01 November 2017

Synopsis

Scroll to read full summaries with links to news articles.

A new **EU** framework will allow members to decipher and declare certain **cyber-attacks** as acts of war, justifying a response with conventional weapons.

The **National Audit Office** has published a report investigating the **NHS's** response to the **WannaCry cyber-attack**. The report concluded that the attack was, "relatively unsophisticated" but that poor management and communication within the NHS meant that the extent of damage and disruption could have been prevented.

Members of the **European Parliament** have agreed to include a human rights safeguard clause as part of a new **technology exports bill**, which if passed will make it harder for companies to export **digital surveillance** technology to other regions.

House and Senate Democrats are to introduce new legislation calling on the **Department of Commerce** to open a voluntary programme to evaluate and certify manufacturers products for **cybersecurity** credibility. The Department would also produce recommendations on **cybersecurity** benchmarks.

Following recent meetings between agencies it was announced that **Kaspersky anti-virus software** was not as deeply widespread in government as was feared. A **Homeland Security** official did not give a figure or percentage on the number of agencies using the software but stated that it was lower than 50%.

The **Senate Intelligence Committee** has ratified the reauthorisation of Section 702 of the **Foreign Intelligence Surveillance Act**, the vote will allow the US government to continue to monitor and extract internet and telecom **communications** both within the USA and beyond for the next eight years. Civil liberties groups have expressed their outrage that the vote was decided during a private session.

North Korea have lambasted claims that they were responsible for the global **WannaCry** ransomware attack, as a gross distortion of truth. They see it as a "wicked attempt" to increase international sanctions on Pyongyang.

46 million mobile records from **Malaysia's** main **telecoms** and network operators have been found for sale on the **Dark Web**. With a population of only 32 million people, concerns have been expressed that potentially every Malaysian citizen has been affected by this breach.

Saudi Arabia has created a **National Authority for Cyber Security** to provide safeguards for the country against emerging threats.

NATO's Secretary General **Jens Stoltenberg**, has met with security experts and officials in **Japan** and **South Korea** to discuss modern **security** challenges and to foster greater collaboration between the alliance and Asian countries.

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

01 November 2017

Table of Contents

Europe

Internet governance

25.10.17

Euractiv

MEPs want human rights safeguard on tech exports

Members of the European Parliament have agreed to include a human rights safeguard clause as part of a new technology exports bill, which if passed will make it harder for companies to export digital surveillance technology to other regions.

"MEPs steering a controversial export control bill through the European Parliament have agreed to apply stricter human rights safeguards for technologies that can be used for online surveillance."

"The European Commission proposed an update to the dual use regulation last year, which controls when companies can export products that can be used either as weapons or for civil purposes. The regulation was agreed in 2009, and the updated proposal adds new restrictions for firms that sell technology products that can be used for surveillance to countries outside the bloc."

30.10.17

Telegraph

EU governments to warn cyber-attacks can be an act of war

A new EU framework will allow members to decipher and declare certain cyber-attacks as acts of war, justifying a response with conventional weapons.

"European Union governments will formally state that cyber-attacks can be an act of war in a show of strength to countries such as Russia and North Korea."

"Diplomats and ambassadors in Brussels have drafted a document, obtained by The Telegraph, that represents an unprecedented deterrent aimed at countries using hackers and cyber espionage against EU members."

Cybersecurity

26.10.17

SC Media

[Anonymous targets Spanish government sites in Catalan independence controversy]

The hacking group, Anonymous have infiltrated Spain's Ministry of Public Works and Transport targeting websites in order to show their support for the Catalan independence movement. Some sites had a, "Free Catalonia" banner added across their websites.

"Hackers from the vigilante group Anonymous targeted websites run by Spain's Ministry of Public Works and Transport in support of the Catalan independence movement."

"The attacks were part of an ongoing dispute that has played out both online and in the streets over Catalan's desire for independence. Some sites were defaced to display a "Free Catalonia" slogan, while others were bombarded with DDoS attacks."

27.10.17

National Audit Office

[Investigation: Wannacry cyber-attack and the NHS]

The National Audit Office has published a report investigating the NHS's response to the WannaCry cyber-attack. The report concluded that the attack was, "relatively unsophisticated" but that poor management and communication within the NHS meant that the extent of damage and disruption could have been prevented.

