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

**06 December 2017**

## Synopsis

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

**NATO** has begun to draw up **cyber warfare** principles after announcing that **cyber-attacks** to bring down enemy networks could be more effective than air strikes.

The European Union Agency for Network and Information Security (**ENISA**), has held its first industry focused event with stakeholders from across the **EU** to discuss how businesses can transform their **cybersecurity** work.

The **UK** Government have announced possible changes to the **Investigatory Powers Act** which would strip senior police officers of their power to access electronic communication channels, to bring the, **"snooper's charter"** in line with **EU law**.

**Privacy** watchdogs from across the **EU** have warned that the **US** needs to appoint an independent ombudsperson, who can manage data complaints by EU citizens, before 25th May 2018 to maintain the current **Privacy Shield**.

Representatives from the House **Homeland Security** Committee have warned that citizens should get comfortable with the fact that their personal information already has or will be compromised, because of constant **data breaches**.

Top executives from **Facebook** and **Apple** Inc. attended the **World Internet Conference** in **China** for the first time to hear the Chinese Government vow to open its **internet**.

To support **net neutrality** in Nigeria, the **Nigerian Communications Commission** (NCC) is increasing its efforts on the code of practice for the internet. The code aims to ensure that consumer's rights are protected online, and that malpractice is minimised.

**ICT** Ministers across nations in the **African Union** have highlighted the importance of **cybersecurity** and **digitisation** at a recent meeting of the Union.

A report has found that the **Ethiopian** Government targeted advocates of the **Oromo** ethnic group across 20 countries, by **hacking** into their computers and tracking journalists with **spyware** software.

The **United States** and **India** are preparing to start collaborating in the next few weeks to jointly deal with **cybersecurity** threats and offensive cyber operations.

The **Indian** Government have accepted new **net neutrality** recommendations from telecom regulator **Trai**, however there has been no indication as to when these recommendations could be converted into legislation.

A partnership between **Liquid Telecom** and **The Innovation Village** has been formed to aid internet and technology start-ups in **Uganda**. The partnership is in response to recent calls for greater **internet access** and availability for those in the nation.

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

**06 December 2017**

## Table of Contents

# Europe

## Internet governance

**03.12.17**

**Public Technology**

**Government puts forward changes to surveillance law in light of ECJ ruling**

The UK Government have announced possible changes to the Investigatory Powers Act which would strip senior police officers of their power to access electronic communication channels, to bring the, "snooper's charter" in line with EU law.

*"The government has launched a consultation into changes to the Investigatory Powers Act that have been proposed in a bid to make the legislation compliant with EU law."*

*"Late last year the European Court of Justice ruled that parts of the act – often informally referred to as the snoopers' charter – were in contradiction of European law. In response to this, the government has put forward a number of alterations and additions."*

**04.12.17**

**Computer Weekly**

**Barclays Bank stops offering Kaspersky software to new users**

Barclays has refused to offer their new customers free Kaspersky software, after warnings from the National Cyber Security Centre to not purchase Russian cybersecurity products.

*"Bank is no longer offering customers Kaspersky anti-virus software after UK security agency issues warning."*

*"Barclays Bank has stopped offering new customers security software from Kaspersky after the National Cyber Security Centre (NCSC) warned the UK government against using Russian cyber security products."*

**04.12.17**

**Europol**

**Andromeda botnet dismantled in international cyber operation**

Long-standing malware, Andromeda, was recently dismantled by the FBI and cybercrime forces in Germany and Europe. The commitment comes from the FBI as part of Europol's efforts to crack down on cybercrime and to make the internet safer to use.

*"On 29 November 2017, the Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue)."*

"*This widely distributed malware created a network of infected computers called the Andromeda botnet. According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month."*

## Cybersecurity

**30.11.17**

**Computer Weekly**

**Security community urges caution on offensive cyber defence**

NATO have begun to draw up cyber warfare principles after announcing that cyber-attacks to bring down enemy networks could be more effective than air strikes. Security industry commentators have warned against this.

