IEEE
GLOBAL INTERNET POLICY MONITOR
Read summaries of significant recent internet technology policy activities around the world

## 17 May 2017

## Synopsis

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

The inescapable cyber story this week is the impact of the **WannaCry ransomware** attack which spread across the world late last week. Analysis of the attack suggests that **cyber tools** developed by the **NSA** and leaked by hackers in recent months may have been responsible. Additional work has also suggested that **North Korean** hackers may have perpetrated the global cyber attack.

Following the global cyberattack Russian President **Vladimir Putin** has warned that national governments should be careful of creating hacking software tools, due to the future potential that **hackers** can use the same tools for malicious means.

In the **EU** this week several member states have made clear their desire to reduce **data privacy** rules for **telecoms** companies and communication services, so that greater levels of customer data can be processed and handed to Governments.

In the **UK** the Prime Minister **Theresa May** has pledged that if re-elected her party will introduce powers to penalise **social media** and communications companies that suffer **breaches** of client data, as well as a tax for government monitoring of the internet.

President **Donald Trump** has published his executive order on **cybersecurity** that will launch a review of the **vulnerabilities** in federal government systems. The executive order had originally been set for publication in the first weeks of the Trump administration, however was delayed to allow for greater input by government experts.

54 international **business** groups have lobbied the **Chinese** Government to postpone the new **cybersecurity** law set to launch in June, claiming that it will violate China’s existing trade agreements and could harm the country’s technology industry.

The Government of **Thailand** is currently considering whether to block access to **Facebook** in the country after the social media giant was ordered to remove illicit urls and posts from the site.

**Rwanda's** President **Paul Kagame** has warned that **African** countries will need to further embrace public-private partnerships if the **Broadband** Commission target of 50% **internet accessibility** is to be reached by 2020.

**ENISA** and **Digital Europe** have both praised the response of **EU** countries in responding to the global **WannaCry** ransomware attack, with ENISA in particular praising the cooperation between countries to minimise the threat.

# IEEE Global Internet Policy Monitor

**17 May 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

**12.05.17**

**Reuters**

**UK PM May pledges new powers to punish and tax social media firms**

The UK Prime Minister Theresa May has pledged that if re-elected her party will introduce powers to penalise social media and communications companies that suffer breaches of client data, as well as a tax for government monitoring of the internet.

*"British Prime Minister Theresa May pledged to create new powers allowing her to punish social media and communications companies that fail to look after users' data, and to demand cash from firms to pay for policing the internet.*

*The election pledge comes after firms like Facebook and Twitter have been criticized the government for not doing enough to stop the spread of extremist content online or help victims of abuse."*

**15.05.17**

**Bloomberg**

**Trade Groups Appeal to Beijing to Postpone Cybersecurity Law**

54 international business groups have lobbied the Chinese Government to postpone the new cybersecurity law set to launch in June, claiming that it will violate China's existing trade agreements and could harm the country's technology industry.

*"A coalition of 54 global business groups appealed to Chinese authorities Monday to postpone enforcing a cybersecurity law they warned violates Beijing's free-trade pledges and might harm information security.*

*The appeal by groups from the United States, Japan, Britain and other countries adds to complaints Beijing is improperly limiting access to its markets for technology products, possibly to support its own fledgling suppliers."*

# Cybersecurity

**12.05.17**

**SC Media**

## Russia blamed for DDoS attacks on Baltic Power grid

Authorities in Lithuania, Latvia and Estonia have all criticised Russia for a recent DDoS attack on the power grids of their respective countries. A NATO official has told Reuters that such probing attacks could signal that a more disruptive attack could take place in future.

*"The Lithuanian, Latvian and Estonian power grids have all been targeted by Russia undergoing a series of limited Distributed Denial of Service (DDoS) over the last few years that may be probing for weaknesses.*

*A Reuters story said law and utility officials from the three NATO members said DDoS attacks have been launched by Russia against different internet gateways that are used to control the power grid for the Baltic area. The unnamed sources also reported attacks against network communications devices that link power sub-stations to central control and a separate attack targeting a petrol-distribution system."*

**12.05.17**

**Politico**

## NSA-created cyber tool spawns global attacks — and victims include Russia

The WannaCry ransomware which attacked companies and hospitals in over 150 countries this week is believed to have originated from NSA hacking tools leaked online earlier this year by the Shadow Brokers collective of hackers.

