dumps alleged secret CIA 'hacking arsenal'](#)

The internet transparency group WikiLeaks has published a new batch of documents alleged to detail how the CIA has transformed smartphones, computers and IoT devices into espionage tools for electronic surveillance. Whilst the authenticity of the leaked documents remains debatable, a former intelligence officer has told Politico that the documents seem genuine.

"WikiLeaks on Tuesday began publishing what it claims is the CIA's secret "hacking arsenal" that reveals how the intelligence agency transforms smartphones, computers and internet-connected televisions into spying devices.

The cache allegedly comes from the agency's Cyber Intelligence Center, potentially spilling into the public domain an unprecedented amount of information about the CIA's electronic snooping. WikiLeaks called it the "largest ever publication of confidential documents" about the agency."

Privacy

02.03.17

Irish Times

US government asks High Court to refuse Facebook case referral

Lawyers for the US government have called on the Irish High Court to reject a motion to move the data privacy case against Facebook to the EU's Court of Justice. The motion was filed by the Irish Data Protection Commissioner, but US lawyers have criticized her decision suggesting it places EU-US data cooperation in jeopardy.

"The US government has urged the [High Court](#) to refuse the Data Protection Commissioner's bid to have the Court of Justice of the EU (CJEU) decide issues with potentially enormous consequences for EU-US data transfers.

Eileen Barrington SC, for the US, said the commissioner's "unique", "unusual" and "unprecedented" application for a reference to the CJEU was based on the commissioner's "fatally flawed" draft finding concerning adequacy of remedies available in the US for breach of data privacy rights of EU citizens.

This application was of "critical significance" to the US for legal and commercial reasons and should be dismissed for reasons including that it had been "entirely overtaken by events", particularly the 2016 agreement between the [European Commission](#) and US on the Privacy Shield framework for EU-US data transfers."

08.03.17

Channel News Asia

UN expert urges states to work towards cyber surveillance treaty

The UN's privacy expert Joe Cannataci has produced a report calling for an international agreement on cyber surveillance, claiming that current standards are outdated in the digital age. The report also calls for the creation of an international warrant for data access, to reduce reliance on US legal safeguards and practices.

"The world needs an international treaty to protect people's privacy from unfettered cybersurveillance, which is being pushed by populist politicians preying on fear of terrorism, according to a U.N. report debated on Wednesday.

The report, submitted to the U.N. Human Rights Council by the U.N. independent expert on privacy, Joe Cannataci, said traditional privacy safeguards such as rules on phone tapping were outdated in the digital age.

*"It's time to start reclaiming cyberspace from the menace of over-surveillance,"
Cannataci told the Council."*

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

03.03.17

SC Magazine

[China releases first cyberpolicy paper](#)

China has published its first cyberpolicy paper, which outlines the country's position on a range of domestic and international cyber issues. In the paper the Chinese Government specifically calls for greater cooperation in internet governance, though with national sovereignty retained by individual countries.

"The goal of the paper is to provide a comprehensive explanation of China's policy and position on cyber-related international affairs among other things.

[China](#) listed peace, sovereignty, shared governance, and shared benefits as its basic principles and included brief explanations as to how they pertain to the cyberspace in its first cyberpolicy paper entitled "International Strategy of Cooperation on Cyberspace."

The goal of the paper is to provide a comprehensive explanation of China's policy and position on cyber-related international affairs as well as the basic principles, strategic goals and plan of action in its external relations, according to an English translation of the policy published by the state-run news agency [Xinhua](#)."

07.03.17

Economic Times (India)

[India open for widest cyber security collaboration: Ravi Shankar Prasad](#)

The Indian Government has announced itself open to further cybersecurity collaboration, following a speech by IT Minister Ravi Shankar Prasad at the ICEGOV conference on international e-governance.

"The government is open for international collaboration in the field of cyber security and favours handling issue of cyber terrorism in cooperation with other countries, IT Minister Ravi Shankar Prasad said today.

"India is willing to have the widest cooperation world over in the quest of cyber security," Prasad said at international conference on e-governance, ICEGOV, here."

Cybersecurity

02.03.17

MIS Asia

[APAC consumers interested in new technologies that enhance digital payment security](#)

A new study has found that 45% of consumers in Asia Pacific have expressed interest in new ways to increase the security of digital payments. The 2017 Mastercard Digital Payments Study found that the most popular technologies were biometrics and digital wallet systems.