"On Friday 12 May 2017 a computer virus, known as WannaCry, which encrypts data on infected computers and demands a ransom payment to allow users access, was released worldwide. WannaCry was the largest cyber-attack to affect the NHS in England, although individual trusts had been attacked before 12 May."

"The National Audit Office investigation focused on the ransomware attack's impact on the NHS and its patients; why some parts of the NHS were affected; and how the Department and NHS national bodies responded to the attack."

31.10.17

Telegraph

North Korea blasts Britain's 'wicked' claim that Pyongyang was behind the NHS hack attack

North Korea have lambasted claims that they were responsible for the global WannaCry ransomware attack, as a gross distortion of truth. They see it as a "wicked attempt" to increase international sanctions on Pyongyang.

"North Korea has slammed Britain for accusing it of being behind a global ransomware attack that hit the National Health Service, calling the allegation a "wicked attempt" to further tighten international sanctions against Pyongyang."

"A third of Britain's public hospitals were affected by the WannaCry worm in May, according to a government report."

Privacy

25.10.17

SC Media

UK to open second investigation into Equifax breach

The Financial Conduct Authority have opened an investigation into the massive Equifax data breach, alongside an existing probe by the UK's Information Commissioner's Office.

"The UK Financial Conduct Authority (FCA) has opened an investigation into the massive Equifax data breach that exposed the personal information of almost 700,000 British citizens and 145.5 million worldwide."

"The FCA's inquiry joins one already underway by the UK's Information Commissioners Office, Bloomberg News reported, along with those being run by the U.S. Federal Trade Commission, the House of Representatives' Oversight Committee, several state attorneys and the Consumer Financial Protection Bureau."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

27.10.17

The Hill

Dems push for program to secure internet-connected devices

House and Senate Democrats are to introduce new legislation calling on the Department of Commerce to open a voluntary programme to evaluate and certify manufacturers products for cybersecurity credibility. The Department would also produce recommendations on cyber security benchmarks.

"Democrats are introducing legislation directing the Department of Commerce to set up a voluntary program to certify internet-connected devices with strong cybersecurity."

"The bill, backed by Sen. Edward Markey (D-Mass.) in the Senate and Rep. Ted Lieu (D-Calif.) in the House, would set up a voluntary program in which device manufacturers can choose to have their products evaluated and certified for meeting set benchmarks on cyber and data security."

27.10.17

Time Magazine

Twitter Bans Ads From Russia Today and the Sputnik Network, Citing Election Meddling

Twitter has announced that it has banned advertisements from Russian media, including Russia Today. The statement comes after interference during the presidential election in 2016 in America and a rise in calls for actions against such interference.

"Twitter Inc. on Thursday accused Russian media outlets Russia Today (RT) and Sputnik of interfering in the 2016 U.S. election and banned them from buying ads on its network, after criticism the social network had not done enough to deter international meddling."

Cybersecurity

27.10.17

SC Media

Cybersecurity firm builds drone-based attack platform

Bishop Fox, a cyber research firm in Arizona have created an aerial drone which can hack into a network inside a building once the drone lands on the roof. It uses a local computer to infiltrate the building's networks.

"An Arizona cyber research firm has developed an aerial drone that can be used to land on a roof and then hack into a network inside the building."

"The company, Bishop Fox, said once the drone lands on the roof it is used as a "local" computer and hacks into the network, although the methodology on how this was accomplished was not discussed, according to a report by 3TV/CBS5. Once the weakness is the computer system is found the company then patches the problem."

27.10.17

NextGov

Early Kaspersky count shows anti-virus not pervasive in agencies

Following recent meetings between agencies it was announced that Kaspersky anti-virus software was not as deeply widespread in government as was feared. A Homeland Security official did not give a figure or percentage on the number of agencies using the software but stated that it was lower than 50%.

"The Homeland Security Department has not faced a deluge of Kaspersky instances as federal agencies file their first reports about how widespread the Russian anti-virus software is within government systems, a department official said Friday. Homeland Security official Michael Duffy confirmed more than half of agencies had met an Oct. 13 deadline to determine if and where the suspect anti-virus was running on their networks, but declined to offer a specific percentage."

