IEEE GLOBAL INTERNET POLICY MONITOR

Read summaries of significant recent internet technology policy activities around the world

25 October 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **EU's** Security Commissioner, **Sir Julian King** has suggested that **technology companies** could become subject to EU wide legislation to mandate the removal of **extremist content** online.

The **UK's** highest intelligence court will decide whether **GCHQ** has collected and monitored **data** from millions of British citizens and shared it with foreign governments without adequate **protections** in place.

A new international **ransomware** attack nicknamed **Bad Rabbit** has targeted the critical infrastructure of a number of countries around the world. Whilst the attack has resulted in no major outages, it has severely disrupted flights and public transport in **Ukraine**.

US Defence Secretary, **James Mattis** has urged Congress to reword sections of the **National Defense Authorization Act**, as current language would force the US to notify foreign governments before it could combat international **cyber attacks**.

Kaspersky Lab have launched a, 'global transparency initiative' in a bid to win back trust after allegations that their **software** was used for **Russian spying**. They have handed over their **security** and software practices for an independent review and will be creating new **data protection** controls for handling secure data which will be independently overseen.

The **Indian Government** is creating a new tri-service agency to deal with growing cyber threats from **Pakistan**. The **Defence Cyber Agency** will employ 1000 experts and work in coordination with the National Cyber Security Advisor.

Organisers behind the **WorldSkills** competition have announced that for the first time **cybersecurity** will be included in the competition as part of a move to replicate the technology interests of the 2018 host, **Singapore**.

Russian hacking group **APT28**, have targeted attendees of NATO's **security** conference, in a **phishing** style campaign. Ironically, the theme of the conference was, 'The future of Cyber Conflict."

ENISA has published new guidance to support responses to the Wi-Fi WPA2 exploit discovered last week.

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

For more information, visit the IEEE Internet Initiative website, and see *IEEE Global Internet Policy Monitor* past issues. Join IEEE Collabratec™ Internet Technology Policy Community discussions related to internet policy issues and to collaborate with other members of the global technical and policy communities.

IEEE Global Internet Policy Monitor

25 October 2017

Table of Contents

Synopsis 1

Europe 4
- Internet governance 4
- Cybersecurity 5
- Privacy 7
- Internet Inclusion 7

United States of America 8
- Internet governance 8
- Cybersecurity 8
- Privacy 10
- Internet Inclusion 11

Pan-Asia 12
- Internet governance 12
- Cybersecurity 12
- Privacy 13
- Internet Inclusion 13

Rest of the World 14
- Internet governance 14
- Cybersecurity 14
- Privacy 15
- Internet Inclusion 16

Global Institutions 17

Diary Dates 19

Europe

Internet governance

23.10.17

Sky News

EU Commissioner Sir Julian King warns tech firms over extremist content

The EU's Security Commissioner, Sir Julian King has suggested that technology companies could become subject to EU wide legislation to mandate the removal of extremist content online.

"The EU Security Commissioner has warned technology companies that they will face regulation if they don't remove extremist content more quickly.

Sir Julian King told Sky News: "I hope that we're going to be able to make progress, we are taking down tens of thousands of such material but there are hundreds of thousands out there, if not more."

24.10.17

Euractiv

EU plans aid to prosecute hackers and support member states

The EU has agreed to provide new funding to allow Member States to pursue hackers beyond the EU's borders as part of a new package to support member state responses to cyber attacks.

"EU diplomats agreed to provide support to find and prosecute hackers outside the bloc and help member states that are hit with cybersecurity breaches, as part of a strategy to step up defence against large-scale attacks.

In a move to stop hackers and respond to major cybersecurity attacks, member states can help investigate criminals in countries outside the EU, according to a set of guidelines that diplomats have agreed on."

Cybersecurity

18.10.17

City A.M

UK businesses have slashed their cyber security budgets by a third

PWC's annual Global State of Information Survey has found that UK businesses are reducing the amount they spend on cyber security despite the growing threats. Company budgets are apparently down to £3.9 million compared to £6.2 million this time last year.