*"Some NATO countries are reportedly considering responding to cyber-attacks with offensive cyber strikes, but security industry commentators warn of dangers."*

*"Seven of the 29 NATO countries are reportedly considering using cyber-attacks designed to bring down enemy networks in response to state-sponsored cyber-attacks."*

**04.12.17**

**ENISA**

**First ‘Industry 4.0’ event to introduce national cybersecurity initiatives to deliver industry transformation across Europe**

The European Union Agency for Network and Information Security (ENISA), has held its first industry focused event with stakeholders from across the EU to discuss how businesses can transform their cybersecurity work.

*“Under the theme “Using cybersecurity to deliver industry transformation (Industry 4.0)”, this event aims to bring together high-level decision makers and key industry players to address best practices and challenges in the cybersecurity field at a European level. The VOICE Manifesto, Secure by Default and l´Alliance pour la Confiance Numérique (ACN) are three of the approaches this open dialogue will focus on.”*

*“The objective of the breakfast is to discuss several approaches, initiated at Member State level, as a demonstration of case studies or best practices to European politicians and European Commission representatives.”*

## Privacy

**30.11.17**

**techUK**

**No Interruptions- Options for the future UK-EU data-sharing relationship**

A report commissioned by international law firm Dentons, TechUK and UK Finance, has urged the UK Government and the EU to safeguard the exchange of personal data post Brexit.

*“It is the view of the technology and financial services sectors that the EU and UK should pursue mutual adequacy decisions to provide a legal framework for the movement of personal data between the UK and EEA after the UK leaves the EU. This outcome requires the following actions:”*

*“Both the EU and the UK should begin their adequacy assessment processes as soon possible; • A standstill transitional arrangement for a set term to avoid a “cliff-edge” in the movement of personal data should be agreed immediately;”*

**30.11.17**

**Euractiv**

**Seven EU countries team up to investigate Uber data breach**

Data protection authorities from seven EU member states are collaborating to investigate Uber after millions of customers credit card details were hacked. Uber could be fined separately in each country.

*"EU privacy watchdogs are uniting to confront Uber over the breach of millions of consumers' data that the ride-hailing app recently reported."*

*"Data protection authorities from seven EU member states will coordinate their legal investigations into the breach, according to a news release that the so-called Article 29 group of privacy watchdogs published on Wednesday (29 November)."*

**01.12.17**

**Computer Weekly**

**Morrisons found liable for data leak in landmark ruling**

A UK court has ruled that Morrisons is legally responsible for a 2014 data breach where a former employee stole and posted thousands of workers personal data online.

*"Court finds supermarket chain liable for data leak by a former employee, which has been hailed as a landmark ruling, but Morrisons says it will appeal"*

*"The High Court has found Morrisons supermarket chain liable for a data breach in which a former employee posted the personal data of thousands of workers online in 2014."*

**01.12.17**

**Euractiv**

**Top EU privacy watchdog wants centralised regulator with muscle to police firms**

Giovanni Buttarelli, the EU's top privacy watchdog has said that EU lawmakers should create a new data protection authority to regulate privacy breaches that affect several member states in the bloc.

*"EU lawmakers should create a new, centralised data protection authority to oversee investigations of privacy breaches that affect more than one-member*

*state in the bloc, Giovanni Buttarelli, the EU's top privacy watchdog, said in an interview."*

*"Giovanni Buttarelli is the European Data Protection Supervisor. He spoke to EURACTIV's Catherine Stupp."*

**06.11.17**

**Reuters**

**EU regulators threaten court challenge to EU-U.S. data transfer pact**

Privacy watchdogs from across the EU have warned that the US needs to appoint an independent ombudsperson, who can manage data complaints by EU citizens, before 25th May 2018 in order to maintain the current Privacy Shield.