31.10.17

The Hill

Senators release new election cybersecurity bill

The Senate Intelligence Committee have introduced a new Cyber Security Bill which is aimed to safeguard the election system from foreign interference, with a number of proposals, including bug bounty programs to be used to assess current defences.

“Sens. Martin Heinrich (D-N.M.) and Susan Collins (R-Maine) introduced a multifaceted election cybersecurity bill Tuesday, including a bug bounty program for systems manufacturers and a grant program for states to upgrade technology.”

"While the Intelligence Committee’s investigation is still ongoing, one thing is clear: The Russians were very active in trying to influence the 2016 election and will continue their efforts to undermine public confidence in democracies," said Collins in a statement celebrating the bill.”

01.11.17

AllAfrica

Consulate Raises Alarm On Increasing Cybercrime, Sees Losses Hit U.S.$6 Tn

Increasing cybercrime in Nigeria has worried the US Consulate. The Consulate General recently encouraged Nigerians to protect themselves against cyberattacks and to be more cautious and vigilant over possible attacks. It is estimated that the global community is set to lose nearly $6 trillion each year by 2021 due to cybercrime.

“The United States of America (USA) Consulate in Nigeria is worried about the increasing cybercrime rate in Nigeria and other part of the world. Referencing the Cybersecurity Ventures, which predicted that the global community will lose more than $6 trillion yearly by 2021, the US Consulate called for concerted efforts to clip its wing.”

Privacy

25.10.17

International Business Times

Tarte Cosmetics data leak: Cru3lty hackers get hold of nearly 2 million customer's data left exposed

A US based company, Tarte cosmetics has had its computers infiltrated exposing the names, addresses, emails and credit card information of nearly 2 million online customers.

"Yet another massive data leak, exposing millions of people's personal information has come to light. Tarte Cosmetics, considered to be a cult favourite beauty brand, freely exposed nearly two million customers' personal data to the public via two unsecured databases."

"New York-based Tarte's cruelty-free cosmetic products are sold at major stores including Sephora and Macy's Ulta. The company also offers customers in countries where the products aren't available in stores, the option of shopping online. The data accidentally leaked affected Tarte's online customers. Sensitive data of both US and international customers, who shopped online between 2008 and 2017, was left publicly exposed via two unsecured MongoDB databases."

27.10.17

POLITICO

Facebook rolls out new ad policy changes ahead of Russia hearings

Mark Zuckerberg has announced that he will make political ads more transparent for users, after several congressional complaints. Facebook will indicate who paid for political advertisement, and will verify whether those purchasing the ads are credible.

"Facebook on Friday unveiled changes to its advertising platform designed to protect election integrity, as the nation's top internet companies rush to show they're taking congressional complaints seriously ahead of a slew of hearings on Russian interference."

"The new policies announced by Facebook and Twitter this week are part of a campaign to show they're capable of policing their own networks. Both companies along with Google face a grilling from lawmakers who've become convinced Silicon Valley was willfully ignorant of Russian efforts to use social media to manipulate American democracy."

27.10.17

SC Media

Senate intel committee votes behind closed doors bill to re-up Section 702

The Senate Intelligence Committee has ratified the reauthorisation of Section 702 of the Foreign Intelligence Surveillance Act, the vote will allow the US government to continue to monitor and extract internet and telecom communications both within the USA and beyond for the next eight years. Civil liberties groups have expressed their outrage that the vote was decided during a private session.

"While a bill approved behind closed doors by the Senate Intelligence Committee to reauthorize Section 702 of the Foreign Intelligence Surveillance Act (FISA) included provisions that would throttle the government's ability to view emails and other communications of Americans, it would codify illegal practices, according to the American Civil Liberties Union (ACLU)."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

30.10.17

Security Asia

PwC: Companies are failing to prepare effectively for cyberattacks

A report by PWC into cybersecurity in Singapore has found that while companies are aware of cyber threats, they remain significantly unprepared to deal with them. 39% said that they do not have an overall information security strategy, 36% said they have no cyber security trainee programme for staff and 44% do not have a process to respond to incidents.

"Massive cybersecurity breaches have become almost commonplace, regularly grabbing headlines that alarm consumers and leaders. But for all of the attention such incidents have attracted in recent years, many organisations worldwide still struggle to comprehend and manage emerging cyber risks in an increasingly complex digital society."