"Businesses in the UK have cut the amount of cash they are spending on cyber security despite the growing threat of attacks."

"Budgets for security are a third of what they were this time last year, down to £3.9m on average, compared to £6.2m according to research from PwC."

20.10.17

ENISA

Vulnerability of Wi-Fi WPA2 networks

ENISA has published new guidance to support responses to the Wi-Fi WPA2 exploit discovered last week.

"A serious vulnerability affecting the Wi-Fi Protected Access II – WPA2 protocol has been discovered. A potential attack would work against most Wi-Fi network setups e.g. the original WPA, WPA2, and even against networks that only use the Advanced Encryption Standard (AES) technique.

Every time a vulnerability affects the security of a network or a cryptographic protocol, a wide range of devices or services are potentially put at risk."

23.10.17

The Telegraph

RAF recruits cyber experts to probe planes' weaknesses

The RAF have hired cyber experts to inspect their planes for vulnerabilities to ensure their aircrafts are cyber proof to mitigate future attacks.

“The Royal Air Force is recruiting cyber security experts to check its aircraft for weaknesses, amid fears hacking attacks on planes will play an increasing role in future conflict.”

“RAF commanders have been advertising for cyber experts to take jobs checking aircraft and their computer support systems for vulnerabilities.”

24.10.17

SC Media

Cyber-Sec pros targeted: NATO cyber-conflict event in cyber- conflict

Russian hacking group APT28, have targeted attendees of the NATO’s security conference, in a phishing style campaign. Ironically, the theme of the conference was, ‘The future of Cyber Conflict.”

“The Russian hacking group known as APT28 or Fancy Bear crafted a phishing campaign designed specifically to target attendees of a security conference in the US, according to researchers.”

“Delegates planning to attend Washington DC-based Cyber Conflict US, or CyCon received an email in early October with an attachment titled "Conference_on_Cyber_Conflict.doc". The file had been lifted from the conference's website and infected with reconnaissance malware known as "Seduploader", according to researchers from Cisco Talos.”

24.10.17

Reuters

New Wave of cyber-attacks hits Russia, other nations

A new international ransomware attack nicknamed Bad Rabbit has targeted the critical infrastructure of a number of countries around the world. Whilst the attack has resulted in no major outages, it has severely disrupted flights and public transport in Ukraine.

“Cyber-attacks using malware called “Bad Rabbit” hit Russia and other nations on Tuesday, affecting Russian Interfax news agency and causing flight delays at Ukraine’s Odessa airport.”

“While no major outages were reported, the U.S. government issued a warning on the attack, which followed campaigns in May and June that used similar malware and resulted in what some economists estimated are billions of dollars in losses.”

Privacy

18.10.17

New Europe

UK intelligence agencies ‘unlawfully’ sharing sensitive personal data, court hears

The UK’s highest intelligence court will decide whether GCHQ has collected and monitored data from millions of British citizens and shared it with foreign governments without adequate protections in place.

“A secret court will decide whether Intelligence agencies are “unlawfully” sharing huge datasets containing sensitive information about the population with industry, government departments and overseas intelligence services.”

Internet Inclusion

No new items of relevance

United States of America

Internet governance

No new items of relevance

Cybersecurity

18.10.17

Reuters

Pentagon chief asks Congress to not hinder cyber defence

US Defence Secretary, James Mattis has urged Congress to reword sections of the National Defense Authorization Act, as current language would force the US to notify foreign governments before it could combat international cyber attacks.

"U.S. Secretary of Defence James Mattis this week asked Congress to halt pending legislation that would compel the U.S. to alert foreign governments when the Pentagon has decided to combat certain cyber-attacks, according to a letter sent to lawmakers."

"The letter, sent to members of Congress on Tuesday and seen by Reuters, comes as lawmakers finalize the Department of Defense's 2018 spending plan, also known as the National Defense Authorization Act for fiscal year 2018, or NDAA."

