IEEE

GLOBAL INTERNET POLICY MONITOR

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

14 February 2018

Synopsis

Scroll to read full summaries with links to news articles.

In addition to **China**, **Vietnam** has been named as one of the top five **cyber-attack** source locations for the first time. Vietnam has attacked businesses across Australia, Singapore, Japan the United States and the United Kingdom.

Singapore has passed its **Cybersecurity** Bill into law which seeks to protect the countries eleven critical **infrastructure** sectors including; water, healthcare, media, Government and aviation.

MINDEF, Singapore's institute of Technology have launched the **Cyber NSF Scheme** which seeks to train full-time national servicemen to become elite cyber defenders of **Singapore's** military networks.

Europe's privacy regulators are working together to establish how they will investigate and sanction companies before a major overhaul in the bloc's **privacy** laws in May with the introduction of **GDPR**.

German judges have ruled that **Facebook's** use of **personal data** is illegal because the US social media platform had not secured the consent of its users before recording their personal information.

Finland's and **Estonia's** data exchange layers were connected to each other on the 7th February. This makes it possible to transfer **data** electronically over the Gulf of Finland.

Equifax has revealed that the **hack** on its systems in late 2017 had exposed more data than previously reported.

Google have announced that they would label all **HTTP** sites as **'not secure'** starting in July 2018.

Leaders of the US **intelligence** agencies have warned that **Russia** will attempt to interfere in the 2018 **US** midterm elections, using social media platforms to spread propaganda.

The **Nigerian Communications Commission** has announced that the number of Nigerian **internet users** increased marginally to 98.3 million in November out of an estimated 180 million people in the country.

The **Internet Society in Nigeria** has announced that it is committed to ensuring all Nigerians have **internet access** by engaging with the Government and private sectors.

Russia has threatened to shut down **social media** networks, **YouTube** and **Instagram** unless a video accusing Deputy Prime Minister **Sergey Prikhodko** and Billionaire **Oleg Deripaska** of corruption is removed.

Russian **communications** watchdog **Roskomnadzor** has announced it will decide later this year whether **Facebook** complies with **Russian** legislation.

NATO Secretary General **Jens Stoltenberg** has announced that Defence Ministers will agree to establish a new **Cyber Operations Centre** 'to keep our nations safe.'

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

14 February 2018

Table of Contents

Europe

Internet governance

13.02.18

Computer Weekly

Home Office fights terrorist content online with detection tool

In collaboration with ASI Data Science, the UK Home Office has created a tool which can automatically detect terrorist content online.

"The Home Office has partnered ASI Data Science to create a tool which automatically detects terrorist content on online platforms."

"Home Office has joined forces with London-based ASI Data Science to launch a tool to detect terrorist content in videos uploaded on the web."

14.02.18

Euractiv

EU adds pressure on online platforms with plan for fast removal of terrorist content

According to a leaked document the European Commissioner wants online platforms such as Facebook and Twitter to delete posts promoting terrorism within one-hour of them being posted.

"Online platforms should remove posts promoting terrorism within one hour after receiving complaints, according to a draft European Commission document that leaked on Tuesday (13 February)."

"The Commission wants "online marketplaces and social media companies" to take down posts that contain illegal content more quickly. The EU executive has focused its attention on terrorist material, which firms should remove within one hour."

Cybersecurity

07.02.18

SC Media

FIC 2018: European cyber-security cooperation will endure post Brexit

Guillaume Poupard, Director General of ANSSI, France's cybersecurity agency has said cooperation on cyber related issues between member states is 'absolutely essential' post-Brexit.

"Guillaume Poupard, director general of Agence Nationale des Systèmes d'Information, France's cyber-security agency - told SC Media UK, that while cyber-security is a matter of national sovereignty, it should not stop at this level."

"Guillaume Poupard, director general of ANSSI (Agence Nationale des Systèmes d'Information), France's cyber-security agency - an equilvalent of the UK's NCSC but one which reports directly to the French Prime Minister - told SC Media UK during FIC 2018 that while cyber-security is a matter of national sovereignty, it should not stop at this level. "Cooperation between States is absolutely essential."

08.02.18

SC Media

Cyber ring takedown one of largest, US says

The United States Justice Department announced one of its largest takedowns of a global cyber-crime ring. Thirty-six individuals were accused of identity theft trafficking and for causing more than £378 million in losses.