30.10.17

NATO

NATO Secretary General arrives in Japan

As part of his Asia tour, NATO's Secretary General Jens Stoltenberg, has met with security experts in Tokyo to discuss modern security challenges and called for NATO-Japan cooperation on several priorities including cyber defence.

"Starting his first official visit to East Asia as Secretary General, Mr. Stoltenberg met with security experts at a roundtable sponsored by the Sasakawa Peace Foundation on Monday morning (30 October 2017). The discussion focused on regional security challenges – particularly North Korea – and how to enhance NATO-Japan cooperation."

31.10.17

Telegraph

North Korea blasts Britain's 'wicked' claim that Pyongyang was behind the NHS hack attack

North Korea have lambasted claims that they were responsible for the global WannaCry ransomware attack, as a gross distortion of truth. They see it as a "wicked attempt" to increase international sanctions on Pyongyang.

"North Korea has slammed Britain for accusing it of being behind a global ransomware attack that hit the National Health Service, calling the allegation a "wicked attempt" to further tighten international sanctions against Pyongyang."

"A third of Britain's public hospitals were affected by the WannaCry worm in May, according to a government report."

01.11.17

NATO

NATO Secretary General arrives in the Republic of Korea

General Jens Stoltenberg, NATO's Secretary General has visited South Korea to talk about growing security challenges. Following their discussions, the Secretary General and North Korea Foreign Minister Kang Kyung-wha signed a new partnership agreement to increase cooperation in cyber defence.

"Meeting with Foreign Minister Kang Kyung-wha, the Secretary General praised the Republic of Korea's contributions to NATO's mission to Afghanistan and efforts to combat piracy off the Horn of Africa. The two also discussed shared concerns over North Korea. Mr. Stoltenberg condemned North Korea's nuclear and ballistic missile tests, which he said undermine regional and international security."

"Following their meeting, the Secretary General and Foreign Minister Kang Kyung-wha signed a new partnership programme between NATO and the Republic of Korea. This will promote political dialogue and practical cooperation in a number of priority areas, including non-proliferation, cyber defence and counter-terrorism."

Privacy

31.10.17

SC Media

Update: Possibly everyone in Malaysia had their mobile records stolen

46 million mobile records from Malaysia's main telecoms and network operators have been found for sale on the Dark Web. With a population of only 32 million people, concerns have been expressed that potentially every Malaysian citizen has been affected by this breach.

"In a country with a population of 32 million, 46 million subscriber records from Malaysia's main telecoms and network operators have been found for sale on the Dark Web. This suggests everyone was affected, although that the data would also cover people with multiple mobile numbers and likely include inactive or temporary numbers used by visitors to the country."

"Local reports say that the data – which includes user-names, prepaid and post-paid phone number, addresses, customer details and SIM card data - may have been successfully traded before it was discovered, having already been in circulation in underground forums."

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

27.10.17

Time Magazine

Twitter Bans Ads From Russia Today and the Sputnik Network, Citing Election Meddling

Twitter has announced that it has banned advertisements from Russian media, including Russia Today. The statement comes after interference during the presidential election in 2016 in America and a rise in calls for actions against such interference.

"Twitter Inc. on Thursday accused Russian media outlets Russia Today (RT) and Sputnik of interfering in the 2016 U.S. election and banned them from buying ads on its network, after criticism the social network had not done enough to deter international meddling."

Cybersecurity

27.10.17

NextGov

Early Kaspersky count shows anti-virus not pervasive in agencies

Following recent meetings between agencies it was announced that Kaspersky anti-virus software was not as deeply widespread in government as was feared. A Homeland Security official did not give a figure or percentage on the number of agencies using the software but stated that it was lower than 50%.

"The Homeland Security Department has not faced a deluge of Kaspersky instances as federal agencies file their first reports about how widespread the Russian anti-virus software is within government systems, a department official said Friday. Homeland Security official Michael Duffy confirmed more than half of agencies had met an Oct. 13 deadline to determine if and where the suspect anti-virus was running on their networks, but declined to offer a specific percentage."

01.11.17

Reuters

[Saudi Arabia sets up new authority for cyber security]

Saudi Arabia has created a National Authority for Cyber Security to provide safeguards for the country against emerging threats.

