IEEE GLOBAL INTERNET POLICY MONITOR

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

15 November 2017

Synopsis

Scroll to read full summaries with links to news articles.

Freedom House has published a new report focused on **internet access** and freedom, finding that only 23% of the world's population have access to truly free internet.

The UK's **National Cyber Security Centre** has now confirmed that **Russia** has attempted to hack into the **UK's** energy, media and telecommunications systems.

The **Kantara Initiative** have called for the introduction of open **standards** for **data protection** to reduce the burden of incoming **General Data Protection Regulations** to be introduced by the **EU** next year.

The Trump administration have released revised rules, to provide greater **transparency** in how federal agencies disclose **cybersecurity** flaws, following criticism that the **US** Government had kept quiet in relation to commercial cyber vulnerabilities so that it could use said vulnerabilities for its own purposes.

The U.S. House Judiciary Committee have reauthorized and reformed section 702, of the **Foreign Intelligence Surveillance Act (FISA**). The reforms will require federal authorities to receive a court order from the Foreign Intelligence Surveillance Court before accessing **data** relating to **US** residents.

At a recent **Indian** cybersecurity conference, a number of speakers from the country's financial services stated that the country needed to focus more on **cybersecurity**, particularly within companies that have largely focused on just IT security.

China has once again been ranked as the worst nation in the world for its **internet freedom** by **Freedom House**. The report ranks countries on how free citizens are to access the internet and its information; some countries such as **North Korea** were not included.

A recent report has revealed that **Ghana** could be losing around $30-60 million every year because of **cyber-attacks** and fraud. The continued digitalisation of banking and telecommunication has allowed for such issues to rise dramatically.

As the **Russian** threat gets more prominent, **NATO's** defence ministers have decided for the first time since the Cold War, to expand its operations to help boost **cybersecurity** responses to aggression from Moscow.

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

15 November 2017

Table of Contents

Europe

Internet governance

08.11.17

Kaspersky

Kaspersky Lab and Council of Europe Jointly Pledge to Protect Citizens' Human Rights Online

The Council of Europe has signed an agreement with Kaspersky Lab and several world leading technology companies to pledge their commitment to promote an open and safe internet.

The Council of Europe today signed an agreement with Kaspersky Lab and a number of the world's leading technology companies to jointly pledge to promote an open and safe Internet.

During a ceremony in Strasbourg, France on the first day of the World Forum for Democracy, Anton Shingarev, vice president of public affairs at Kaspersky Lab, and Council of Europe secretary general Thorbjørn Jagland signed the agreement, which is designed to extend the protection of human rights, democracy and the rule of law to the Internet.

10.11.17

Computer Weekly

Open standards will ease GDPR risk, says Kantara

The Kantara Initiative, have called for the introduction of open standards for data protection to reduce the burden of incoming General Data Protection Regulations to be introduced by the EU next year.

"Open standards will help organisations comply with new EU data protection regulations, while ensuring interoperability and a good user experience, according to a global standardisation group."

"The use of open standards can help organisations comply with requirements of the EU's General Data Protection Regulation (GDPR), says Colin Wallis, Executive Director of the Kantara Initiative."

15.11.17

The Times

Russia used Twitter bots and trolls ‘to disrupt’ Brexit vote

A new report from the Times has revealed that Russia used hundreds of fake accounts to promote Brexit ahead of the EU referendum. 150,000 Russian accounts posted more than 45,000 messages relating to Brexit in just 48 hours, in an attempt to influence the outcome.

“Russian Twitter accounts posted more than 45,000 messages about Brexit in 48 hours during last year’s referendum in an apparently co-ordinated attempt to sow discord, The Times can reveal.”

“More than 150,000 accounts based in Russia, which had previously confined their posts to subjects such as the Ukrainian conflict, switched attention to Brexit in the days leading up to last year’s vote, according to research for an upcoming paper by data scientists at Swansea University and the University of California, Berkeley.”

Cybersecurity

08.11.17

Scottish Government

Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland-Public Sector Action Plan 2017-18

The Scottish Government has published a cybersecurity action plan, to help public sector institutions improve their cyber resiliency.

“Whether in the public, private or third sectors, our ability to inform and interact with citizens and consumers is being transformed by the digital world. Scottish public bodies, businesses and charities are developing ambitious plans to embrace these opportunities.”