*"European Union privacy regulators have threatened to bring a legal challenge to a year-old EU-U.S. pact on the cross-border transfer of personal data if their concerns about its functioning and U.S. surveillance practices are not resolved by "*

**06.12.17**

**TheCitizenLab**

**Ethiopian dissidents targeted with new commercial spyware**

A report has found that the Ethiopian Government targeted advocates of the Oromo ethnic group across 20 countries, by hacking into their computers and tracking journalists with spyware software.

*"This report describes how Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins.*

*"Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of our investigation, one of the authors of this report was also targeted."*

## Internet Inclusion

***No new items of relevance***

# United States of America

## Internet governance

**01.12.17**

**The Hill**

**Dems reintroduce bill to jail those who don't alert victims of a data breach**

Three Democratic senators have re-introduced a Bill which threatens firms with the prospect of jail time if they fail to notify their customers about a data breach promptly after the incident.

*"Three Democratic senators have reintroduced a bill to require firms to promptly notify users whose data may have been taken by hackers or have those who had knowledge of the breach face prison time."*

*"We need a strong federal law in place to hold companies truly accountable for failing to safeguard data or inform consumers when that info has been stolen by hackers", Sen. Bill Nelson (D-Fla.), who headed the bill, said in a statement."*

**04.12.17**

**Europol**

**Andromeda botnet dismantled in international cyber operation**

Long-standing malware, Andromeda, was recently dismantled by the FBI and cybercrime forces in Germany and Europe. The commitment comes from the FBI as part of Europol's efforts to crack down on cybercrime and to make the internet safer to use.

*"On 29 November 2017, the Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue)."*

"*This widely distributed malware created a network of infected computers called the Andromeda botnet. According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month."*

**05.12.17**

**Channel NewsAsia**

**Apple, Facebook find something to praise China for amid internet clamp**

Top executives from Facebook and Apple Inc attended the China's World Internet Conference for the first time to hear the Government vow to open up its internet.

*"Top executives at Apple Inc and Facebook Inc managed to find something to praise Beijing for at an internet conference in China this week, even as its Communist Party rulers ban Western social media and stamp on online dissent."*

*"China's World Internet Conference attracted the heads of Google and Apple for the first time to hear China vow to open up its internet - just as long as it can guard cyberspace in the same way it guards its borders."*

**05.12.17**

**Channel NewsAsia**

**10,000 Google staff set to police YouTube content: CEO**

Google is deploying 10,000 staff to find and remove extremist content after Susan Wojcicki, CEO of YouTube said that "bad actors" had used the online platform to "mislead, manipulate, harass or even harm."

*"Google is to deploy a staff of 10,000 to hunt down extremist content on its YouTube platform following recent criticism, the video-sharing site's chief executive told Britain's Daily Telegraph Tuesday (Dec 5)."*

*"Susan Wojcicki admitted in the broadsheet that "bad actors" had used the website to "mislead, manipulate, harass or even harm.""*

## Cybersecurity

**30.11.17**

**Nextgov**

**GAO Asks: Exactly How Does CYBERCOM Help After Cyberattacks?**

The US Government Accountability Office has said that the Defence Department has failed to tell Congress how it is effectively training its forces to be cyber resilient and help civil authorities when there is a major cyber-attack against the United States.

*“The Defense Department hasn’t told Congress how it’s training forces to help civil authorities if there’s a major cyberattack against the United States, an auditor said Thursday.”*

*“Congress ordered the Pentagon to give it an overview of that training in the 2016 version of an annual defense policy bill, along with several other cyber readiness measurements.”*

**30.11.17**

**Nextgov**

**FBI, DHS Warn of Hacker Mercenaries Funded by Nation-States**

US officials have become increasingly concerned that cyber criminals in parts of Russia, could become, “patriotic hackers” for hacking operations that serve the Kremlin’s interests.

*“Lines between government-backed hackers and cyber criminals are getting fuzzier, top officials told lawmakers Thursday.”*

*“That’s one message the FBI wanted to send when it indicted two Russian intelligence officers and two criminal co-defendants for a major breach of the Yahoo email service in March, Director Christopher Wray said.”*

**06.12.17**

**The Print**

**Come January, India-US cyber security cooperation to take off**

The United States and India are preparing to start collaborating in the next few weeks to jointly deal with cybersecurity threats and offensive cyber operations.