"The US Justice Department indicted 36 people in a cyber-ring created by a Ukrainian national on identity theft trafficking charges.

It was from the Infraud online forum that the ring, whose slogan is "In Fraud We Trust," helped cyber-criminals buy and sell US Social Security numbers, passwords and other private information, and fleeced victims of more than US$ 530 million (£378 million)."

14.02.18

Security Brief Asia

From Vietnam without love: Asia Pacific's next cyber-attack hub

In addition to China, Vietnam has been named as one of the top five cyber-attack source locations for the first time. Vietnam has attacked businesses across Australia, Singapore, Japan the United States and the United Kingdom.

"Vietnam may be hailed as the next Silicon Valley for its technology prowess, but for the first time it is now one of the top five cyber-attack source locations."

"ThreatMetrix's Q4 2017 Cybercrime report shows an increase in attacks that appeared to be from Vietnam and Russia. Attackers used automated bots and location spoofing tools to create mayhem."

Privacy

07.02.18

Euractiv

National privacy watchdogs brace for new pan-EU powers

Europe's privacy regulators are working together to establish how they will investigate and sanction companies before a major overhaul in the bloc's privacy laws in May with the introduction of GDPR.

"Europe's powerful data protection regulators are banding together to coordinate how they investigate and sanction misbehaving companies before a major overhaul of the bloc's privacy law takes effect in May."

"National watchdogs are about to get a lot more power under the strict new EU rules. And they will be forced to work together more as part of a restructured and muscled up umbrella group."

09.02.18

Euractiv

Commission lobbies for police access to website owners list

Law enforcement authorities in Europe have complained to the European Commission that new laws to restrict enforcement officers from accessing a WHOIS database which identifies website owners will be damaging.

"The European Commission has suggested that law enforcement authorities could soon have restricted access to the WHOIS database that identifies website owners because the system is on a collision course with the EU's strict new data protection law."

"Law enforcement authorities have complained to the Commission about plans to change the system in May because they rely on WHOIS to look up a "significant number" of websites every week as part of criminal investigations."

09.02.18

Channel NewsAsia

YouTube found no evidence of Russian interference in Brexit referendum

Juniper Downs, global head of public policy of American video-sharing website, YouTube has announced that YouTube has found no evidence that Russia had interfered in the UK's 2016 Brexit referendum.

"YouTube found no evidence of Russian interference in the 2016 Brexit referendum; a senior executive told a British parliamentary committee inquiry into fake news."

"Britain's Digital, Media, Culture and Sport Committee is taking evidence on Thursday at George Washington University as part of its inquiry."

13.02.18

Euractiv

German court rules Facebook use of personal data illegal

German judges have ruled that Facebook's use of personal data is illegal because the US social media platform had not secured the consent of its users before recording their personal information.

"A German consumer rights group said on Monday (12 February) that a court had found Facebook's use of personal data to be illegal because the US social media platform did not adequately secure the informed consent of its users."

"Under German law, personal information can only be recorded and used by a company with explicit agreement from the individual."

Internet Inclusion

12.02.18

Open Gov

Estonia and Finland connect their data exchange layers for seamless cross-border data transfer

Finland’s and Estonia’s data exchange layers were connected to each other on the 7th February. This has made it possible to transfer data electronically over the Gulf of Finland.

“This was done because of increasing migration and commuting between the two countries. The connection will make it technologically possible to transfer data electronically through a uniform transfer method over the Gulf of Finland between organisations that have joined the countries' data exchange layers.”

“For instance, register data can be exchanged automatically so that the home municipality of Estonians living in Finland is marked correctly in Estonian registries.”

United States of America

Internet governance

08.02.18

Channel NewsAsia

Russian watchdog says to examine Facebook later in 2018

Russian communications watchdog Roskomnadzor has announced it will decide later this year whether Facebook complies with Russian legislation.

“Russian communications watchdog Roskomnadzor said on Thursday it would carry out an audit into Facebook's compliance with Russian legislation in the second half of the year.”

“Alexander Zharov, head of Roskomnadzor, met Facebook executives in Moscow on Thursday to discuss the company's compliance with Russian law, the watchdog said in a statement.”