“Trust and confidence are fundamental to the success of these plans. As the threat from cyber criminals and other hostile actors in cyberspace grows, we must do all we can to ensure our digital services are as secure as possible, and can recover quickly when cyber-attacks succeed.”

09.11.17

The Straits Times

Facing Russian threat, NATO expands operations, focuses on cybersecurity

As the Russian threat gets more prominent, NATO's defence ministers have decided for the first time since the Cold War, to expand its operations to help boost cybersecurity responses to aggression from Moscow.

"As the spectre of conflict with Russia looms over Europe, NATO defence ministers have decided to expand the alliance's operations for the first time since the Cold War, sharpen its focus on cyber operations, and boost their powers to respond to Kremlin aggression."

"The moves came as tensions with Russia remain the highest they have been in the nearly three decades since the end of the Cold War. Secretary of Defence James Mattis briefed fellow defence ministers on Wednesday (Nov 8) about Russian violations of the Intermediate Range Nuclear Forces Treaty, underlining the nuclear risk that is a worst-case consequence of the bitter back-and-forth."

14.11.17

The Hill

Russia-type meddling found in 18 nations' elections last year: report

The Annual Freedom House, "Freedom on the Net" report has found that other than the US, 18 nations holding elections in 2016 suffered from attacks similar to the Russian social media campaign.

"At least 18 nations holding elections in 2016 experienced some kind of information attacks similar to the Russian social media campaign in the U.S., according to a new report."

"The annual Freedom House "Freedom on the Net" report, released Tuesday, tabulates this kind of election interference into its nation-by-nation rankings of internet freedom, under the theory that diluting authentic speech stifles legitimate debate."

14.11.17

Reuters

Dutch central bank sets up 'friendly' hacking team to attack own banks: report

A cybersecurity team of experts have gathered in the Netherlands to attack the country's own financial infrastructure in order to test and improve its defence systems to help response to future threats.

"The Netherlands' central bank (DNB) is setting up a team of cyber security experts and hackers to attack the country's own financial infrastructure in order to test and improve its defenses, Het Financieele Dagblad reported on Tuesday."

"In an interview with the paper, the bank's Payments and Infrastructure chief Petra Hielkema said the team would be carrying out secret attacks on banks, markets and clearing houses."

14.11.17

Vice News

Russian cybersecurity firm Kaspersky wants to run your next election

Russian cybersecurity company Kaspersky have released a new cybersecurity tool, Polys, to support the protection of online and digital voting platforms through the use of blockchain. Whilst Kaspersky has approached a number of European and Asian countries with the product, the company has ruled out introducing the product in the United States as a result of continuing suspicion by US authorities relating to Kaspersky's alleged ties to Russian Intelligence.

"Kaspersky, the Russian cybersecurity company accused of helping the Kremlin spy on the U.S. intelligence agencies as part of its 2016 election meddling, has launched a new product aimed at helping secure online voting and make elections more transparent and open.

Polys, an online voting platform built using the same blockchain technology that underpins bitcoin, allows anyone to conduct "secure, anonymous, and scalable online voting with results that cannot be altered by participants or organizers," the company said."

15.11.17

Business Insider UK

Russia tried to hack UK media, telecoms, and energy

The UK's National Cyber Security Centre has now confirmed that Russia has attempted to hack into the UK's energy, media and telecommunications systems.

"The head of one of Britain's leading government cybersecurity agencies has confirmed that Russia tried to hack the UK media, telecommunications system, and energy sector in the past year.

Ciaran Martin, the CEO of the National Cyber Security Centre (NCSC), will say at the Times Tech Summit on Wednesday: 'I can't get into precise details of intelligence matters, but I can confirm that Russian interference, seen by the National Cyber Security Centre over the past the year, has included attacks on the UK media, telecommunication and energy sectors.'"

Privacy

No new items of relevance

Internet Inclusion

14.11.17

NextGov

Only 23% of the World has a free and open internet

Freedom House has published a new report focused on internet access and freedom, finding that only 23% of the world's population have access to truly free internet.

"Though more people around the world are going online than ever before, almost two-thirds of them live in areas where the government has taken steps to limit freedom on the internet, a study found.

Less than a quarter of worldwide internet users have access to a "free" internet, while 64 percent reside in countries where the internet is designated as "partly free" or "not free," according to the 2017 Freedom of the Net report by independent watchdog group Freedom House. Citizens in 32 of the 65 countries analyzed in the report saw their online freedom decline from last year, including the United States."