*“US diplomat says the need now is to operationalise the joint policy, and a bilateral meeting in Washington in January will create a roadmap for implementation.”*

*“India and the US are set to operationalise a cyber security cooperation agreement in the next few weeks. The pact is likely to see response teams of the two countries joining hands, real-time sharing of threat assessments, and table-top exercises to jointly deal with offensive cyber operations.”*

## Privacy

**30.11.17**

**Nextgov**

**Congress Wants to Ditch Security Questions**

Representatives from the House Homeland Security Committee have warned that citizens should get comfortable with the fact that their personal information already has or will be compromised, because of constant data breaches.

*“Citizens should get used to the fact that most of their personal information already is, or will be, public because of constant data breaches, a Congressional committee warned.”*

*“A recent large-scale intrusion into credit bureau Equifax is just one example. Another is a state-sponsored Chinese hack exposed 22 million peoples’ government background check information a few years ago.”*

**06.11.17**

**Reuters**

**EU regulators threaten court challenge to EU-U.S. data transfer pact**

Privacy watchdogs from across the EU have warned that the US needs to appoint an independent ombudsperson, who can manage data complaints by EU citizens, before 25th May 2018 in order to maintain the current Privacy Shield.

*“European Union privacy regulators have threatened to bring a legal challenge to a year-old EU-U.S. pact on the cross-border transfer of personal data if their concerns about its functioning and U.S. surveillance practices are not resolved by “*

**06.12.17**

**TheCitizenLab**

**ETHIOPIAN DISSIDENTS TARGETED WITH NEW COMMERCIAL SPYWARE**

A report has found that the Ethiopian Government targeted advocates of the Oromo ethnic group across 20 countries, by hacking into their computers and tracking journalists with spyware software.

*“This report describes how Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins.*

*“Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of our investigation, one of the authors of this report was also targeted.”*

## Internet Inclusion

***No new items of relevance***

# Pan-Asia

## Internet governance

**29.11.17**

**South China Morning Post**

**Spike in Chinese censorship over Beijing migrant worker evictions, kindergarten scandal**

According to Weiboscope, a Chinese monitoring group, censorship of content online has spiked recently as the Government has attempted to quell public anger over forced evictions of migrant workers, and child abuse.

*"Censorship in China has spiked in recent days as the government scrambles to contain public anger over the forced evictions of migrant workers and claims of child abuse at a kindergarten in Beijing, according to a monitoring group."*

*"The percentage of posts deleted on Weibo, China's equivalent of Twitter, has risen sharply in the wake of the controversies, according to Weiboscope, a University of Hong Kong project tracking censorship on the social media platform."*

**30.11.17**

**ITU**

**New ITU case study shares insight into Singapore's 'Smart Nation' strategy**

An evaluation of Singapore's 'Smart Nation' strategy has been released in a recent report by the ITU. The strategy has tried to improve technology innovation in the nation and the report reaffirms the nation's strong commitment in this area.

*"A new ITU case study offers an evaluation of Singapore's progress in meeting the objectives of the country's 'Smart Nation' strategy, an evaluation undertaken using the Key Performance Indicators for Smart Sustainable Cities developed by ITU and the United Nations Economic Commission for Europe (UNECE)."*

*"Singapore's Smart Nation strategy aims to enrich citizens' lives by capitalizing on the potential of information and communication technology (ICT) to improve environmental sustainability, resilience, and equitable social and economic growth."*

**03.12.17**

**Reuters**

### China's Xi says country will not close door to global internet

Chinese President XI Jinping, has said that while China is committed to the open global internet, cyber sovereignty is key to their vision of internet governance.