09.02.18

Channel NewsAsia

Competition Commission of India fines Google for abusing dominant position

India’s antitrust watchdog has fined Google $21.17 million for ‘search bias” and abuse of its dominant position.

“India's antitrust watchdog on Thursday imposed 1.36 billion rupees (US$21.17 million) fine on Google for "search bias" and abuse of its dominant position, in the latest regulatory setback for the world's most popular internet search engine.”

“The Competition Commission of India (CCI) said Google, the core unit of U.S. firm Alphabet Inc, was abusing its dominance in online web search and online search advertising markets.”

12.02.18

SC Media

[Google will label all HTTP sites 'not secure' starting in July 2018]

Google announced that they will label all HTTP sites as ‘not secure’ starting in July 2018.

“Google recently announced that the Chrome browser will soon start flagging every site not using HTTPS encryption as “not secure.”

“Google said that beginning in July 2018 with the release of Chrome 68, the browser will begin marking the sites as part of its move toward a more secure web by strongly advocating that sites adopt HTTPS encryption, according to a February 8, 2018 press release.”

13.02.18

ABC News

Russia is threatening to block YouTube and Instagram over video of oligarch

Russia has threatened to shut down social media networks, YouTube and Instagram unless a video accusing Deputy Prime Minister Sergey Prikhodko and Billionaire Oleg Deripaska of corruption is removed.

“Russia has threatened to block access to YouTube and Instagram if the sites do not remove video and photographs that show a senior government official sailing on a yacht with a billionaire oligarch, who has links with the former Trump campaign manager Paul Manafort.”

“Russia’s state-controlled media watchdog, Roskomnadzor, on Saturday ordered that 14 Instagram posts and seven YouTube videos be deleted that show metals magnate Oleg Deripaska on a yacht with a Russian deputy prime minister, Sergey Prikhodko, and a woman who has described herself as an escort.”

14.02.18

Euractiv

EU adds pressure on online platforms with plan for fast removal of terrorist content

According to a leaked document the European Commissioner wants online platforms such as Facebook and Twitter to delete posts promoting terrorism within one-hour of them being posted.

"Online platforms should remove posts promoting terrorism within one hour after receiving complaints, according to a draft European Commission document that leaked on Tuesday (13 February)."

"The Commission wants "online marketplaces and social media companies" to take down posts that contain illegal content more quickly. The EU executive has focused its attention on terrorist material, which firms should remove within one hour."

Cybersecurity

08.02.18

SC Media

Cyber ring takedown one of largest, US says

The United States Justice Department announced one of its largest takedowns of a global cyber-crime ring. Thirty-six individuals were accused of identity theft trafficking and for causing more than £378 million in losses.

"The US Justice Department indicted 36 people in a cyber-ring created by a Ukrainian national on identity theft trafficking charges."

"The US Justice Department indicted 36 people in a cyber-ring created by a Ukrainian national on identity theft trafficking charges."

13.02.18

SC Media

US intel pays £72,000 to Russian for NSA tools hacked by Shadow Brokers

The USA's National Security Agency has been reportedly working undercover to retrieve classified US Government documents from Russian operatives. They even offered them £72,000, but later stopped the deal.

"The US intelligence community reportedly negotiated in secret to retrieve classified documents stolen from the National Security Agency (NSA) by the Shadow Brokers and passed along to Russian intelligence."

"Working with Russian and American intermediaries in Europe over the past year, the US intelligence community reportedly negotiated in secret to retrieve classified documents stolen from the National Security Agency (NSA) by the Shadow Brokers and passed along to Russian intelligence – and even paid US$ 100,000 (£72,000) as a first installment payment toward getting back its hacking tools, but eventually stopped the deal because they feared being sucked into a Russian effort to interject chaos into the US government."

13.02.18

Channel NewsAsia

US 2018 elections 'under attack' by Russia - US intelligence chief

Leaders of the US intelligence agencies have warned that Russia will attempt to interfere in the 2018 US midterm elections, using social media platforms to spread propaganda.

“Leaders of U.S. intelligence agencies warned on Tuesday that Russia will try to interfere in the 2018 U.S. midterm elections by using social media to spread propaganda and misleading reports, much as it did in the 2016 campaign.”