United States of America

Internet governance

15.11.7

whitehouse.gov

[Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do]

The Trump administration have released revised rules, to provide greater transparency in how federal agencies disclose cybersecurity flaws, following criticism that the US Government had kept quiet in relation to commercial cyber vulnerabilities so that it could use said vulnerabilities for its own purposes.

"There can be no doubt that America faces significant risk to our national security and public safety from cyber threats. During the past 25 years, we have moved much of what we value to a digital format and stored it in Internet-connected devices that are vulnerable to exploitation."

"This risk is increasing as our dependence on technology and the data we store continues to grow such that technology now connects nearly every facet of our society and the critical services that sustain our way of life. This fact is not lost on criminal actors and adversarial nation states who discover and exploit existing flaws in software, hardware, and the actions of legitimate users to steal, disrupt, and destroy data and services critical to our way of life."

14.11.17

The Hill

[More than 94 percent of federal agencies on schedule with Kaspersky purge]

The Department of Homeland Security has announced that as a review of federal computer systems, 95 of 102 agencies have now uninstalled programs from Kaspersky Lab.

"Only six out of 102 federal agencies failed to meet the first deadline in the Department of Homeland Security's (DHS) directive to identify and uninstall all Kaspersky Lab software, a House Science, Space and echnology subcommittee heard Tuesday."

"A small number of very small agencies" are receiving DHS help to complete the first stage of the directive, testified Jeanette Manfra, assistant secretary for

cybersecurity and communications at DHS's National Protection and Programs Directorate."

Cybersecurity

09.11.17

The Straits Times

Facing Russian threat, NATO expands operations, focuses on cybersecurity

As the Russian threat gets more prominent, NATO's defence ministers have decided for the first time since the Cold War, to expand its operations to help boost cybersecurity responses to aggression from Moscow.

"As the spectre of conflict with Russia looms over Europe, NATO defence ministers have decided to expand the alliance's operations for the first time since the Cold War, sharpen its focus on cyber operations, and boost their powers to respond to Kremlin aggression."

"The moves came as tensions with Russia remain the highest they have been in the nearly three decades since the end of the Cold War. Secretary of Defence James Mattis briefed fellow defence ministers on Wednesday (Nov 8) about Russian violations of the Intermediate Range Nuclear Forces Treaty, underlining the nuclear risk that is a worst-case consequence of the bitter back-and-forth."

09.11.17

SC Media

Former Yahoo Chief Executive Mayer testified before Congress, blamed Russia

Marissa Mayer, the former Chief Executive of Yahoo has apologized to the near 3 billion people who had their credentials stolen, while testifying to Congress that Russian agents were to blame for at least one of the attacks.

"Former Yahoo Chief Executive Marissa Mayer apologized on Wednesday for the two massive data breaches at Yahoo that occurred during her tenure and resulted in 3 billion credentials being stolen, blaming Russian agents for at least one of the breaches."

"Unfortunately, while all our measures helped Yahoo successfully defend against the barrage of attacks by both private and state-sponsored hackers, Russian agents intruded on our systems and stole our users' data," Mayer said in her testimony before a Senate Commerce, Science and Transportation hearing."

13.11.17

The Independent

[Donald Trump insists Vladimir Putin was telling the truth in denying Russian meddling in US election]

During an Asia-Pacific summit, US President Donald Trump has met with Russian counterpart Vladimir Putin. Both leaders refused to acknowledge the US intelligence agency findings which blamed Russia for meddling in the US election.

“President Donald Trump said that President Vladimir Putin had assured him again Saturday that Russia did not interfere in the 2016 presidential campaign, and indicated that he believed Putin's sincerity, drawing immediate criticism from lawmakers and former intelligence officials who assessed that the meddling took place.”

“I asked him again,” Trump said after what he described as several brief, informal chats with Putin in Danang, Vietnam, where they were attending a regional conference. “You can only ask so many times... He said he absolutely did not meddle in our election. He did not do what they are saying he did.”

14.11.17

The Hill

[Russia-type meddling found in 18 nations' elections last year: report]

The Annual Freedom House, “Freedom on the Net” report has found that other than the US, 18 nations holding elections in 2016 suffered from attacks similar to the Russian social media campaign.

“At least 18 nations holding elections in 2016 experienced some kind of information attacks similar to the Russian social media campaign in the U.S., according to a new report.”

“The annual Freedom House “Freedom on the Net” report, released Tuesday, tabulates this kind of election interference into its nation-by-nation rankings of internet freedom, under the theory that diluting authentic speech stifles legitimate debate.”