*“Chinese President Xi Jinping said on Sunday the country will not close its door to the global internet, but that cyber sovereignty is key in its vision of internet development.”*

*“Xi’s comments were read by Huang Kunming, head of the Chinese Communist Party’s publicity department at the country’s largest public cyber policy forum in the town of Wuzhen in eastern China.”*

**05.12.17**

**Channel NewsAsia**

### Apple, Facebook find something to praise China for amid internet clamp

Top executives from Facebook and Apple Inc have attended the World Internet Conference in China for the first time to hear the Government vow to open up its internet.

*“Top executives at Apple Inc and Facebook Inc managed to find something to praise Beijing for at an internet conference in China this week, even as its Communist Party rulers ban Western social media and stamp on online dissent.”*

*“China's World Internet Conference attracted the heads of Google and Apple for the first time to hear China vow to open up its internet - just as long as it can guard cyberspace in the same way it guards its borders.”*

## Cybersecurity

**05.12.17**

**The Indian Express**

### ‘Need to understand cyber threats before fighting them’

At the National Security and the Growing Threat from Cyber Space’ conference in New Delhi, a panel of experts discussed the implications and challenges posed by cyber-attacks.

*“The confluence of national security and cyberspace is a dark area. A panel of experts — comprising Abhinav Kumar, IG Operations, Western Command, BSF Chandigarh; Sanjeev Tripathi, former chief, R&AW; Lt Gen. D S Hooda (retd), former Northern Army Commander; and Sandesh Anand, Cyber Security Consultant, Synopsys Inc — discussed the implications and challenges it poses.”*

*“The discussion was moderated by Sushant Singh, Associate Editor, The Indian Express. Edited excerpts.”*

**06.12.17**

**The Print**

**Come January, India-US cybersecurity cooperation to take off**

The United States and India are preparing to start collaborating in the next few weeks to jointly deal with cybersecurity threats and offensive cyber operations.

*“US diplomat says the need now is to operationalise the joint policy, and a bilateral meeting in Washington in January will create a roadmap for implementation.”*

*“India and the US are set to operationalise a cyber security cooperation agreement in the next few weeks. The pact is likely to see response teams of the two countries joining hands, real-time sharing of threat assessments, and table-top exercises to jointly deal with offensive cyber operations.”*

## Privacy

**06.12.17**

**TheCitizenLab**

**ETHIOPIAN DISSIDENTS TARGETED WITH NEW COMMERCIAL SPYWARE**

A report has found that the Ethiopian Government targeted advocates of the Oromo ethnic group across 20 countries, by hacking into their computers and tracking journalists with spyware software.

*“This report describes how Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins.*

*“Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of our investigation, one of the authors of this report was also targeted.”*

## Internet Inclusion

**30.11.17**

**BBC News**

**India net neutrality rules could be world's strongest**

The Indian Government have accepted new net neutrality recommendations from telecom regulator Trai, however there has been no indication as to when these recommendations could be converted into legislation.

*"India's telecom regulator has published recommendations strongly backing net neutrality, bringing the country a step closer to what could be the world's most progressive policy on equal internet access for all."*

*"This is in sharp contrast to current efforts in the US to reverse net neutrality rules introduced by former President Barack Obama."*

**30.11.17**

**Network Asia**

**DHL invests $364 million to further develop Cyberjaya data center**

DHL is investing $364 million in its IT Services Data Center in Cyberjaya, which will provide more jobs and opportunities for IT talent in Malaysia.

*"DHL expects to invest nearly RM 1.5 billion (US$364 million) between now and 2020 to further develop its IT Services Data Center in Cyberjaya, creating further opportunities for emerging IT talent in Malaysia and around the region."*

*"The IT Services Data Center has provided critical IT infrastructure, business application development and support initially for the company's Asia Pacific and, subsequently, global operations over the past 20 years, with DHL investing more than RM 4.7 billion (EUR 941.1M) in its development since 1997."*

**04.12.17**

**Diplomacy and Defence**

**China's internet industry second only to US, Beijing-backed study says**

Despite recent figures describing China as one of the worst nations for freedom of the internet, a questionable report by a Beijing think tank claimed that the USA was the only nation currently beating China on internet development, innovation, and governance.