“Nearly half of consumers (45 percent) in the Asia Pacific (APAC) region expressed interest in biometrics and other forms of authentication to enhance digital payment security, reduce fraud, and eliminate passwords.

This according to the 2017 edition of Mastercard Digital Payments Study, in partnership with PRIME Research and Synthesio. The study analysed more than 3.5 million conversations on Twitter, Facebook, Instagram, and Weibo in 2016 to identify the key trends around digital payment methods, technologies, and purchases.

In APAC, consumers' excitement around new biometric and authentication technologies drove positive sentiment (66 percent) for safety and security discussions. New developments in facial recognition and fingerprint and touch authentication drove over half of biometric/authentication conversations (51 percent).”

03.03.17

Channel News Asia

[Singapore to set up new Defence Cyber Organisation](#)

Singapore has announced that a new Defence Cyber Organisation will be established to better defend the country's armed forces network. The Government was prompted to establish the new body following a breach of personal details of both civilian and military officials within the Ministry of Defence.

“A new Defence Cyber Organisation (DCO) will be set up to monitor and defend the Singapore Armed Forces' (SAF) networks around-the-clock from cyberthreats, Defence Minister Ng Eng Hen announced in Parliament on Friday (Mar 3).

Earlier this week, a [breach in an Internet access system at MINDEF](#) resulted in the personal data of 850 national servicemen and employees being stolen. The

growing risk of such threats in recent times has seen the SAF doubling the number of cyberdefence personnel and investing in emerging technologies through the Cyber Security Operations Centre 2.0 initiative in April last year. A Cyber Defence Operations Hub was also built in 2013.”

05.03.17

Times of India

[India, US set to bolster security ties, focus on cyber, maritime security](#)

The US and Indian Governments have announced further cooperation on security issues. The bilateral alliance will further strengthen training and exchange programs covering issues from cybersecurity to hostage negotiation.

“India and the US are set to further strengthen their bilateral security ties under the [Trump](#) administration with the two countries deciding to continue exchange programmes on hostage crisis, terror crime scene probe and cybercrime.

A delegation of officials from the US met their counterparts in the home ministry last week and discussed ways to streamline the training programmes being conducted under the [Anti-Terrorism Assistance](#) (ATA) pact.

Indian police officers will undergo training programmes in the US training institutes on negotiations in hostage situations, terror crime scene investigations, besides on two new courses relating to cyber crime and maritime security.”

06.03.17

Telangana Today

[India, Portugal to collaborate in electronic manufacturing, cyber security](#)

India and Portugal have agreed to a new collaboration on electronic and digital issues. The partnerships will focus on the manufacturing of electronics, as well as collaboration on cybersecurity and e-governance.

“[India](#) and [Portugal](#) on Monday agreed to set up an institutional mechanism to collaborate in areas of electronic manufacturing, ITeS, start-ups, cyber security and e-governance, an official said.

“We had a very good discussion and have agreed to collaborate in the areas of electronic manufacturing, ITeS, cyber security, e-governance and capacity building. We will support the Portugal team in scaling up their initiatives — Simplex and Portuguese Citizen Shops, which are like our MyGov and Common Service Centre initiatives,” [IT Minister Ravi Shankar Prasad](#) said.”

07.03.17

Network Asia

[Managing cybersecurity has become more complex: study](#)

Intel Security's South East Asia Cyber Awareness Study has found that cybersecurity specialists in the region believe that cybersecurity has become more complex in recent years. Whilst some view on complexity differed across the region, the majority of respondents agreed on the increased complexity of cybersecurity.

"Managing cybersecurity has become more complex, reveals the Intel Security South East Asia Cyber Awareness Study.

Of the countries surveyed, about 1 in 3 respondents from Thailand and almost 1 in 2 respondents from Singapore felt that managing cybersecurity had become more complex. In fact, in Singapore, only 20 percent of respondents believe that it had become less complex. 44 percent of respondents from Philippines, the country reported to be the least "cyber mature" in Southeast Asia, also felt managing cybersecurity had become more complex.