19.10.17

The Hill

FERC proposes new cyber controls for power grid

The Federal Energy Regulatory Commission has proposed new measures to protect the US' electricity grid from cyber-attacks. One of the suggestions from the Commission is for the creation of a new critical infrastructure protection standard to mitigate threats.

"The federal entity responsible for regulating the energy sector on Thursday proposed new rules to enhance the cybersecurity of the U.S. electric grid, including those aimed at addressing risks posed by malware."

“The Federal Energy Regulatory Commission (FERC) outlined new proposed security management controls for operators of electric grid systems aimed at enhancing “the reliability and resilience of the nation’s bulk electric systems,” according to a release.”

20.10.17

The Hill

[Dems to hear from state officials on election security]

The Democrats have formed a committee of state officials last week to discuss what steps should be taken to secure the United States’ elections from cyber threats. Their aim is to avoid the same mistakes made in the run up to the 2016 presidential election.

“A task force formed by congressional Democrats will hear from state officials next week on the steps they are taking to secure future elections from cyber threats.”

“The commission, formed over the summer by Reps. Bennie Thompson (D-Miss.) and Robert Brady (D-Pa.), has invited Rhode Island Secretary of State Nellie Gorbea (D) and Virginia Department of Elections Commissioner Edgardo Cortes, as well as a representative from the Election Assistance Commission (EAC), to meet with the panel next Tuesday.”

20.10.17

SC Media

[Not Good: Ransom is cheap to buy and developers are well paid]

A new report by Carbon Black has concluded that those that sell ransomware make the equivalent or more than a law-abiding software developer.

“A report by Carbon Black that studied 21 of the largest dark web markets in August and September 2017 found that some of those who develop and sell ransomware can haul in as much, if not more, than a law-abiding software developer and overall ransomware sales on the dark web are skyrocketing. Other findings include that for the period ransomware sales totaled about $6 million, and were being sold on about 6,300 dark marketplaces with more than 63,000 products available.”

21.10.17

The Hill

[Feds warn about cyberattacks on energy, industrial firms]

The Department for Homeland Security and the Federal Bureau of investigation made a statement last Friday, warning that hackers are now attacking energy and nuclear industries.

“The Department of Homeland Security and the Federal Bureau of Investigation issued a joint statement on Friday warning of an increased danger posed to infrastructure sectors by a malicious "multi-stage intrusion campaign," which the agencies warned had successfully compromised several of their security networks.”

24.10.17

Reuters

[New Wave of cyber-attacks hits Russia, other nations]

A new international ransomware attack nicknamed Bad Rabbit has targeted the critical infrastructure of a number of countries around the world. Whilst the attack has resulted in no major outages, it has severely disrupted flights and public transport in Ukraine.

“Cyber-attacks using malware called “Bad Rabbit” hit Russia and other nations on Tuesday, affecting Russian Interfax news agency and causing flight delays at Ukraine’s Odessa airport.”

“While no major outages were reported, the U.S. government issued a warning on the attack, which followed campaigns in May and June that used similar malware and resulted in what some economists estimated are billions of dollars in losses.”

Privacy

23.10.17

The Guardian

[Kaspersky: security firm tries to win back trust after Russian spying scandal]

Kaspersky Lab have launched a, ‘global transparency initiative’ in a bid to win back trust after allegations that their software has been used by Russian espionage services.

"Cybersecurity firm Kaspersky Lab has launched a "global transparency initiative" in an attempt to win back trust and prove it is safe to use after allegations of Russian spying."

"The initiative will begin with an independent review of Kaspersky's source code, an independent assessment of its own security practices, and the creation of new data protection controls for its handling of secure data, also independently overseen."

Internet Inclusion

23.10.17

The Hoya

Washington needs more cybersecurity skills, Experts Say

As part of Washington, D.C. CyberWeek, a panel of cyber experts emphasized the need for more professionals within the security field. Terry McAuliffe from the Virginia Cyber Security Commission said he was shocked at the lack of highly skilled cyber security experts, which is further exacerbated by the lack of interest US students have in STEM subjects.