*“China ranks second only to the United States in terms of internet development and innovation, but among the worst on cybersecurity and industry infrastructure, according to a survey of 38 countries by a Beijing-backed think tank.”*

*“The rankings, compiled by the Chinese Academy of Cyberspace Studies, were released on Monday at the World Internet Conference in Wuzhen, eastern China’s Zhejiang province, and provide an unprecedented insight into how the country sees its internet development in comparison with other nations.”*

# Rest of the World

## Internet governance

**04.12.17**

**Web Africa**

**Nigeria pushes open internet agenda**

In an attempt to support net neutrality in Nigeria, the Nigerian Communications Commission (NCC) is increasing its efforts on the code of practice for the internet. The code aims to ensure that consumers rights are protected online, and that malpractice is minimised.

*"The Nigerian Communications Commission (NCC) is stepping up efforts to solicit input from internet stakeholders to cement its draft code of practice in support of net neutrality and an open internet in the country."*

*"The regulator says the proposed Code of Practice seeks to protect the rights and interests of ISPs and consumers, as well as provide solutions to effectively address issues such as discriminatory traffic management practices and online abuse."*

## Cybersecurity

**30.11.17**

**Nextgov**

**FBI, DHS Warn of Hacker Mercenaries Funded by Nation-States**

US officials have become increasingly concerned that cyber criminals in parts of Russia, could become, "patriotic hackers" for hacking operations that serve the Kremlin's interests.

*"Lines between government-backed hackers and cyber criminals are getting fuzzier, top officials told lawmakers Thursday."*

*"That's one message the FBI wanted to send when it indicted two Russian intelligence officers and two criminal co-defendants for a major breach of the Yahoo email service in March, Director Christopher Wray said."*

**03.12.17**

**Citifmonline**

**[African hackers now using sophisticated approaches]**

Internet scamming and cybercrime in Africa has grown in sophistication, according to Delta3 International. The company has highlighted the risks associated with social media, which is being exploited by cyber criminals to access personal and sensitive information.

*"Mr. Mike Komla Etchi, Managing Consultant of Delta3 International, an Informational Security Advisory Company, has said cybercrime in Africa has moved from a 419 scam to much more sophisticated approaches."*

*"He said most of the attacker's still rely on poor security habits of the public to succeed in their operations."*

**04.12.17**

**Computer Weekly**

**[Barclays Bank stops offering Kaspersky software to new users]**

Barclays has refused to offer their new customers free Kaspersky software, after warnings from the National Cyber Security Centre to not purchase Russian cybersecurity products.

*"Bank is no longer offering customers Kaspersky anti-virus software after UK security agency issues warning."*

*"Barclays Bank has stopped offering new customers security software from Kaspersky after the National Cyber Security Centre (NCSC) warned the UK government against using Russian cyber security products."*

**04.12.17**

**Telecompaper**

**[African Union ministers discuss digitisation and cyber-security]**

ICT Ministers across nations in the African Union have highlighted the importance of cybersecurity and digitisation at a recent meeting of the Union.

*"Ministers in charge of ICT and postal services have declared digitisation a priority for Africa, Newsghana reported. At a two-day African Union meeting of the Specialised Technical Committee on Communication and ICT in Addis Ababa that ended on 01 December, they discussed and made decisions on continental and regional programmes concerning the centre."*

*“Communication and ICT sub-sectors in Africa still face many challenges, despite the significant gains in the African media landscape, telecoms and ICT and postal services, the conference noted.”*

## Privacy

**06.12.17**

**TheCitizenLab**

**ETHIOPIAN DISSIDENTS TARGETED WITH NEW COMMERCIAL SPYWARE**

A report has found that the Ethiopian Government targeted advocates of the Oromo ethnic group across 20 countries, by hacking into their computers and tracking journalists with spyware software.