14.11.17

The Hill

U.S. government shares technical details on North Korean hacking campaign

The US Government released a technical alert about North Korean cyber-attacks which have targeted, financial industries, telecommunications and the aerospace industry. They warned that the country was using a malware known as "FALLCHILL" to unlawfully infiltrate network systems.

"The U.S. government on Tuesday issued a technical alert about cyber-attacks it said are sponsored by the North Korean government that have targeted the aerospace, telecommunications and financial industries since 2016."

"The alert, from the FBI and Department of Homeland Security, said North Korean hackers were using a type of malware known as "FALLCHILL" to gain entry to computer systems and compromise network systems."

14.11.17

Vice News

Russian cybersecurity firm Kaspersky wants to run your next election

Russian cybersecurity company Kaspersky have released a new cybersecurity tool, Polys, to support the protection of online and digital voting platforms through the use of blockchain. Whilst Kaspersky has approached a number of European and Asian countries with the product, the company has ruled out introducing the product in the United States as a result of continuing suspicion by US authorities relating to Kaspersky's alleged ties to Russian Intelligence.

"Kaspersky, the Russian cybersecurity company accused of helping the Kremlin spy on the U.S. intelligence agencies as part of its 2016 election meddling, has launched a new product aimed at helping secure online voting and make elections more transparent and open.

Polys, an online voting platform built using the same blockchain technology that underpins bitcoin, allows anyone to conduct "secure, anonymous, and scalable online voting with results that cannot be altered by participants or organizers," the company said."

Privacy

09.11.17

SC Media

Legislation adding privacy protections to FISA passes through committee

The U.S. House Judiciary Committee have reauthorized and reformed section 702, of the Foreign Intelligence Surveillance Act (FISA). The reforms will require federal authorities to receive a court order from the Foreign Intelligence Surveillance Court before accessing data relating to US residents.

"The U.S. House Judiciary Committee on Wednesday approved the USA Liberty Act, which reauthorizes Section 702 of the Foreign Intelligence Surveillance Act (FISA), but with new privacy protections."

"FISA allows U.S. government agencies to conduct surveillance on the communications of non-U.S. persons located on foreign soil. The bipartisan bill, which passed 27-8, clarifies that U.S. authorities may query "702" surveillance databases for communications content if it is for national security reasons, but need a probable cause-based order from the Foreign Intelligence Surveillance Court to view and disseminate such information for the purpose of finding criminal evidence (with two notable exceptions)."

14.11.17

SC Media

In historic decision, FISA court allows NSA surveillance transparency lawsuit to continue

The Foreign Intelligence Surveillance Court ruled last Thursday that the court could be challenged to publicly disclose secret justifications behind the NSA's electronic surveillance program.

"In a historic en banc decision, the U.S. Foreign Intelligence Surveillance Court ruled last week that there is sufficient standing to proceed with a lawsuit that could require the court to publicly disclose the secret justifications behind the NSA's electronic surveillance program that was exposed by Edward Snowden."

"Never before have all 11 FISC judges collectively heard a case in an en banc review. The 6-5 ruling reverses a previous FISA court decision by FISC Judge Rosemary Collyer, who had ruled that the ACLU and Yale Law School's Media Freedom and Information Access Clinic lacked the necessary standing to pursue their case in court."

Internet Inclusion

14.11.17

NextGov

Only 23% of the World has a free and open internet

Freedom House has published a new report focused on internet access and freedom, finding that only 23% of the world's population have access to truly free internet.

"Though more people around the world are going online than ever before, almost two-thirds of them live in areas where the government has taken steps to limit freedom on the internet, a study found.

Less than a quarter of worldwide internet users have access to a "free" internet, while 64 percent reside in countries where the internet is designated as "partly free" or "not free," according to the 2017 Freedom of the Net report by independent watchdog group Freedom House. Citizens in 32 of the 65 countries analyzed in the report saw their online freedom decline from last year, including the United States."

Pan-Asia

Internet governance

10.11.17

Network Asia

Industry Transformation Map launched for Singapore's infocomm media sector

The Infocomm Media Development Authority (IMDA) has released the Industry Transformation Map (ITM) which seeks to help Singapore harness the digital economy. It will help the country prepare in several ways including by investing in cybersecurity and Data Analytics.