“Director of National Intelligence Dan Coats told a congressional committee that Russia and other foreign entities were likely to attack U.S. and European elections this year and beyond, adding that Moscow believes similar efforts successfully undermined U.S. democracy two years ago.”

14.02.18

Security Brief Asia

From Vietnam without love: Asia Pacific's next cyber-attack hub

In addition to China, Vietnam has been named as one of the top five cyber-attack source locations for the first time. Vietnam has attacked businesses across Australia, Singapore, Japan, the United States and the United Kingdom.

“Vietnam may be hailed as the next Silicon Valley for its technology prowess, but for the first time it is now one of the top five cyber-attack source locations.”

“ThreatMetrix’s Q4 2017 Cybercrime report shows an increase in attacks that appeared to be from Vietnam and Russia. Attackers used automated bots and location spoofing tools to create mayhem.”

Privacy

09.02.18

SC Media

Equifax data breach may have exposed a wider range of data

Equifax has revealed that the hack on its systems in late 2017 had exposed more data than previously reported. This included data such as Passport numbers, first, last and middle names, credit card numbers with the expiration and CV2 security numbers.

“Equifax revealed to a Senate committee in a document that even more personal data than had been originally reported may have been exposed during the massive data breach the credit monitoring company experienced last year.”

“The Wall Street Journal is reporting that it reviewed a document sent to the Senate Banking Committee by the company that said in addition to the Social Security numbers, birth dates, addresses and driver's license numbers that were initially reported exposed - passport numbers, first, last, and middle names and suffixes, gender, phone numbers, credit card numbers with expiration date and “CV2” security numbers, email addresses and tax ID numbers may also have been exposed.”

09.02.18

Channel NewsAsia

YouTube found no evidence of Russian interference in Brexit referendum

Juniper Downs, global head of public policy of American video-sharing website, YouTube has announced that YouTube has found no evidence that Russia had interfered in the UK’s 2016 Brexit referendum.

“YouTube found no evidence of Russian interference in the 2016 Brexit referendum; a senior executive told a British parliamentary committee inquiry into fake news.”

“Britain's Digital, Media, Culture and Sport Committee is taking evidence on Thursday at George Washington University as part of its inquiry.”

13.02.18

Euractiv

German court rules Facebook use of personal data illegal

German judges have ruled that Facebook’s use of personal data is illegal because the US social media platform had not secured the consent of its users before recording their personal information.

“A German consumer rights group said on Monday (12 February) that a court had found Facebook’s use of personal data to be illegal because the US social media platform did not adequately secure the informed consent of its users.”

“Under German law, personal information can only be recorded and used by a company with explicit agreement from the individual.”

Internet Inclusion

13.02.18

Arstechnica

Trump’s infrastructure plan has no dedicated money for broadband

US President Trump’s 10-year plan for ‘rebuilding infrastructure in America’ prioritises funding for broadband however nothing is earmarked for improving internet access.

“President Trump's new 10-year plan for "rebuilding infrastructure in America" doesn't contain any funding specifically earmarked for improving Internet access. Instead, the plan sets aside a pool of funding for numerous types of infrastructure projects, and broadband is one of the eligible categories.”

“The plan's $50 billion Rural Infrastructure Program lists broadband as one of five broad categories of eligible projects.”

Pan-Asia

Internet governance

07.02.18

Channel NewsAsia

Chinese regulator raps internet firms over vulgar content

A Chinese content regulator has said they will severely punish tech companies, including Alibaba, Tencent and Baidu for failing to remove ‘harmful information’ published on their sites.

“A Chinese content regulator has rapped major tech companies, including Alibaba, Tencent and Baidu, for not doing enough to root out "harmful information" published on their platforms.”

“The anti-pornography office of China's powerful broadcasting watchdog convened a meeting with 16 major internet companies, telling them they needed to tighten oversight of vulgar and obscene information, the official Xinhua news agency said.”

09.02.18

Channel NewsAsia

Competition Commission of India fines Google for abusing dominant position

India’s antitrust watchdog has fined Google $21.17 million for ‘search bias” and abuse of its dominant position.

“India's antitrust watchdog on Thursday imposed 1.36 billion rupees (US$21.17 million) fine on Google for "search bias" and abuse of its dominant position, in the latest regulatory setback for the world's most popular internet search engine.”