"Greater understanding of cyberspace and government support for improving cybersecurity are urgently needed, according to a panel of cyber experts who spoke Oct. 17 as a part of the Washington, D.C. CyberWeek."

"The panel in the Healey Family Student Centre Social Room featured David Fahrenkrug, a former U.S. Air Force analyst and current director of strategic planning at Northrop Grumman; Meredith Burkart, an assistant professor in the Center for Security Studies in the School of Foreign Service; and John Wood, the CEO of Telos Corporation, a private technology consulting company. Suzanne Hall, a managing director at PricewaterhouseCoopers, moderated the discussion."

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

19.10.17

Network Asia

[Cyber-espionage groups are now attacking banks in Asia Pacific]

Kaspersky Lab experts have found that cyber criminals are going beyond traditional cyberespionage and are now attacking banks in the Asia Pacific region. Financial institutions in Malaysia, South Korea, Indonesia, Philippines, China (Hong Kong), Bangladesh, and Vietnam have all been subject to attacks.

"From spying, stealing, and leaking state, military, and trade secrets, cybersecurity researchers at Kaspersky Lab discovered that cybercriminals operating in the region now aim for monetary gain as they infect banks in APAC countries."

19.10.17

The Economic Times

[India is quietly preparing a cyber warfare unit to fight a new kind of enemy]

The Indian Government is creating a new tri-service agency to deal with growing cyber threats from Pakistan. The Defence Cyber Agency will employ 1000 experts and work in coordination with the National Cyber Security Advisor.

"Recently, Pakistani hackers compromised 10 Indian websites which included National Aeronautics, Army Institute of Management and Technology, Defence Institute of Advanced Technology, Army Institute of Management, and the Board of Research in Nuclear Sciences."

"The hacker group — Pakistan Haxor Crew — claimed the action was to avenge the defacement of the Pakistan Railways website by an Indian hacker and to show solidarity with Kashmiris."

24.10.17

Reuters

New Wave of cyber-attacks hits Russia, other nations

A new international ransomware attack nicknamed Bad Rabbit has targeted the critical infrastructure of a number of countries around the world. Whilst the attack has resulted in no major outages, it has severely disrupted flights and public transport in Ukraine.

"Cyber-attacks using malware called "Bad Rabbit" hit Russia and other nations on Tuesday, affecting Russian Interfax news agency and causing flight delays at Ukraine's Odessa airport."

"While no major outages were reported, the U.S. government issued a warning on the attack, which followed campaigns in May and June that used similar malware and resulted in what some economists estimated are billions of dollars in losses."

Privacy

No new items of relevance

Internet Inclusion

24.10.17

Channel News Asia

WorldSkills Singapore 2018 to feature cybersecurity; include university students

World Skills Singapore is a competition to discover the world's most technically skilled youth. This year the competition has expanded its remit, including competition areas that are relevant to industries in Singapore such as cyber security.

"WorldSkills Singapore 2018 will be expanded to include university students and introduce competition areas that are relevant to industries in Singapore such as cybersecurity, SkillsFuture chief executive Ng Cher Pong said on Wednesday"

"Mr Ng was speaking to the media on the sidelines of the 44th international WorldSkills competition in Abu Dhabi. Dubbed the "Olympics of Skills", the biennial competition pits youths around the world in skilled trade areas."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

24.10.17

SC Media

Cyber-Sec pros targeted: NATO cyber-conflict event in cyber- conflict

Russian hacking group APT28, have targeted attendees of NATO's security conference, in a phishing style campaign. Ironically, the theme of the conference was, 'The future of Cyber Conflict."

"The Russian hacking group known as APT28 or Fancy Bear crafted a phishing campaign designed specifically to target attendees of a security conference in the US, according to researchers."

"Delegates planning to attend Washington DC-based Cyber Conflict US, or CyCon received an email in early October with an attachment titled "Conference_on_Cyber_Conflict.doc". The file had been lifted from the conference's website and infected with reconnaissance malware known as "Seduploader", according to researchers from Cisco Talos."