*"Leaked alleged NSA hacking tools appear to be behind a massive cyberattack disrupting hospitals and companies across Europe, Asia, with Russia among the hardest-hit countries.*

*But the Department of Homeland Security told POLITICO it had not confirmed any attacks in the U.S. on government targets or vital industries, such as hospitals and banks."*

## Privacy

**16.05.17**

**EURACTIV**

**Member states want looser data rules in draft ePrivacy bill**

A number of EU member states have made clear their desire to reduce data privacy rules for telecoms companies and communication services, so that greater levels of customer data can be processed and handed to Governments.

*"EU member states are divided over a proposal to change privacy rules for telecoms operators, with some countries calling for looser rules on when they can use consumers' personal data.*

*Draft rules detailing when telecoms companies and digital communication services like WhatsApp can process consumer data should be softened, according to a report dated 15 May on the progress of national governments' negotiations on the European Commission's proposal to overhaul the ePrivacy legislation."*

**17.05.17**

**Computing**

**European Commission launches €5m DECODE blockchain project**

To further explore the future potential of blockchain as a secure method of data storage and distribution the European Commission has launched a €5m project to explore and develop the technology.

*"The European Commission has launched a new €5m project to explore the possibilities of using blockchain technology to control how data is stored and shared.*

*It forms part of Horizon 2020, an €80bn EU research and innovation programme which began back in 2014. The seven-year programme is designed to ensure that Europe can continue to compete on a global scale."*

## Internet Inclusion

***No new items of relevance***

# United States of America

## Internet governance

**15.05.17**

**Bloomberg**

**Trade Groups Appeal to Beijing to Postpone Cybersecurity Law**

54 international business groups have lobbied the Chinese Government to postpone the new cybersecurity law set to launch in June, claiming that it will violate China's existing trade agreements and could harm the country's technology industry.

*"A coalition of 54 global business groups appealed to Chinese authorities Monday to postpone enforcing a cybersecurity law they warned violates Beijing's free-trade pledges and might harm information security.*

*The appeal by groups from the United States, Japan, Britain and other countries adds to complaints Beijing is improperly limiting access to its markets for technology products, possibly to support its own fledgling suppliers."*

## Cybersecurity

**10.05.17**

**SC Media**

**FTC launches cybersecurity site for small businesses**

A new website that provides advice to small businesses on cybersecurity issues has been launched by the Federal Trade Commission. The new website will attempt to provide protections for smaller businesses who have collectively experienced a dramatic increase in cyberattacks from sophisticated actors.

*"The Federal Trade Commission (FTC) has launched a new website where small businesses can receive tips and advice on cybersecurity issues.*

*The site, FTC Small Business, is geared toward helping the 28 million small businesses in the country, employing some 57 million people, become better prepared for dealing with scams and securing their computer networks."*

**11.05.17**

**Politico**

**Trump signs long-awaited cyber order, launching hacking defense review**

President Donald Trump has published his executive order on cybersecurity that will launch a review of the vulnerabilities in federal government systems. The executive order had originally been set for publication in the first weeks of the Trump administration, however was delayed to allow for greater input by government experts.

*"President Donald Trump on Thursday signed a long-delayed cybersecurity executive order that launches sweeping reviews of the federal government's digital vulnerabilities and directs agencies to adopt specific security practices.*

*The directive is Trump's first major action on cyber policy and sets the stage for the administration's efforts to secure porous federal networks that have been repeatedly infiltrated by digital pranksters, cyber thieves and government-backed hackers from China and Russia."*

**12.05.17**

**SC Media**

**Millions of identities stolen from education platform Edmodo**

The education platform Edmodo has suffered a significant breach in which the account details of several million users have been stolen and put up for sale on the dark web. The account details stolen include hashed passwords which may delay the access of accounts by hackers.

*"The account details of millions of subscribers to the education platform Edmodo have not only been stolen but witnessed to be for sale on the dark web, according to a post on Motherboard.*

*The platform is used by more than 78 million teachers, students and parents to compose lesson plans, make homework assignments and other tasks."*

**12.05.17**

**Politico**

**NSA-created cyber tool spawns global attacks — and victims include Russia**

The WannaCry ransomware which attacked companies and hospitals in over 150 countries this week is believed to have originated from NSA hacking tools leaked online earlier this year by the Shadow Brokers collective of hackers.