“The Competition Commission of India (CCI) said Google, the core unit of U.S. firm Alphabet Inc, was abusing its dominance in online web search and online search advertising markets.”

14.02.18

Channel NewsAsia

[South Korea vows firm action against illegal, unfair cryptocurrency trading]

South Korea have announced that they will take firm action against unfair cryptocurrency trading after a 280,000 petition was signed and sent to the Presidential Blue House.

"South Korea said it will take firm action against illegal and unfair acts in cryptocurrency trading after a 280,000-signature petition was sent to the presidential Blue House."

"The petition followed the justice minister saying the government may shut down cryptocurrency exchanges. It demanded that the government never impose unreasonable regulation on virtual currency trading."

Cybersecurity

07.02.18

Security Brief Asia

[Singapore passes Cybersecurity Bill for nation's critical infrastructure providers]

Singapore has passed its Cybersecurity Bill into law which seeks to protect the countries eleven critical infrastructure sectors including; water, healthcare, media, Government and aviation.

"Singapore's parliament has successfully passed the country's Cybersecurity Bill into law this week after months of drafting and feedback from the public."

"Singapore's overall cybersecurity strategy puts data protection, critical information infrastructure, threat intelligence and international partnerships at the forefront of its agenda and the Cybersecurity Bill is now one part of that strategy."

12.02.18

SC Media

Russian actors mentioned as possibly launching cyberattack on 2018 Winter Olympic Games

Industry executives are pointing the finger at Russia for the cyberattack that hit the 2018 Pyeongchang Winter Olympic Games during the opening ceremony.

“Fingering the culprit behind the cyberattack that hit the 2018 Pyeongchang Winter Olympic Games during the opening ceremony will never be nailed down with 100 percent accuracy, but industry executives have gathered some circumstantial evidence is pointing toward a Russian group.”

“The primary reason Russia, or someone acting on that country's behalf, has been singled out is the fact that the International Olympic Committee (IOC) banned that nation from competing due to its athletes using illegal performance enhancing drugs during previous Olympic games.”

13.02.18

Open Gov

Singapore MINDEF launches Cyber NSF Scheme to bolster cyber defence capabilities

MINDEF, Singapore’s institute of Technology have launched the Cyber NSF Scheme which seeks to train full-time national servicemen to become elite cyber defenders of Singapore’s military networks.

“MINDEF is launching the Cyber NSF scheme to tap on cyber talents from the NSF pool. The scheme aims to develop committed and skilled Cyber NSFs to defend Singapore’s military networks.”

“On Feb 12, Singapore Ministry of Defence (MINDEF) signed its first work-learn Memorandum of Understanding (MOU) with an education institute where full-time national servicemen (NSF) are sent for academic upgrading while employed in an operational role.”

14.02.18

Security Brief Asia

From Vietnam without love: Asia Pacific's next cyber-attack hub

In addition to China, Vietnam has been named as one of the top five cyber-attack source locations for the first time. Vietnam has attacked businesses across Australia, Singapore, Japan the United States and the United Kingdom.

"Vietnam may be hailed as the next Silicon Valley for its technology prowess, but for the first time it is now one of the top five cyber-attack source locations."

"ThreatMetrix's Q4 2017 Cybercrime report shows an increase in attacks that appeared to be from Vietnam and Russia. Attackers used automated bots and location spoofing tools to create mayhem."

Privacy

no new items of relevance

Internet Inclusion

14.02.18

Open Gov

Singapore's Security ITM seeks to transform operating models through tech and innovation

Mrs Josephine Teo, Second Minister for Home Affairs and Manpower has launched the Security Industry Map which seeks to encourage security companies to use technology to deliver security solutions instead of manpower.

"The ITM will focus on four strategies: 1) supporting technology and innovation; 2) promoting 'best sourcing' of services, with Government taking the lead; 3) aligning regulations with ITM objectives to improve standards; and 4) improving skills to enable career progression."

"Mrs Josephine Teo, Minister, Prime Minister's Office and Second Minister for Home Affairs and Second Minister for Manpower, launched the Security Industry Transformation Map (ITM [1]) today at the Lifelong Learning Institute."

Rest of the World

Internet governance

08.02.18

Channel NewsAsia

Russian watchdog says to examine Facebook later in 2018

Russian communications watchdog Roskomnadzor has announced it will decide later this year whether Facebook complies with Russian legislation.