"The Infocomm Media Development Authority (IMDA) has released the Industry Transformation Map (ITM) for the Infocomm Media sector, which outlines the strategies to prepare Singapore for the digital economy."

"Speaking at the launch of the ITM, Minister for Communications and Information Dr Yaacob Ibrahim, said the ITM aims to grow the ICM industry's value-add by around 6% annually (almost twice as fast as the overall economy). It is also expected to employ more than 210,000 workers (from approximately 194,000 workers in 2016), and create more than 13,000 new PMET jobs by 2020."

15.10.17

Shanghaiist

China ranks dead last in internet freedom survey for second straight year

China has once again been ranked as the worst nation in the world for its internet freedom by Freedom House. The report ranks countries on how free citizens are to access the internet and its information; some countries such as North Korea were not included.

"For the second year in a row, *a report released by Freedom House on internet freedom has listed China dead last out of all nations surveyed. The* report, *which rates freedom on sale of 1 (free) to 100 (not free) gave China a score of 88, the same score that it received last year, once again ranking the country below Syria, Iraq, Ethiopia, Uzbekistan, Cuba and every other country surveyed. In 2014, China came in third from last place."*

"It's important to note that a number of nations were not included in the survey, most notably North Korea, which would have certainly ranked lower than China."

Cybersecurity

09.11.17

Computer Weekly

Malaysia partners Huawei in cybersecurity

Malaysia has announced that a new committee will convene twice a year to discuss and debate the different cybersecurity threats and issues facing the nation. The country has teamed with Huawei, a Chinese tech company, in order to further its cybersecurity capability.

“A joint steering committee will meet twice a year to address cyber security issues, among other measures to shore up Malaysia’s cyber security capabilities. The Malaysian government will work with Chinese technology giant Huawei to deepen its capabilities in combatting cyber threats that have been plaguing the country in recent months.

As part of the collaboration, Malaysia’s cyber security agency, CyberSecurity Malaysia, will establish a joint steering committee with Huawei that will meet twice a year to discuss issues such as cyber security standards and approaches in fending off cyber threats*. A taskforce from both organisations will be tasked to execute all decisions made by the committee.”*

10.11.17

The Indian Express

Cybersecurity conference: ‘Need for India to move from IT security to cybersecurity’

At a recent Indian cybersecurity conference, a number of speakers from the country’s financial services stated that the country needed to focus more on cybersecurity, particularly within companies that have largely focused on just IT security.

“Speakers at a cyber security conference on Thursday said private organisations must find a balance between setting the law into motion and managing their reputations in the face of constant threat from cyber attacks. On the first day of the Cyber Security Summit organised by the Confederation of Indian Industry, the panelists insisted on the need for India to move on from IT security to cyber security. “We don’t have a cyber security mindset. We are only doing IT security. People still don’t understand cyber risks to an organisation,” said Nilesh Mhatre, Chief Information Officer, HSBC India.”

13.11.17

OpenGovAsia

MAS seeks to strengthen financial sector cybersecurity through collaboration with FS-ISAC and ABS

Ravi Menon, Managing Director of the Monetary Authority of Singapore has announced that the financial sector would be implementing several measures to strengthen cyber defences. These include a new cyber threat information Centre to deal with emerging threats.

"Speaking at the Singapore FinTech Festival, Mr. Ravi Menon, Managing Director of MAS (Monetary Authority of Singapore), announced several measures for strengthening cyber defence in the financial services sector."

"Mr. Menon said, "As we go more digital and online, cyber risks will mount. And if these risks are not managed well, public trust and confidence in technology will suffer. To fully harness the benefits of digital technology, we must build robust cyber defences and have effective remediation plans when things go wrong."

13.11.17

SC Media

KISA fingers North Korea for boosting cyberattacks

The South Korean Internet & Security Agency (KISA) has published a report stating that in the first nine months of 2017, 5,166 cases of ransomware attacks were reported, with victims tending to be cryptocurrency markets. KISA has blamed North Korea for the sharp increase in attacks.

"The Korea Internet & Security Agency (KISA) has issued a new report stating that 5,166 cases of ransomware were reported during the first nine month of 2017 with attacks targeting cryptocurrency markets on the rise."

"The number of incidents, which KISA is attributing to North Korea, represents an almost 4-fold increase from the 1,438 that took place during the same period in 2016, reported the South Korean Yonhapnews.com. KISA, which suspects the attackers to be from North Korea, said the attacks included attempts in July and August to infiltrate South Korean bitcoin exchanges along with an attempt to manipulate digital wallet passwords in order to steal the cryptocurrency."