*“Leaked alleged NSA hacking tools appear to be behind a massive cyberattack disrupting hospitals and companies across Europe, Asia, with Russia among the hardest-hit countries.*

*But the Department of Homeland Security told POLITICO it had not confirmed any attacks in the U.S. on government targets or vital industries, such as hospitals and banks.”*

**15.05.17**

**SC Media**

**Cyber Czar Giuliani's 'cyber doctrine' still unfinished**

The new US cyber doctrine currently being crafterd by Rudy Giuliani the White House Cyber Czar remains unfinished according to the Director of National Intelligence.

*“A legal framework for the U.S. to respond to cyber-offensive operations is still hanging in Limbo as the Director of National Intelligence draws a blank on its status.*

*The White house Cyber Czar and former Mayor of New York is working on a “cyber doctrine” for the U.S., according to the Director of National Intelligence (DNI).”*

**15.05.17**

**Next Gov**

**White House: No US Federal systems hit by Wannacry ransomware**

The US Government has issued a statement that no Federal systems where affected by the WannaCry ransomware attack this week.

*“A massive ransomware offensive that raged across 150 countries has not hit any U.S. federal agencies or critical infrastructure such as energy plants and airports, President Donald Trump’s top homeland security adviser said Monday.*

*The campaign has struck more than 300,000 machines globally, Homeland Security Adviser Tom Bossert said during a White House news conference Monday. The attack relies on a computer vulnerability that may have been initially discovered by the National Security Agency and used to spy on adversaries."*

**15.05.17**

**Government Technology**

**National Intelligence Chief Says Smart Device Security Must Improve**

The Director of National Intelligence Dan Coats has called for an increase in action to counteract the perceived security risk posed by the Internet of Things.

*"The director of intelligence is warning that the "Internet of Things" gives cyber criminals new ways to use our connectivity against us.*

*As consumers demand further integration of these devices, the risk increases — unless we demand stricter security standards by manufacturers."*

## Privacy

***No new items of relevance***

## Internet Inclusion

***No new items of relevance***

# Pan-Asia

## Internet governance

**15.05.17**

**Bloomberg**

**Trade Groups Appeal to Beijing to Postpone Cybersecurity Law**

54 international business groups have lobbied the Chinese Government to postpone the new cybersecurity law set to launch in June, claiming that it will violate China's existing trade agreements and could harm the country's technology industry.

*"A coalition of 54 global business groups appealed to Chinese authorities Monday to postpone enforcing a cybersecurity law they warned violates Beijing's free-trade pledges and might harm information security.*

*The appeal by groups from the United States, Japan, Britain and other countries adds to complaints Beijing is improperly limiting access to its markets for technology products, possibly to support its own fledgling suppliers."*

## Cybersecurity

**12.05.17**

**Politico**

**NSA-created cyber tool spawns global attacks — and victims include Russia**

The WannaCry ransomware which attacked companies and hospitals in over 150 countries this week is believed to have originated from NSA hacking tools leaked online earlier this year by the Shadow Brokers collective of hackers.

*"Leaked alleged NSA hacking tools appear to be behind a massive cyberattack disrupting hospitals and companies across Europe, Asia, with Russia among the hardest-hit countries.*

*But the Department of Homeland Security told POLITICO it had not confirmed any attacks in the U.S. on government targets or vital industries, such as hospitals and banks."*

**16.05.17**

**SC Media**

**[WannaCry ransomware code appears linked to suspected North Korean APT]**

Analysis from Symantec suggests that the WannaCry ransomware attack may have origninated from the North Korean hacking organisation known as the Lazarus Group. In a blog post the company argues that early versions of the ransomware appear to have been implemented through the use of tools commonly associated with the group.

*“If North Korea is indeed behind the May 11 WannaCry attack, it would be the first known time a nation-state sponsored and perpetrated a ransomware attack.*

*Analysis of the WanaCrypt0r 2.0 ransomware that bedeviled enterprises across the globe this past weekend has turned up apparent links to the alleged North Korean hacking institution known as the Lazarus Group.”*

## Privacy

***No new items of relevance***

## Internet Inclusion

**16.05.17**

**Bangkok Post**

**Facebook faces immediate shutdown threat**

The Government of Thailand is currently considering whether to block access to Facebook in the country after the social media giant was ordered to remove illicit urls and posts from the site.