"Russian communications watchdog Roskomnadzor said on Thursday it would carry out an audit into Facebook's compliance with Russian legislation in the second half of the year."

"Alexander Zharov, head of Roskomnadzor, met Facebook executives in Moscow on Thursday to discuss the company's compliance with Russian law, the watchdog said in a statement."

13.02.18

ABC News

Russia is threatening to block YouTube and Instagram over video of oligarch

Russia has threatened to shut down social media networks, YouTube and Instagram unless a video accusing Deputy Prime Minister Sergey Prikhodko and Billionaire Oleg Deripaska of corruption is removed.

"Russia has threatened to block access to YouTube and Instagram if the sites do not remove video and photographs that show a senior government official sailing on a yacht with a billionaire oligarch, who has links with the former Trump campaign manager Paul Manafort."

"Russia's state-controlled media watchdog, Roskomnadzor, on Saturday ordered that 14 Instagram posts and seven YouTube videos be deleted that show metals magnate Oleg Deripaska on a yacht with a Russian deputy prime minister, Sergey Prikhodko, and a woman who has described herself as an escort."

Cybersecurity

12.02.18

Open Gov

State Government of South Australia released Cyber Security Strategic Plan 2018-2021

South Australia has published a Cyber Security Strategic Plan which seeks to protect the country's infrastructure, digital assets and citizen information against cyber-attacks.

"According to the Plan, the first 12 to 18 months of the strategy will witness a significant amount of work undertaken across three strategic themes. This initial period will form the foundation for the future deliverables and inform the first strategic plan review in early 2019."

"The state government of South Australia (SA) recently released a Cyber Security Strategic Plan 2018-2021."

12.02.18

SC Media

Russian actors mentioned as possibly launching cyberattack on 2018 Winter Olympic Games

Industry executives are pointing the finger at Russia for the cyberattack that hit the 2018 Pyeongchang Winter Olympic Games during the opening ceremony.

"Fingering the culprit behind the cyberattack that hit the 2018 Pyeongchang Winter Olympic Games during the opening ceremony will never be nailed down with 100 percent accuracy, but industry executives have gathered some circumstantial evidence is pointing toward a Russian group."

"The primary reason Russia, or someone acting on that country's behalf, has been singled out is the fact that the International Olympic Committee (IOC) banned that nation from competing due to its athletes using illegal performance enhancing drugs during previous Olympic games."

13.02.18

SC Media

US intel pays £72,000 to Russian for NSA tools hacked by Shadow Brokers

The USA's National Security Agency has been reportedly working undercover to retrieve classified US Government documents from Russian operatives. They even offered them £72,000, but later stopped the deal.

"The US intelligence community reportedly negotiated in secret to retrieve classified documents stolen from the National Security Agency (NSA) by the Shadow Brokers and passed along to Russian intelligence."

"Working with Russian and American intermediaries in Europe over the past year, the US intelligence community reportedly negotiated in secret to retrieve classified documents stolen from the National Security Agency (NSA) by the Shadow Brokers and passed along to Russian intelligence – and even paid US$ 100,000 (£72,000) as a first installment payment toward getting back its hacking tools, but eventually stopped the deal because they feared being sucked into a Russian effort to interject chaos into the US government."

13.02.18

Channel NewsAsia

Russia says hackers stole more than US$17 million from its banks in 2017

A central bank official announced this week that hackers had stolen more than $17 million from Russian banks using the Cobalt Strike security-testing tool in 2017.

"Hackers stole more than 1 billion roubles (US$17 million) from Russian banks using the Cobalt Strike security-testing tool in 2017, a central bank official said on Tuesday."

"Russia is under intense scrutiny over cyber crime following allegations hackers backed by Moscow have attacked targets in the United States and Europe, accusations the Kremlin has repeatedly denied."

13.02.18

Channel NewsAsia

US 2018 elections 'under attack' by Russia - US intelligence chief

Leaders of the US intelligence agencies have warned that Russia will attempt to interfere in the 2018 US midterm elections, using social media platforms to spread propaganda.

“Leaders of U.S. intelligence agencies warned on Tuesday that Russia will try to interfere in the 2018 U.S. midterm elections by using social media to spread propaganda and misleading reports, much as it did in the 2016 campaign.”