14.11.17

The Hill

Russia-type meddling found in 18 nations' elections last year: report

The Annual Freedom House, “Freedom on the Net” report has found that other than the US, 18 nations holding elections in 2016 suffered from attacks similar to the Russian social media campaign.

“At least 18 nations holding elections in 2016 experienced some kind of information attacks similar to the Russian social media campaign in the U.S., according to a new report.”

“The annual Freedom House “Freedom on the Net” report, released Tuesday, tabulates this kind of election interference into its nation-by-nation rankings of internet freedom, under the theory that diluting authentic speech stifles legitimate debate.”

14.11.17

The Hill

U.S. government shares technical details on North Korean hacking campaign

The US Government has released a technical alert about North Korean cyber-attacks which have targeted, financial industries, telecommunications and the aerospace industry. They warned that the country has been using malware known as “FALLCHILL” to unlawfully infiltrate network systems.

“The U.S. government on Tuesday issued a technical alert about cyber attacks it said are sponsored by the North Korean government that have targeted the aerospace, telecommunications and financial industries since 2016.”

“The alert, from the FBI and Department of Homeland Security, said North Korean hackers were using a type of malware known as “FALLCHILL” to gain entry to computer systems and compromise network systems.”

15.11.17

News18

Centre to Offer Grants to Start-Ups For Cybersecurity Solutions

India is hoping to improve its cybersecurity protections by offering, ‘Challenge Grants’ to encourage cybersecurity start-ups to create new solutions in the sector. The MEIT and Data Security Council of India will work together in order to ensure the success of the new programme.

“The Ministry of Electronics and Information Technology is in the process of working with the Data Security Council of India to offer Challenge Grants for cybersecurity to encourage start-ups to develop innovative technologies, IT Minister Ravi Shankar Prasad said on Wednesday. "Rs 5 crore in grant will be for growth start-ups to come up with new solutions in the field of cybersecurity," Prasad said at the first Asia Pacific Computer Emergency Response Team (APCERT) Open Conference in India, the first in South Asia.”

Privacy

No new items of relevance

Internet Inclusion

09.11.17

Computer Weekly

Bangalore offers the best ecosystem for digital transformation, says Economist report

The Indian city of Bangalore has been crowned as the number one city for digital transformation for businesses, as revealed by the Economist Intelligence Unit.

“Bangalore ranked as the number one location for businesses looking to access the right ecosystem to support digital transformation. Indian city Bangalore has the best environment for businesses to transform digitally, according to research of 45 global cities by the Economist Intelligence Unit (EIU). Mumbai and New Delhi were also ranked in the top four locations.

14.11.17

NextGov

Only 23% of the World has a free and open internet

Freedom House has published a new report focused on internet access and freedom, finding that only 23% of the world’s population have access to truly free internet.

“Though more people around the world are going online than ever before, almost two-thirds of them live in areas where the government has taken steps to limit freedom on the internet, a study found.

Less than a quarter of worldwide internet users have access to a “free” internet, while 64 percent reside in countries where the internet is designated as “partly free” or “not free,” according to the 2017 Freedom of the Net report by independent watchdog group Freedom House. Citizens in 32 of the 65 countries analyzed in the report saw their online freedom decline from last year, including the United States.”

Rest of the World

Internet governance

15.11.17

The Times

Russia used Twitter bots and trolls 'to disrupt' Brexit vote

A new report from the Times has revealed that Russia used hundreds of fake accounts to promote Brexit ahead of the EU referendum. 150,000 Russian accounts posted more than 45,000 messages relating to Brexit in just 48 hours, in an attempt to influence the outcome.

"Russian Twitter accounts posted more than 45,000 messages about Brexit in 48 hours during last year's referendum in an apparently co-ordinated attempt to sow discord, The Times can reveal."

"More than 150,000 accounts based in Russia, which had previously confined their posts to subjects such as the Ukrainian conflict, switched attention to Brexit in the days leading up to last year's vote, according to research for an upcoming paper by data scientists at Swansea University and the University of California, Berkeley."

Cybersecurity

09.11.17

The Straits Times

Facing Russian threat, NATO expands operations, focuses on cybersecurity

As the Russian threat gets more prominent, NATO's defence ministers have decided for the first time since the Cold War, to expand its operations to help boost cybersecurity responses to aggression from Moscow.