*“Thailand could lose all access to Facebook on Tuesday as the military regime puts up a hardball command: Censor 131 posts or lose millions of Thai users.*

*The Thai Internet Service Provider Association (Tispa) says it is under government pressure to immediately shut down the all access to Facebook as early as Tuesday morning, over the social medium's refusal to take down every post dictated.”*

# Rest of the World

## Internet governance

**15.05.17**

**Reuters**

**Putin warns of risks of governments creating hacking tools**

Following the global cyberattack Russian President Vladimir Putin has warned that national governments should be careful of creating hacking software tools, due to the future potential that hackers can use the same tools for malicious means.

*“Russian President Vladimir Putin said on Monday that intelligence services should beware of creating software that can later be used for malicious means - a reference to global 'ransomware' attacks that researchers say exploited a hacking tool built by the U.S. National Security Agency.*

*Speaking to reporters in Beijing, where he is taking part in a conference, Putin said that there was no significant damage to Russian institutions, including its banking and healthcare systems, from the computer worm known as WannaCry.”*

**15.05.17**

**Bloomberg**

**Trade Groups Appeal to Beijing to Postpone Cybersecurity Law**

54 international business groups have lobbied the Chinese Government to postpone the new cybersecurity law set to launch in June, claiming that it will violate China’s existing trade agreements and could harm the country’s technology industry.

*“A coalition of 54 global business groups appealed to Chinese authorities Monday to postpone enforcing a cybersecurity law they warned violates Beijing's free-trade pledges and might harm information security.*

*The appeal by groups from the United States, Japan, Britain and other countries adds to complaints Beijing is improperly limiting access to its markets for technology products, possibly to support its own fledgling suppliers.”*

**18.05.17**

**MIS Asia**

**[More business transparency with new ASEAN digital registry: Malaysia, New Zealand]**

New Zealand's Foster Moore International and Malaysia's Omesti have agreed a new partnership to develop a digital transparency registry for ASEAN countries, to meet the demands of governments and regulatory bodies from across the region.

*"More business transparency throughout the Asean region may be possible following a recent partnership involving Malaysia's Omesti and New Zealand's Foster Moore International.*

*This move is to help meet the demand from governments and regulatory bodies through the Asean region for greater transparency across the corporate landscape, said the technology partners."*

## Cybersecurity

**12.05.17**

**Politico**

**NSA-created cyber tool spawns global attacks — and victims include Russia**

The WannaCry ransomware which attacked companies and hospitals in over 150 countries this week is believed to have originated from NSA hacking tools leaked online earlier this year by the Shadow Brokers collective of hackers.

*"Leaked alleged NSA hacking tools appear to be behind a massive cyberattack disrupting hospitals and companies across Europe, Asia, with Russia among the hardest-hit countries.*

*But the Department of Homeland Security told POLITICO it had not confirmed any attacks in the U.S. on government targets or vital industries, such as hospitals and banks."*

## Privacy

***No new items of relevance***

## Internet Inclusion

**11.05.17**

**IT Web Africa**

**Africa has three years to meet 2020 internet access deadline**

Rwanda’s President Paul Kagame has warned that African countries will need to further embrace public-private partnerships if the Broadband Commission target of 50% internet accessibility is to be reached by 2020.

*“Public-private partnerships and bridging the digital divide will help Africa meet the Broadband Commission target of providing at least 50% of its population with internet accessby 2020.*

*This is according to Rwanda's President Paul Kagame who addressed delegates at Transform Africa Summit 2017 in Kigali under the banner 'Smart Cities: Fast Forward.”*

# Global Institutions

**11.05.17**

**ITU**

**WSIS Prizes 2017: World's top 'ICT for Development' initiatives announced**

ITU has announced the 90 finalists for the 2017 WSIS prizes to be awarded a the WSIS Forum in Geneva in June.