"Saudi Arabia has set up a new authority for cyber security and named its minister of state Musaed al-Aiban its chairman, strengthening security in the world's largest oil exporter, a royal decree said."

"The National Authority for Cyber Security will be made up of the head of state security, the head of intelligence, the deputy interior minister and assistant to the minister of defense, SPA said late on Tuesday."

31.10.17

AllAfrica

[Deputy Minister Stella Ndabeni-Abrahams Conducts Cybersecurity Awareness Portal Launch in Polokwane]

Ms Ndabeni-Abrahams, the Deputy Minister of Telecommunications in the South African Government, has announced the launch of a Cybersecurity Awareness Portal for the 3rd of November.

"The Deputy Minister of Telecommunications and Postal Services, Ms. Stella Ndabeni-Abrahams, will on the 3rd November 2017, conduct the first provincial launch of the Cybersecurity Awareness Portal in Polokwane, Limpopo.

International Cybersecurity Awareness Month is an annual campaign to raise awareness about the importance of Cybersecurity; and is globally recognised annually in October. South Africa has adopted a National Cybersecurity Policy Framework which mandates the Department of Telecommunications and Postal Services (DTPS) and the Cybersecurity Hub to develop and implement Cybersecurity Awareness programs."

31.10.17

SecurityBrief

[ANU establishes Australia's first 'Cyber Institute']

A new Cyber Institute has been created at the Australian National University. The Institute will engage in research on cybersecurity issues, bringing experts in from a number of different areas within cybersecurity.

"The Australian National University officially established the country's first interdisciplinary Cyber Institute, which was announced as part of an Australian cybersecurity and innovation delegation's visit to Israel last week. Dan Tehan, the Minister Assisting the Prime Minister on Cyber Security, led the delegation and welcomed the announcement as part of its visit to Israel.

The ANU Cyber Institute will bring together experts from various disciplines. They will conduct research across cybersecurity and innovation that will help to 'shape the nation's future'. ANU Vice Chancellor Professor Brian Schmidt says the Institute is the first of its kind in Australia."

01.11.17

AllAfrica

Consulate Raises Alarm On Increasing Cybercrime, Sees Losses Hit U.S.$6 Tn

Increasing cybercrime in Nigeria has worried the US Consulate. The Consulate General recently encouraged Nigerians to protect themselves against cyberattacks and to be more cautious and vigilant over possible attacks. It is estimated that the global community is set to lose nearly $6 trillion each year by 2021 due to cybercrime.

"The United States of America (USA) Consulate in Nigeria is worried about the increasing cybercrime rate in Nigeria and other part of the world. Referencing the Cybersecurity Ventures, which predicted that the global community will lose more than $6 trillion yearly by 2021, the US Consulate called for concerted efforts to clip its wing."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

Global Institutions

30.10.17

NATO

NATO Secretary General arrives in Japan

As part of his Asia tour, NATO's Secretary General Jens Stoltenberg, has met with security experts in Tokyo to discuss modern security challenges and called for NATO-Japan cooperation on several priorities including cyber defence.

"Starting his first official visit to East Asia as Secretary General, Mr. Stoltenberg met with security experts at a roundtable sponsored by the Sasakawa Peace Foundation on Monday morning (30 October 2017). The discussion focused on regional security challenges – particularly North Korea – and how to enhance NATO-Japan cooperation."

01.11.17

NATO

NATO Secretary General arrives in the Republic of Korea

General Jens Stoltenberg, NATO's Secretary General has visited South Korea to talk about growing security challenges. Following their discussions, the Secretary General and North Korea Foreign Minister Kang Kyung-wha signed a new partnership agreement to increase cooperation in cyber defence.

"Meeting with Foreign Minister Kang Kyung-wha, the Secretary General praised the Republic of Korea's contributions to NATO's mission to Afghanistan and efforts to combat piracy off the Horn of Africa. The two also discussed shared concerns over North Korea. Mr. Stoltenberg condemned North Korea's nuclear and ballistic missile tests, which he said undermine regional and international security."

"Following their meeting, the Secretary General and Foreign Minister Kang Kyung-wha signed a new partnership programme between NATO and the Republic of Korea. This will promote political dialogue and practical cooperation in a number of priority areas, including non-proliferation, cyber defence and counter-terrorism."

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