"As the spectre of conflict with Russia looms over Europe, NATO defence ministers have decided to expand the alliance's operations for the first time since the Cold War, sharpen its focus on cyber operations, and boost their powers to respond to Kremlin aggression."

"The moves came as tensions with Russia remain the highest they have been in the nearly three decades since the end of the Cold War. Secretary of Defence James Mattis briefed fellow defence ministers on Wednesday (Nov 8) about

Russian violations of the Intermediate Range Nuclear Forces Treaty, underlining the nuclear risk that is a worst-case consequence of the bitter back-and-forth."

09.11.17

SC Media

Former Yahoo Chief Executive Mayer testified before Congress, blamed Russia

Marissa Mayer, the former Chief Executive of Yahoo has apologized to the near 3 billion people who had their credentials stolen, while testifying to Congress that Russian agents were to blame for at least one of the attacks.

"Former Yahoo Chief Executive Marissa Mayer apologized on Wednesday for the two massive data breaches at Yahoo that occurred during her tenure and resulted in 3 billion credentials being stolen, blaming Russian agents for at least one of the breaches."

"Unfortunately, while all our measures helped Yahoo successfully defend against the barrage of attacks by both private and state-sponsored hackers, Russian agents intruded on our systems and stole our users' data," Mayer said in her testimony before a Senate Commerce, Science and Transportation hearing."

13.11.17

The Independent

Donald Trump insists Vladimir Putin was telling the truth in denying Russian meddling in US election

During an Asia-Pacific summit, US President Donald Trump has met with Russian counterpart Vladimir Putin. Both leaders refused to acknowledge the US intelligence agency findings which blamed Russia for meddling in the US election.

"President Donald Trump said that President Vladimir Putin had assured him again Saturday that Russia did not interfere in the 2016 presidential campaign, and indicated that he believed Putin's sincerity, drawing immediate criticism from lawmakers and former intelligence officials who assessed that the meddling took place."

"I asked him again," Trump said after what he described as several brief, informal chats with Putin in Danang, Vietnam, where they were attending a regional conference. "You can only ask so many times... He said he absolutely did not meddle in our election. He did not do what they are saying he did."

14.11.17

The Hill

Russia-type meddling found in 18 nations' elections last year: report

The Annual Freedom House, “Freedom on the Net” report has found that other than the US, 18 nations holding elections in 2016 suffered from attacks similar to the Russian social media campaign.

“At least 18 nations holding elections in 2016 experienced some kind of information attacks similar to the Russian social media campaign in the U.S., according to a new report.”

“The annual Freedom House “Freedom on the Net” report, released Tuesday, tabulates this kind of election interference into its nation-by-nation rankings of internet freedom, under the theory that diluting authentic speech stifles legitimate debate.”

14.11.17

IT Web Africa

South Africa, prepare for more cyber attacks

Fortinet, the cybersecurity solutions firm, has warned businesses across South Africa that they should expect a rise in cyberattacks. A recent rise in attacks in the nation has stirred greater activity from businesses.

“Cyber security solutions firm Fortinet has issued a stern warning to South African businesses and organisations: prepare for an escalation in cyberattacks as digital criminals expand targets to home network devices and mobile devices.

According to Fortinet's Global Threat Landscape Report for Q2 2017, 90% of organisations recorded attacks targeting system and device vulnerabilities that were at least 3 years old – even though updates and patches that corrected those vulnerabilities had long been available.”

15.11.17

GhanaWeb

Ghana losing between 30-60 million dollars yearly through cyber fraud - Report

A recent report has revealed that Ghana could be losing around $30-60 million every year because of cyber-attacks and fraud. The continued digitalisation of banking and telecommunication has allowed for such issues to rise dramatically.

"Ghana is losing a whopping amount of between 30 to 60 million dollars through the internet and other forms of cyber fraud, particularly as a result of hacking into bank and cash transfers. What makes the situation even more alarming is that there is a lower level of knowledge by actors in the banking industry and mobile telecommunication, in most cases of how thieves and criminals operate to swindle the unwary.

These were made known during the presentation of a report titled; "2017 West Africa Cybersecurity Indexing and Assessment Report," by a team from 3T Solutions Consulting to the University of Ghana Business School (UGBS) at Legon."

15.11.17

Business Insider UK

Russia tried to hack UK media, telecoms, and energy

The UK's National Cyber Security Centre has now confirmed that Russia has attempted to hack into the UK's energy, media and telecommunications systems.