“Director of National Intelligence Dan Coats told a congressional committee that Russia and other foreign entities were likely to attack U.S. and European elections this year and beyond, adding that Moscow believes similar efforts successfully undermined U.S. democracy two years ago.”

14.02.18

Security Brief Asia

From Vietnam without love: Asia Pacific's next cyber-attack hub

In addition to China, Vietnam has been named as one of the top five cyber-attack source locations for the first time. Vietnam has attacked businesses across Australia, Singapore, Japan the United States and the United Kingdom.

“Vietnam may be hailed as the next Silicon Valley for its technology prowess, but for the first time it is now one of the top five cyber-attack source locations.”

“ThreatMetrix’s Q4 2017 Cybercrime report shows an increase in attacks that appeared to be from Vietnam and Russia. Attackers used automated bots and location spoofing tools to create mayhem.”

Privacy

09.02.18

Channel NewsAsia

YouTube found no evidence of Russian interference in Brexit referendum

Juniper Downs, global head of public policy of American video-sharing website, YouTube has announced that YouTube has found no evidence that Russia had interfered in the UK's 2016 Brexit referendum.

"YouTube found no evidence of Russian interference in the 2016 Brexit referendum; a senior executive told a British parliamentary committee inquiry into fake news."

"Britain's Digital, Media, Culture and Sport Committee is taking evidence on Thursday at George Washington University as part of its inquiry."

Internet Inclusion

07.02.18

The Guardian

'Connecting Nigerians to opportunities in Silicon Valley crucial to national development'

According to information technology expert and Principal Consultant, Lonadek Inc., Dr. Ibilola Amao more of Nigeria's tech savvy youths need to connect with experts from the US Silicon Valley to ensure national development.

"An information technology expert and Principal Consultant, Lonadek Inc., Dr. Ibilola Amao, has stressed the need for the nation's brightest tech savvy youths to connect with opportunities experts from the Silicon Valley in America are bringing to Nigeria to ensure economic growth and national development."

"Recall that Silicon Valley Nigerian Economic Development (SV-NED Inc), a company dedicated to the establishment of a strategic, bilateral economic relationship between the country and Silicon Valley, recently announced plans to bring experts into the country to train and connect the youth to the vast opportunities in the Valley."

07.02.18

The Guardian

Internet Society unveils plan to deepen accessibility for Nigerians

The Internet Society in Nigeria has announced that it is committed to ensuring all Nigerians have internet access by engaging with the Government and private sectors.

"The Internet Society (ISOC) Nigeria, has expressed its commitment to ensuring that all Nigerians have access to internet."

"The Society, while warning that Nigeria has a lot to lose if it fails to utilise the opportunities that internet presents, regretted that most Nigerians have no access to internet and that this retards the development of the country."

08.02.18

The Guardian

Nigerian internet users hit 98.3 million in December

The Nigerian Communications Commission has announced that the number of Nigerian internet users increased marginally to 98.3 million in November out of an estimated 180 million people in the country.

"Nigerian internet users increased marginally to 98.3million in November, the Nigerian Communications Commission (NCC), has said."

"The NCC made this disclosure in its Monthly Internet Subscribers Data for December 2017 on its website on Thursday in Abuja."

Global Institutions

14.02.18

NATO

Doorstep statement

NATO Secretary General Jens Stoltenberg has announced that Defence Ministers will agree to establish a new Cyber Operations Centre 'to keep our nations safe.'

"Today and tomorrow, Defence Ministers will meet here in Brussels to prepare for our Summit in July."

"We will begin with a meeting of the Nuclear Planning Group. Part of our regular consultations to keep NATO nuclear forces safe, secure and effective.We will also take decisions to modernise NATO's Command Structure."

Diary Dates

Global Internet and Jurisdiction Conference 2018 – 26.02.18-28.02.18

Ottawa, Canada

Cybersecurity and Data Opportunities in Sub-Saharan Africa – 05.03.18

London, England

Living in the Internet of Things- Cybersecurity of the IoT – 28.03.18-29.03.18

London, England

RSA – 16.04.18–20.04.18

San Francisco, USA

Data Centre Risk Radar- Technical Skills Shortage – 26.04.18

London, England

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal

EuroDIG – 05.06.18-06.06.18

Tbilisi, Georgia