In contrast, respondents from Malaysia, Indonesia and Vietnam felt managing cybersecurity had become less complex at 31 percent, 34 percent and 41 percent respectively."

Privacy

08.03.17

Channel News Asia

[UN expert urges states to work towards cyber surveillance treaty](#)

The UN's privacy expert Joe Cannataci has produced a report calling for an international agreement on cyber surveillance, claiming that current standards are outdated in the digital age. The report also calls for the creation of an international warrant for data access, to reduce reliance on US legal safeguards and practices.

"The world needs an international treaty to protect people's privacy from unfettered cybersurveillance, which is being pushed by populist politicians preying on fear of terrorism, according to a U.N. report debated on Wednesday.

The report, submitted to the U.N. Human Rights Council by the U.N. independent expert on privacy, Joe Cannataci, said traditional privacy safeguards such as rules on phone tapping were outdated in the digital age.

"It's time to start reclaiming cyberspace from the menace of over-surveillance," Cannataci told the Council."

Internet Inclusion

02.03.17

Economic Times

[India ranks 36th in Internet inclusiveness, 46th in availability: Facebook-EIU](#)

A new report by the Facebook-Economist Intelligence Unit has found that India ranks 36th out of 75 nations for internet inclusiveness. The report ranked countries based on affordability, availability and access policies. The top 5 countries were Singapore, Sweden, USA, UK and Japan.

"India ranked 36th among 75 nations in Internet inclusiveness based on factors like availability, affordability and policies for access, a Facebook-Economist Intelligence Unit (EIU) report today said.

The top countries in the tally included Singapore, Sweden, the US, the UK and Japan.

In terms of availability, India ranked 46th, while it jumped a few spots to 26th position in terms of affordability."

07.03.17

India Times

[Kerala Has Become The First Indian State To Make Internet Access A Basic Right, A Model For The Country To Follow](#)

The Indian State of Kerala has become the first in the country to make internet access a basic right for citizens. The Kerala government will seek to increase internet access in the next 18 months through a new fibre optic network.

"After Finland became the first country in the world to recognise 'the right to Internet access', Kerala is all set to become the first state to do the same in India.

The Kerala budget presented by state finance minister Thomas Issac on Friday proposed to make internet access a human right. Under the proposal, the government aims to provide free internet access to 20 lakhs households.

The project named K-FON (Kerala Fibre Optic Network) has been allocated Rs1,000 crore in the budget. The project is expected to be completed within 18 months."

Rest of the World

Internet governance

03.03.17

IT Web Africa

[Digital rights group bemoans Nigeria's internet regulation](#)

A new consultation launched by the Nigerian government will seek to establish an industry code of practice for net neutrality and internet transparency. The consultation features leading stakeholders and the country's Internet Service Providers.

"Nigeria has initiated an online public consultation with a list of key stakeholders to help it establish an industry Code of Practice in support of net neutrality and an open internet. However, the exclusion of digital rights group Paradigm Initiative Nigeria has not gone unnoticed by its executive director.

The Nigerian Communications Commission's (NCC) proposed Code of Practice is expected to establish best practices for internet governance in line with emerging issues and global trends, and promote the safe and responsible use of internet services.

It will seek to provide solutions to address issues of discriminatory traffic management practices, as well as protect the rights and interests of both consumers and Internet Service Providers (ISPs)."

Cybersecurity

06.03.17

The Hill

[British defense officials call for more cooperation between NATO, EU on cyber](#)

The UK's Defence Minister and leading Defence Civil Servant Stephen Lovegrove have both called for greater cybersecurity cooperation between NATO and the EU. Speaking at the Atlantic Council in Washington D.C. Mr Lovegrove warned NATO members not to become complacent on their security.

"Officials with Britain's Defense Ministry on Monday called for greater cooperation on cybersecurity between NATO and the European Union.

The demands come in the wake of Britain's vote to leave the EU, which British Defense Secretary Michael Fallon indicated Monday would not affect Britain's security cooperation with other European nations.

Fallon and Stephen Lovegrove, the Defense Ministry's permanent secretary, both said in separate remarks on Monday that NATO and EU should strengthen cooperation on cybersecurity."