*“This report describes how Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins.*

*“Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of our investigation, one of the authors of this report was also targeted.”*

## Internet Inclusion

**04.12.17**

**IT News Africa**

**Liquid Telecom partnership to support Ugandan start-ups**

A partnership between Liquid Telecom and The Innovation Village has been formed in an attempt to aid internet and technology start-ups in Uganda. The partnership is in response to recent calls for greater internet access and availability for those in the nation.

*“Liquid Telecom has announced a partnership with The Innovation Village, a hub and co-working space in Kampala to support Ugandan start-ups with high-speed internet and cloud-based services.*

*“Liquid Telecom together with The Innovation Village to provide new opportunities for start-ups operating in Kampala, enabling access to additional resources and expertise that can help them scale and launch locally relevant solutions.”*

**05.12.17**

**The Times of Israel**

**Israel program aims to give Haredim cybersecurity skills**

A new programme has been designed in Israel to provide training in cyber-tech and information security to the ultra-Orthodox and religious Zionist sectors.

*“A new national program targeting women and men from the ultra-Orthodox and religious Zionist sectors will provide training in the fields of cyber-tech and information security to help them integrate in Israel’s high-tech industry.”*

*“The program aims to bring diversity into Israel’s tech workforce and to expand the pool of workers of Israel’s flourishing cyber industry, the organizers of the initiative said.”*

## Global Institutions

**30.11.17**

**Computer Weekly**

**Security community urges caution on offensive cyber defence**

NATO have begun to draw up cyber warfare principles after announcing that cyber-attacks to bring down enemy networks could be more effective than air strikes. Security industry commentators have warned against this.

*"Some NATO countries are reportedly considering responding to cyber-attacks with offensive cyber strikes, but security industry commentators warn of dangers."*

*"Seven of the 29 NATO countries are reportedly considering using cyber-attacks designed to bring down enemy networks in response to state-sponsored cyber-attacks."*

**30.11.17**

**ITU**

**New ITU case study shares insight into Singapore's 'Smart Nation' strategy**

An evaluation of Singapore's 'Smart Nation' strategy has been released in a recent report by the ITU. The strategy has tried to improve technology innovation in the nation and the report reaffirms the nation's strong commitment in this area.

*"A new ITU case study offers an evaluation of Singapore's progress in meeting the objectives of the country's 'Smart Nation' strategy, an evaluation undertaken using the Key Performance Indicators for Smart Sustainable Cities developed by ITU and the United Nations Economic Commission for Europe (UNECE)."*

*"Singapore's Smart Nation strategy aims to enrich citizens' lives by capitalizing on the potential of information and communication technology (ICT) to improve environmental sustainability, resilience, and equitable social and economic growth."*

**04.12.17**

**Europol**

**[Andromeda botnet dismantled in international cyber operation]**

Long-standing malware, Andromeda, was recently dismantled by the FBI and cybercrime forces in Germany and Europe. The commitment comes from the FBI as part of Europol's efforts to crack down on cybercrime and to make the internet safer to use.

*"On 29 November 2017, the Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue)."*

"*This widely distributed malware created a network of infected computers called the Andromeda botnet. According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month."*

**04.12.17**

**ENISA**

**First 'Industry 4.0' event to introduce national cybersecurity initiatives to deliver industry transformation across Europe**

The European Union Agency for Network and Information Security (ENISA), has held its first industry focused event with stakeholders from across the EU to discuss how businesses can transform their cyebersecurity work.

*"Under the theme "Using cybersecurity to deliver industry transformation (Industry 4.0)", this event aims to bring together high-level decision makers and key industry players to address best practices and challenges in the cybersecurity field at a European level. The VOICE Manifesto, Secure by Default and l´Alliance pour la Confiance Numérique (ACN) are three of the approaches this open dialogue will focus on."*

*"The objective of the breakfast is to discuss several approaches, initiated at Member State level, as a demonstration of case studies or best practices to European politicians and European Commission representatives."*

## Diary Dates

**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