*"The International Telecommunication Union (ITU) has announced the top-90 winning Information and Communication Technology for Development (ICT4D) initiatives from around the world competing for prestigious WSIS Prizes 2017, from which will emerge one top Winner and four Champions in each of the 18 prize categories. These 18 category Winners will be announced and presented with their awards, and Champions honoured, on 13 June at the WSIS Prizes 2017 ceremony to be held at the Geneva International Conference Centre during WSIS Forum 2017. WSIS Prizes honour outstanding projects that leverage the power of ICT to accelerate socio-economic development around the globe."*

**11.05.17**

**ENISA**

**ENISA welcomes the publication of the DSM mid-term review**

ENISA has published a note praising the mid-term review of the EU's Digital Single Market. In particular the agency has highlighted a number of key considerations on cybersecurity that they will look to support in the coming years.

*"ENISA is in full agreement on the importance of this subject and the economic opportunities that arise from a successful delivery of the DSM.*

*It has to be recognised that a key component to the success of any Digital Market Strategy is a secure digital environment. In this context, ENISA is pleased to note that a number of fundamental issues on cybersecurity have been identified in this report."*

**12.05.17**

**Digital Europe**

**DIGITAL EUROPE replies to Commission International Data Transfer Communication**

Digital Europe has responded to the European Commissions communication on International Data Transfers, highlighting its belief that the time is right for the creation of an international data flows unit within the Jusice Directorate of the Comission.

*“DIGITAL EUROPE sent a letter to the European Commission regarding its recent International Data Transfers Communication. The Communication, published in January 2017, set out the Commission’s future agenda on ‘exchanging and protecting personal data in a globalised world’ and covered issues related to adequacy decisions, potential new standard contractual clauses (“SCCs”) and possible future Binding Corporate Rules (“BCRs”) developments.”*

**15.05.17**

**ENISA**

**WannaCry Ransomware: First ever case of cyber cooperation at EU level**

ENISA has praised the EU’s response to the WannaCry ransomware attack, highlighting the unprecedented levels of cooperation between member states to limit the extent of the damaged caused.

*“As of Friday 12 May 2017, multiple variants of a ransomware named WannaCry have been spreading globally, affecting hundreds of thousands of users, organizations, including users in the European Union. It is understood that the cyber attack is focussed on Microsoft Windows based operating systems.*

*Udo HELMBRECHT, Executive Director of ENISA, said “as the European Cybersecurity Agency, we are closely monitoring the situation and working around the clock with our stakeholders to ensure the security of European citizens and businesses, and the stability of the Digital Single Market. We are reporting on the evolution of the attacks to the European Commission and liaising with our partners in the European Union CSIRT Network”.”*

**16.05.17**

**ITU**

**[Plans for ITU Telecom World 2017 advance with MoA signing by Republic of Korea and ITU]**

ITU have announced that preparations for the ITU Telecom World 2017 set to run from 25 to 28 September are advancing following the signing of a memorandum of arrangement with the South Korean Ministry of Science, ICT and Future Planning.

*"The International Telecommunication Union (ITU) has today signed a Memorandum of Arrangement (MoA) with the Republic of Korea through its Ministry of Science, ICT and Future Planning for the hosting in Busan of ITU Telecom World 2017. This leading global information and communications technology (ICT) event will take place 25-28 September and will focus on the creative digital economy and fostering tech small- and medium-sized enterprises (SMEs). ITU Telecom events are designed to help ideas go further, faster to make the world better, sooner."*

**16.05.17**

**Digital Europe**

**[WannaCry cyber-attack confirms EU cyber policy actions heading in right direction]**

Digital Europe has praised the progression of EU cyber policy following the WannaCry ransomware, stating that the Bloc's preparedness have allowed it to prevent a major cybersecurity incident from escalating further.

*"DIGITAL EUROPE is relieved that this weekend's WannaCry ransomware cyber-attack appears to be slowing. Our members remain highly vigilant and are proactively sharing any insights they have into forestalling further attacks.*

*The weekend's events have highlighted the need for greater efforts in cybersecurity, but also that the EU is on the right path. No legislation can ever remove the risk of cyber-attacks, but the right policy framework does make it easier to respond to them more effectively. The EU's Network and Information Security Directive ("NIS-D") and General Data Protection Regulation ("GDPR") will provide a framework for critical infrastructure providers to notify governments of cyber incidents, require authorities to share information across national borders, while also allowing organisations to process and exchange personal data such as IP addresses and other network identifiers for legitimate network and information security purposes. These are welcomed and needed steps when it comes to tackling complex cyber-threats."*

# Diary Dates

**Modernising the regulations establishing the .eu top-level domain name – 05.05.17-04.08.17**

European Commission

**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