Privacy

08.03.17

Channel News Asia

[UN expert urges states to work towards cyber surveillance treaty](#)

The UN's privacy expert Joe Cannataci has produced a report calling for an international agreement on cyber surveillance, claiming that current standards are outdated in the digital age. The report also calls for the creation of an international warrant for data access, to reduce reliance on US legal safeguards and practices.

"The world needs an international treaty to protect people's privacy from unfettered cybersurveillance, which is being pushed by populist politicians preying on fear of terrorism, according to a U.N. report debated on Wednesday.

The report, submitted to the U.N. Human Rights Council by the U.N. independent expert on privacy, Joe Cannataci, said traditional privacy safeguards such as rules on phone tapping were outdated in the digital age.

"It's time to start reclaiming cyberspace from the menace of over-surveillance," Cannataci told the Council."

Internet Inclusion

07.03.17

IT Web Africa

[Benin, Botswana climb on affordable internet ranking](#)

The Alliance for Affordable Internet has published its 2017 rankings of Internet affordability. The report finds that the biggest increases have occurred in African countries, following the introduction of new policies and greater implementation of existing ones.

“The 2017 Affordability Drivers Index rankings by the Alliance for Affordable Internet (A4AI) shows that two of the five countries that have made the biggest improvements in their scores since 2016 are in Africa.

In its Affordability Report released last week, the global coalition working to make broadband affordable for all notes that Benin and Botswana recorded changes - alongside Jordan, Ecuador and Vietnam - that stemmed primarily from the introduction of new or updated policies or the effective implementation of existing ones.

The report seeks to measure progress toward affordable internet and highlights related changes made to drive prices down and expand access in some 58 low- and middle-income countries.”

Global Institutions

01.03.17

Digital Europe

[DIGITALEUROPE's thoughts and recommendations on the Electronic Communications Code](#)

Digital Europe have published a new position paper on the EU's proposed Electronic Communications Code. The paper largely agrees with the EU's plans, though states that consideration has to be paid to the development of technology in the future.

"On 1 March, DIGITALEUROPE published its new position paper on the Electronic Communications Code (ECC), the core piece of legislation poised to revamp the European telecoms framework. Announced by the Commission back in September 2016, the ECC promises to deliver on better connectivity in the EU and foster investment in high-capacity networks.

DIGITALEUROPE worked with the Commission and stakeholders in the lead-up to this proposal, through consultations and outreach meetings. Overall we welcome the provisions of the ECC and are glad to see the Commission recognize the need for an overhaul in order to meet the connectivity and capacity needs of tomorrow. The proposed measures, on access regulation and coordinated spectrum management, are steps in the right direction."

02.03.17

ICANN

[Annual IANA Functions, DNSSEC Audits Validate ICANN Systems Controls](#)

ICANN's system controls of IANA's registry management systems and the Domain Name System Security Extensions have been audited by PricewaterhouseCoopers, who have validated ICANN's existing protocols.

"The Internet Corporation for Assigned Names and Numbers (ICANN) has completed audits of the IANA registry management systems and the Domain Name System Security Extensions (DNSSEC) services it provides. International accounting firm PricewaterhouseCoopers conducted the audits for the period of 1 December 2015 through 30 September 2016.

For the fourth consecutive year, a Service Organization Control (SOC) 2 audit of the IANA registry maintenance systems shows that ICANN has the appropriate controls in place to ensure the security, availability and processing integrity of IANA functions transactions."

07.03.17

ICANN

[Competition, Consumer Trust and Consumer Choice Review Team Draft Report of Recommendations For New gTLDs Available for Public Comment](#)

ICANN have published a draft report from its Competition, Consumer Trust and Consumer Choice Review Team into the body's new gTLD Program. The report will now be open for public comment until 27 April 2017.

*“The Internet Corporation for Assigned Names and Numbers (ICANN) today announced the publication of the **Draft** Report from the Competition, Consumer Trust and Consumer Choice (CCT) Review Team with its recommendations for the New gTLD Program.*

[Executive summary.](#) [PDF, 71 KB]

[Summary of Recommendations.](#) [PDF, 1.34 MB]

[Read the report.](#) [PDF, 3.91 MB]”

Diary Dates

[Building the European data economy](#) – 10.01.17-26.04.17

[ENISA evaluation and review](#) – 18.01.17 – 12.04.17

Open from 18 January to 12 April 2017.

[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

[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