"The head of one of Britain's leading government cybersecurity agencies has confirmed that Russia tried to hack the UK media, telecommunications system, and energy sector in the past year.

Ciaran Martin, the CEO of the National Cyber Security Centre (NCSC), will say at the Times Tech Summit on Wednesday: 'I can't get into precise details of intelligence matters, but I can confirm that Russian interference, seen by the National Cyber Security Centre over the past the year, has included attacks on the UK media, telecommunication and energy sectors.'"

Privacy

No new items of relevance

Internet Inclusion

13.11.17

Computer Weekly

GE Digital to transform Middle East industry using the power of the internet

General Electric is expanding its operations in the Middle East in order to roll out the, ‘fourth industrial revolution’. Digital technology is aiming to be utilized by GE in order to encourage greater opportunities for all in the Middle East.

“US giant GE is a leading light *and sees a huge opportunity in the Middle East to embark on what is described as the* “fourth industrial revolution*”. “We built GE Digital to create digital solutions for the industrial world, and set out to make our own operations the proving ground for new ways of working in a digitized era,” said* Bill Ruh, CEO at GE Digital*.”*

“He added that digital transformation is an organisation-wide commitment for GE Digital, and it has been central to all that the company does, extending from its internal processes to partnerships with external stakeholders. Ruh said digital technology can unlock huge potential and billions of dollars in the Middle East.”

14.11.17

NextGov

Only 23% of the World has a free and open internet

Freedom House has published a new report focused on internet access and freedom, finding that only 23% of the world’s population have access to truly free internet.

“Though more people around the world are going online than ever before, almost two-thirds of them live in areas where the government has taken steps to limit freedom on the internet, a study found.

Less than a quarter of worldwide internet users have access to a “free” internet, while 64 percent reside in countries where the internet is designated as “partly free” or “not free,” according to the 2017 Freedom of the Net report by independent watchdog group Freedom House. Citizens in 32 of the 65 countries analyzed in the report saw their online freedom decline from last year, including the United States.”

Global Institutions

09.11.17

The Straits Times

Facing Russian threat, NATO expands operations, focuses on cybersecurity

As the Russian threat gets more prominent, NATO's defence ministers have decided for the first time since the Cold War, to expand its operations to help boost cybersecurity responses to aggression from Moscow.

"As the spectre of conflict with Russia looms over Europe, NATO defence ministers have decided to expand the alliance's operations for the first time since the Cold War, sharpen its focus on cyber operations, and boost their powers to respond to Kremlin aggression."

"The moves came as tensions with Russia remain the highest they have been in the nearly three decades since the end of the Cold War. Secretary of Defence James Mattis briefed fellow defence ministers on Wednesday (Nov 8) about Russian violations of the Intermediate Range Nuclear Forces Treaty, underlining the nuclear risk that is a worst-case consequence of the bitter back-and-forth."

15.11.17

ITU

ITU reveals latest global ICT Development Index country ranking with release of Measuring the Information Society 2017 report

The International Telecommunication Union has published its annual Measuring the Information Society Report detailing global ICT Development.

"The ninth edition of the annual Measuring the Information Society Report has been released today by the International Telecommunication Union (ITU) – the United Nations Specialized agency for information and communication technology (ICT).

"The Measuring the Information Society Report (MIS) is an ITU flagship publication widely recognized as the repository of the world's most reliable and impartial global data and analysis on the state of global ICT development. It is extensively relied upon by governments, international organizations, development banks and private sector analysts and investors worldwide."

15.11.17

ENISA

I say ransomware, you say crypto virus: the cyber-insurance language problem

A study and report entitled, “Recommendations of cyber-insurance” has been published by ENISA. It aims to aid people in understanding cyber-insurance and security and the risks that they pose.

“ENISA publishes ‘Recommendations on cyber-insurance’, a study on the commonality of risk assessment language in cyber-insurance, which proposes recommendations for achieving a higher level of language harmonisation. The study provides a comprehensive analysis of the factors that influence the harmonization, or lack thereof, of risk assessment language in cyber-insurance, its practical impact on the growth prospects of the cyber-insurance market and forthcoming trends.

‘Recommendations on cyber-insurance’ is based on feedback provided by multiple insurance carriers, brokers and other key industry stakeholders. Its recommendations are intended to support the cyber-insurance industry and policy makers to leverage the key market drivers towards harmonisation of the language used in underwriting and insurance coverage policies.”

Diary Dates

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