24.10.17

Reuters

New Wave of cyber-attacks hits Russia, other nations

A new international ransomware attack nicknamed Bad Rabbit has targeted the critical infrastructure of a number of countries around the world. Whilst the attack has resulted in no major outages, it has severely disrupted flights and public transport in Ukraine.

"Cyber-attacks using malware called "Bad Rabbit" hit Russia and other nations on Tuesday, affecting Russian Interfax news agency and causing flight delays at Ukraine's Odessa airport."

“While no major outages were reported, the U.S. government issued a warning on the attack, which followed campaigns in May and June that used similar malware and resulted in what some economists estimated are billions of dollars in losses.”

24.10.17

IT Web Africa

Johannesburg, Cairo ranked among top 60 digitally safe cities globally

According to the Safe Cities Index 2017, released by the Economist Intelligence Unit, African cities Cairo and Johannesburg rank in the top 60 global list of digitally safe and cyber secure cities.

“Cairo and Johannesburg have featured on the top 60 global list of digitally safe cities, according to the Safe Cities Index 2017, released by The Economist Intelligence Unit (EIU).”

“The report is based on the second iteration of the Index, which ranks 60 cities across 49 indicators covering digital security, health security, infrastructure security and personal security.”

Privacy

23.10.17

The Guardian

Kaspersky: security firm tries to win back trust after Russian spying scandal

Kaspersky Lab have launched a, ‘global transparency initiative’ in a bid to win back trust after allegations that their software has been used by Russian espionage services.

“Cybersecurity firm Kaspersky Lab has launched a “global transparency initiative” in an attempt to win back trust and prove it is safe to use after allegations of Russian spying.”

“The initiative will begin with an independent review of Kaspersky’s source code, an independent assessment of its own security practices, and the creation of new data protection controls for its handling of secure data, also independently overseen.”

Internet Inclusion

No new items of relevance

Global Institutions

19.10.17

NATO

NATO Deputy Secretary General attends Cyber Security Conference

Rose Gottemoeller, NATO Deputy Secretary General has addressed industry experts at the NATO Information Assurance Symposium Cyber Conference last week, to talk about the importance of cyber defence.

"NATO Deputy Secretary General, Rose Gottemoeller, spoke of the vital importance of cyber defence when she addressed industry experts at the NATO Information Assurance Symposium (NIAS) Cyber Conference today (19 October 2017) in Mons, Belgium."

20.10.17

ENISA

Vulnerability of Wi-Fi WPA2 networks

ENISA has published new guidance to support responses to the Wi-Fi WPA2 exploit discovered last week.

"A serious vulnerability affecting the Wi-Fi Protected Access II – WPA2 protocol has been discovered. A potential attack would work against most Wi-Fi network setups e.g. the original WPA, WPA2, and even against networks that only use the Advanced Encryption Standard (AES) technique.

Every time a vulnerability affects the security of a network or a cryptographic protocol, a wide range of devices or services are potentially put at risk."

24.10.17

SC Media

Cyber-Sec pros targeted: NATO cyber-conflict event in cyber- conflict

Russian hacking group APT28, have targeted attendees of the NATO's security conference, in a phishing style campaign. Ironically, the theme of the conference was, 'The future of Cyber Conflict."

“The Russian hacking group known as APT28 or Fancy Bear crafted a phishing campaign designed specifically to target attendees of a security conference in the US, according to researchers.”

“Delegates planning to attend Washington DC-based Cyber Conflict US, or CyCon received an email in early October with an attachment titled "Conference_on_Cyber_Conflict.doc". The file had been lifted from the conference's website and infected with reconnaissance malware known as "Seduploader", according to researchers from Cisco Talos.”

Diary Dates

ICANN 60 – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

BSG – 02.11.17

Bride Street, London, United Kingdom

GCCS – 23.11.17-21.11.17

Aero City, New Delhi, India.

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland

Manusec Europe – 07.02.18-08.02.18

Munich, Germany

Global Internet and Jurisdiction Conference 2018 – 26.02.18-28.02.18

Ottawa, Canada

RSA – 16.04.18–20.04.18

San Francisco, USA

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal