IEEE Global Internet Governance Monitor

25 January 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **EU** has stated that it will begin to stress test the **cyber defenses** of continental banks. The new program will replicate the cyber tests used by the UK's central bank since 2013.

The **UK's** surveillance agency **GCHQ** has announced its intentions to target teenage girls as it attempts to build up tech savvy analysts and spies for the future.

The **EU's** Justice Commissioner **Vra Jourová** has this week announced her intention to engage new American officials on **data protection** issues, in order to maintain EU-US agreements on the **Privacy Shield** and the **Umbrella Agreement** during the Trump Administration.

In the **United States** President Trump's Commerce Secretary nominee **Wilbur Ross** has stated that there will be no return of US oversight over the domain name authority **ICANN**.

President Trump has this week selected **Ajit Pai** as the new chairman of the **FCC**. Mr. Pai has been a member of the FCC since 2012. During his time on the Commission Mr. Pai has been a noted opponent to **net neutrality**.

The **US** Army has this week announced that the **"Hack the Army"** bug bounty scheme has revealed 118 vulnerabilities during its three-week time span.

In **China** this week the Government has announced a new crack down on **internet access**, as attempts are made to shore up the "Great Firewall". The new restrictions will target **VPN** services and other unauthorized connections that attempt to get around Chinese censors.

A new report this week has found that **India's** military network is at risk to **Chinese** hackers. One comment by the **Army Design Bureau** argues that the reliance on foreign developed computer pieces has put the Indian Army at risk.

2016 saw the number of **internet users** in **China** grow to over 731 million, with a year on year increase of 43 million equivalent to the population of Ukraine. The increase is believed to be a result of widely available smart phones and greater access in rural areas.

In **Africa** this week Ghana has announced the adoption of a **Cyber Security** policy and strategy, with an accompanying roadmap for how the Government intends to secure the country's **cyberspace**.

In institutional news, **ICANN's** PTI board has adopted its budget for the 2018 Financial Year, along with its operating plan. Alongside these documents the board has released a response to the public comments received in relation to its 2018 plans.

Contents

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

Europe

Internet governance

No new items of relevance

Net neutrality

No new items of relevance

Cyber security

23.01.17

Banks racing to use Blockchain are warned of security risks by EU watchdog

Amid the rush to utilise blockchain, financial services firms have been told by the European Union Agency for Network and Information Security (Enisa), that they must address security issues associated with the technology.

Banks have been in the process of testing the distributed ledger technology with the target of improving efficiency while cutting costs on security settlements and remittances. Enisa has conducted its own report on blockchain, in which it recognises the obvious advantages in transaction privacy, and in the ability to follow an audit trail for agreements. Despite this, the potential for consensus hijacking and smart contract management pose significant challenges.

According to the Enisa report, consensus hijacking can occur when an attacker takes control of a large enough number of the participants clients, allowing them to 'tamper with the validation process'. The same risk has been noticed with Bitcoin, and has been referred to as a "51% attack". It is said that this access could allow an attacker to get ahead of other participants in the process and imitate legitimacy.

The Enisa report offers a plan of action; encouraging firms to monitor internal activity, disclose information only to relevant counterparts and authorities, and to adopt industry level governance procedures.

24.01.17

100% increase in DDoS highlights growing scale of attacks across EMEA

A 100 percent increase in F5 DDoS customers was spotted in Q1 (October through December 2016), compared to the same period in 2015.

New figures from F5 Networks' EMEA Security Operations Centre (SOC) highlight the growing scale of DDoS attacks across the EMEA region.

In 2016, the SOC based in Warsaw handled and mitigated 8536 DDoS instances alone.

The most commonly observed type of DDoS attack in Q1 was user datagram protocol (UDP) fragmentations (23 percent) followed by DNS reflections and UDP floods (both 15 percent), syn floods (13 percent) and NTP reflections (eight percent).

During Q1, Web Application Firewall (WAF) customers were up 136 percent and anti-fraud rose by 88 percent.

One of the attacks featured among the largest globally, a 448 Gbps UDP/ ICMP fragmentation flood using over 100,000 IP addresses from multiple regions. IP attack traffic originated largely from Vietnam (28 percent), Russia (21 percent), China (21 percent), Brazil (15 percent) and the US (14 percent). This incident highlights a growing trend for global coordination to achieve maximum impact.

24.01.17

Dutch government helps political parties boost cybersecurity

The Dutch government is working with political parties on security measures to prevent cyber attacks and other interference in the run up to general elections in March.

The plans are outlined in a letter from Dutch Minister of Interior Affairs Ronald Plasterk and Minister of Security Ard van der Steur sent to the Dutch parliament Monday.

The government is analyzing vulnerabilities in organization connected to the elections, the digital security of politicians and the threat of fake news, the letter reads. The interior minister's cabinet is "is aware of the risk" of election hacking and the government has to be "very alert."

The government "organized a meeting of people responsible for ICT within the political parties" together with security services, adding that parties, responsible for their own cybersecurity, are now implementing the suggested measures.

On fake news, the ministers said it is largely up to media to act as gatekeepers, but the Dutch government is “stimulating awareness.”

24.01.17

Europe's security chief warns of growing threat of cyber attacks by criminals and the EU's political enemies

The EU's security chief has warned Europe faces a 'growing threat' of cyber attacks by criminals and the organisation's political enemies.

EU security commissioner Julian King said Brussels must shore up its defences in the face of a mounting danger.

He gave the example of the European Commission, the EU's powerful executive, which was hit by a 20-percent surge in cyber-attacks last year.

Speaking ahead of a cyber security conference in Lille, he said cybercrime cost the European economy 'nearly 60billion euros (£51billion) in 2016' and the bill will continue to rise.

Mr King, a former British Ambassador to France, added: 'An increasing number of hackers use cyber space to spread doubt about our political systems.'

'The people who are trying to do that, with criminal or other objectives, would like to work in the dark.'

25.01.17

EU to put banks’ cyber-security to the test

The EU is considering a plan to test banks defences against cyber-attacks. This initiative is similar to a plan already initiated by the Bank of England.

The Bank of England has been focused on this issue since 2013, with as many as thirty out of thirty-five major firms having to undergo a stress test known as CBEST. In November last year, authorities also outlined plans to make firms focus on their own security, by encouraging them to conduct regular security checks themselves. In addition to this, the Bank of England will also carry out spot checks.

Rob Norris, VP Head of Enterprise & Cyber Security EMEIA at Fujitsu said: “The news that the EU is considering cyber stress testing, similar to that of

the UK is a wise idea. With the number of threats continuing to increase exponentially, customer trust has never been so valuable or hard to come by and as such it has never been more important for banks to test and ensure they are protected appropriately".

Banks in particular are making great strides towards a digital future, with other financial services such as Schroders, the asset management firm, transforming in order to succeed in the digital world. However, with this evolution, new challenges arise. There is an indication that the attitude towards cyber-security must fundamentally change and as cyber threats increase, firms must also take a more proactive approach.

Cyber Skills

18.01.17

GCHQ targets teenage girls to find cyber spies of the future

Teenage girls are being invited to put their technology skills to the test in a competition that could unearth the cyber spies of the future.

The contest has been set up by GCHQ's new National Cyber Security Centre as part of efforts to inspire more women to join the fight against online crime. Only 10% of the global cyber workforces are female, the intelligence agency said.

Girls aged 13 to 15 can enter the CyberFirst Girls Competition in teams of four. The first stage of the competition involves a series of online challenges, with the top 10 teams then progressing to a national final in London in March.

The GCHQ director, Robert Hannigan, said: "I work alongside some truly brilliant women who help protect the UK from all manner of online threats.

"The CyberFirst Girls Competition allows teams of young women a glimpse of this exciting world and provides a great opportunity to use new skills. My advice to all potential applicants would be: enjoy the experience and I look forward to meeting some of you."

24.01.17

Dutch Military Intelligence Service looks for new cyber specialists

The challenge of keeping the Netherlands digitally safe is increasingly growing, according to Onno Eichelsheim, director of Dutch military intelligence service MIVD. The MIVD is therefore urgently looking for the next generation of cyber specialists to keep hackers out, he said to newspaper Trouw on Tuesday.

According to Eichelsheim, the specialists he is looking for is hard to come by, as they first need more training. "In order to understand new threats, I for example need people who can build algorithms to filter large amounts of internet data", he said to the newspaper.

The MIVD director the Netherlands is facing all kinds of digital threats. Recently American specialists warned that Russian hackers may target the Netherlands with influence operations during the elections, similar to what happened with leaked emails from the Democratic Party during the run up to the American elections.

"Russia and China perform all kinds of digital espionage attempts, influence operations and cyber attacks. What happened in the United States shows that the Russians are good at using information for political purposes. It is conceivable that the Russians or other parties may also try something towards the Dutch elections, through there are as yet no concrete indications for that", Eichelsheim said to the newspaper.

Cyber Privacy

19.01.17

Irish firms 'woefully unprepared' for new EU data protection law

Irish companies are “woefully unprepared” for a major new EU-wide data protection law, which comes into effect next year, a leading IT expert has warned.

Speaking ahead of the announcement of a new cyber security conference to be held in Dublin in early March, Ronan Murphy, chief executive of the IT services firm Smarttech and chairman of IT@Cork, said the Government must do more to help organisations become aware of the legislation.

The General Data Protection Regulation (GDPR), which comes into force in May 2018, is the biggest data protection legislation to be passed in the history of the European Union.

The regulation governs the privacy practices of any company handling EU citizens’ data, whether or not that company is located in the EU. It also requires that public authorities and certain companies processing personal data on a “large scale” must have an independent data protection officer.

20.01.17

Jourová seeks data protection talks with Trump’s people ‘as soon as possible’

Data protection agreements are an important part of EU-US relations, and the Privacy Shield pact and Umbrella Agreement will continue under Donald Trump’s administration, EU Justice Commissioner Věra Jourová told EurActiv Czech Republic.

Despite questions remaining on how Donald Trump will approach the European Union, Justice Commissioner Jourová is confident that his administration will not backtrack on crucial data protection agreements.

“I have been assured by insiders that President Trump and his administration do understand the importance of trade relations between the United States and the European Union,” Jourová told EurActiv.cz.

“A significant part of the EU-US trade exchange depends also on personal data transfers. Therefore, I believe that the Privacy Shield should go on and that it is also in the interest of the American side,” the Commissioner said.

According to Jourová, who was responsible for negotiations on the new framework for transatlantic exchange of personal data for commercial

purposes, the Privacy Shield agreement is an important element of strategic cooperation between Europe and the United States.

United States of America

Internet governance

18.01.17

Ross: No Rolling Back Internet Handoff

Trump Commerce secretary nominee and billionaire investor Wilbur Ross laid to rest any possibility of rolling back the Obama administration's handoff of internet domain name oversight to the international community Wednesday.

Ross said there's "no realistic way" to walk back the transition of U.S. oversight of the internet's domain name authority to a global stakeholder model since the Commerce Department declined to renew its contract with the Internet Corporation for Assigned Names and Numbers (ICANN) last fall.

"As such a big market and really as the inventors of the internet, I'm a little surprised that we seem to be essentially voiceless in the governance of that activity," Ross said during his Senate confirmation hearing Wednesday. "That strikes me as an intellectually incorrect solution."

Net neutrality

19.01.17

Netflix is so big that it doesn't need net neutrality rules anymore

Netflix has long been an outspoken supporter of net neutrality rules, but the streaming video provider says it is now so popular with consumers that it wouldn't be harmed if the rules were repealed.

The potential of reversing net neutrality rules increased the moment Donald Trump became president-elect, as Republicans in the Federal Communications Commission and Congress want to get rid of the rules. But in a letter to shareholders yesterday, Netflix reassured investors that this wouldn't affect the company's financial performance or service quality.

"Weakening of US net neutrality laws, should that occur, is unlikely to materially affect our domestic margins or service quality because we are now popular enough with consumers to keep our relationships with ISPs stable," Netflix wrote.

The FCC's rules prohibit ISPs from blocking or throttling traffic or giving priority to Web services in exchange for payment. Because of the rules, small video providers that aren't as popular as Netflix don't have to worry about being blocked or throttled by ISPs or having to pay ISPs for faster access to customers. ISPs would prefer that customers subscribe to the ISPs' own video services, and thus have incentive to shut out competitors who need access to their broadband networks.

20.01.17

Outgoing FCC chair warns against overturning net neutrality

Outgoing U.S. Federal Communications Commission Chairman Tom Wheeler warned Republicans against dismantling the Obama administration's landmark "net neutrality" protections that bar internet service providers from slowing consumer access to web content.

Wheeler, in an interview this week, repeatedly questioned why Republicans would institute new policies that he said would benefit major internet service providers such as Comcast Corp, AT&T Inc., Verizon Communications Inc. and CenturyLink Inc. at the expense of thousands of other companies and consumers.

The FCC rules set in early 2015 prohibit broadband providers from giving or selling access to speedy internet, essentially a "fast lane" on the web's information superhighway, to certain internet services over others.

"These are serious things," said Wheeler, who steps down Friday as Republican Donald Trump replaces Democrat Barack Obama as president. "People have made business decisions based on the expectation of an open internet and to take that away in order to favor half a dozen companies just seems to be a shocking decision.

23.01.17

Ajit Pai, staunch opponent of consumer protection rules, is now FCC chair

President Trump today made it official, selecting Ajit Pai as chairman of the Federal Communications Commission. "I am deeply grateful to the President of the United States designating me the 34th Chairman of the Federal Communications Commission," Pai said in a statement. "I look forward to working with the new Administration, my colleagues at the Commission, members of Congress, and the American public to bring the benefits of the digital age to all Americans."

Fellow Republican Commissioner Michael O'Rielly offered congratulations. [Pai's] "thoughtful approach, deep knowledge base, and sense of humor have been great assets to the Commission, and it makes sense that President Trump hand-picked him to carry out the new Administration's broad vision for the agency," O'Rielly said. Democratic Commissioner Mignon Clyburn also congratulated Pai, saying, "Ajit is bright, driven and committed to bringing connectivity to all Americans. I am hopeful that we can come together to serve the public interest by supporting competition, public safety, and consumer protection."

Cyber security

23.01.17

Hack the Army bug bounty program finds 118 vulnerabilities

The U.S. Army's three-week "Hack the Army" bug bounty trial ended last week with several hundred bug reports being received.

The Army reported, according to Kaspersky Labs' ThreatPost blog, that 400 hundred bug reports were received, of which, 118 were unique and actionable. The 371 people who participated were mainly civilians, however, 17 military personnel and eight government employees also submitted reports.

The bounties totaled about $100,000.

The Army was reticent to share many details regarding the vulnerabilities that were found, but it noted two flaws were discovered on the GoArmy.com website that could be used to enter a Department of Defense website.

The Hack the Army program was modelled on an earlier trial called Hack the Pentagon, which resulted in 138 flaws being found in May.

23.01.17

White House to End Defense Sequester, Boost Military's Cyber Capabilities

Donald Trump's administration will end the defense sequester and direct U.S. military leaders to develop defensive and offensive cyber capabilities to bolster the armed forces.

The military budget, missile defense, and cyber defense are priorities for the new White House, according to a statement on its website laying out Trump's plan to "make our military strong again."

Military leaders have spotlighted how reductions in defense spending have compromised the future military readiness of the joint force. In congressional testimony last fall, service leaders disclosed that their forces would not be able to defend the United States against current and future threats if sequestration continued.

According to the White House, Trump plans to end the defense sequester and send a new budget to Congress outlining his plan to rebuild the military. It is unclear how much defense spending Trump will propose, but the White House said he will commit to providing military leaders "with the means to plan for our future defense needs." The Pentagon operates on a roughly $600 billion annual budget.

Cyber Skills

21.01.17

Amazon To Teach Cloud Computing Skills To US Veterans

Apprenticeship program signed with government following CEO Jeff Bezos pledge to hire 25,000 veterans and their wives in five years.

The US Department of Labor (DoL) has signed an agreement with Amazon to create an apprenticeship program to train and prepare American veterans for new technical careers.

Veterans will be taken into Amazon to learn the ropes of cloud with AWS and other technologies.

The agreement follows Amazon's CEO Jeff Bezos pledge to hire 25,000 veterans and military spouses until 2021 and training 10,000 more in cloud computing skills as part of former-First Lady Michelle Obama and Dr. Jill Biden's "Joining Forces Initiative".

The first cohort of apprentices under the new agreement will be trained for AWS' Cloud Support Associate role, the DoL announced.

Cyber Privacy

20.01.17

Jourová seeks data protection talks with Trump's people 'as soon as possible'

Data protection agreements are an important part of EU-US relations, and the Privacy Shield pact and Umbrella Agreement will continue under Donald Trump's administration, EU Justice Commissioner Věra Jourová told EurActiv Czech Republic.

Despite questions remaining on how Donald Trump will approach the European Union, Justice Commissioner Jourová is confident that his administration will not backtrack on crucial data protection agreements.

"I have been assured by insiders that President Trump and his administration do understand the importance of trade relations between the United States and the European Union," Jourová told EurActiv.cz.

"A significant part of the EU-US trade exchange depends also on personal data transfers. Therefore, I believe that the Privacy Shield should go on and that it is also in the interest of the American side," the Commissioner said.

According to Jourová, who was responsible for negotiations on the new framework for transatlantic exchange of personal data for commercial purposes, the Privacy Shield agreement is an important element of strategic cooperation between Europe and the United States.

24.01.17

NY introduces legislation to limit warrantless stingray use

New York State legislators are following a national trend of proposing local legislation to protect citizens from warrantless stingray surveillance.

The bill (Assembly Bill 1895) was sponsored by New York Assemblyman Jeffrey Dinowitz along with a coalition of 18 other State Assembly members

on Jan. 13 and would ban law enforcement from warrantless stingray data collection and from compelling third party communications from divulging mobile device information without a warrant.

The bill also includes provision, which would prevent the sharing of any data that is legally obtained by the device as well and provides a legal remedy for those whose information is obtained unlawfully.

The bill is similar to legislation passed in California in 2015 and does contain exemptions for warrantless stingray use in the case of an emergency. Missouri and a host of other states have introduced similar legislation barring warrantless stingray on a state level.

25.01.17

US has no right to seize data from world's servers—court ruling stands

An evenly split federal appeals court ruled Tuesday that it won't revisit its July decision that allowed Microsoft to squash a US court warrant for e-mail stored on its servers in Dublin, Ireland. The 4-4 vote by the 2nd US Circuit Court of Appeals sets the stage for a potential Supreme Court showdown over the US government's demands that it be able to reach into the world's servers with the assistance of the tech sector.

A three-judge panel of the 2nd Circuit had ruled that federal law, notably the Stored Communications Act, allows US authorities to seize content on US-based servers, but not on overseas servers. Because of how the federal appellate process works, the Justice Department asked the New York-based appeals court to revisit the case with a larger *en banc* panel—but the outcome fell one judge short.

Justice Department spokesman Peter Carr said the agency was reviewing the decision and "considering our options." Those options include appealing to the Supreme Court or abiding by the ruling.

In its petition for a rehearing, the government said Microsoft didn't have the legal right to defend the privacy of its e-mail customers, and that the July ruling isn't good for national security. The authorities believe information in the e-mail could help it investigate a narcotics case.

Pan-Asia

Internet governance

23.01.17

China cracks down on unauthorized internet connections

China is reinforcing its censorship of the internet with a campaign to crack down on unauthorized connections, including virtual private network (VPN) services that allow users to bypass restrictions known as the Great Firewall.

The Ministry of Industry and Information Technology said in a notice on its website on Sunday that it is launching a nationwide clean-up campaign aimed at internet service provider (ISP), internet data centrer (IDC), and content delivery network (CDN) companies.

It ordered checks for companies operating without government licenses or beyond the scope of licenses.

Net neutrality

19.01.17

Net neutrality 2.0: Eye on traffic management

A new phase of net neutrality discussions has begun, and this time it is sharply focused on the issue of traffic management plans. Such plans are put into place to make sure that internet bandwidth is maintained, or network security is in place. The Telecom Regulatory Authority of Indiahas asked a set of 14 questions in its latest consultation paper. Most of these seek comments on ideal internet traffic management plans, the ways to regulate them, and the ways to ensure that they do not violate net neutrality.

The principle of net neutrality or network neutrality mandates that all data be treated equally. Internet service providers (ISPs) and owners of large content-based networks can control how data moves through the pipes. Depending on the kind of service they offer, they can determine how quickly your video buffers or whether a website appears blocked for you. These actions are part of standard traffic management practices. An internet service provider may regulate the amount of bandwidth available to you depending on whether you are just sending an email or playing a graphic-heavy multi-player online game. They may also need to handle network congestion by timing out requests if there are too many devices trying to connect.

Cyber security

20.01.17

Chinese hackers can bring down India's military network: report

According to a recent report, Chinese malware has the ability to bring down India's military network and disrupt the army's communication.

A report on future core technologies and problem statements claims that Chinese hackers can compromise Indian communication network and can disrupt correspondence during operations. Not only that, the report claims

that Chinese malware has the ability to steal sensitive information during peacetime.

"War plans would be protected by hundreds of firewalls but there are enough sensitive documents that can be stolen," said former Indian Air Force chief Fali Major. "The attackers can crash your systems and corrupt your data by gaining full control of computers."

The report states that the problem is compounded with the fact that a large amount of the equipment that the Indian army uses is imported; hence the chance of an embedded spyware or virus is always present.

"This has been compounded by the fact that origin of a large amount of electronic circuitry being used in communication equipment is of Chinese origin," claims the report, put together by the Army Design Bureau.

24.01.17

RBI tests banks' cyber security... by hacking into their systems

Cyber crime, data theft and online fraud have been on the rise in the past few years globally and many experts fear that with the push on Digital India, such incidents are to happen more in the country.

To make sure whether banks in India are prepared to face such challenges or not, Reserve Bank of India (RBI) has opted to use ethical hacking to test the cyber security vulnerabilities of banks and has unearthed shortcomings in four state-owned banks, reports the Economic Times.

“RBI is looking at international standards when it comes to protecting itself and banks from cyber-attacks. The regulator is planning a mix of ethical hacking, planned and unplanned audits of banks’ security systems to ensure that best practices are followed strictly,” a source familiar with the development told ET.

Since April 2013 to November 2016, the top 51 banks in India have lost nearly Rs 485 crore of which 56 percent was because of net-banking thefts and card cloning.

24.01.17

New type of cyber attacks to rise in South Korea: Report

New types of cyber attacks linked to Internet of Things (IoT) devices against government agencies and social infrastructure-related facilities are likely to increase this year.

A series of Distributed Denial of Service (DDoS) attacks — that occur when multiple systems flood the resources of a targeted system — on infrastructure systems through IoT-enabled devices may occur next year, Yonhap news agency reported on Tuesday, quoting Internet and Security Agency (KISA) in South Korea.

The agency said the DDoS attacks may occur with the aim of stirring political and social instability as South Korea may hold the next presidential election if President Park Geun-hye's impeachment motion is adopted by the Constitutional Court.

"There is the possibility that huge DDoS attacks could occur by using IoT devices from both home and abroad," KISA official Jeon Kil-soo said, noting that presidential candidates could also be the targets of such attacks.

25.01.17

Poorly secured infrastructure at cybersecurity risk in India: Kaspersky lab

There is a rise in the number of cyber attacks on critical infrastructure in India and it will not stop as most of the sectors are poorly protected, a top executive from the global internet security giant Kaspersky lab said here on Wednesday.

After the demonetisation move, the drive to digitisation has accelerated, bringing to the fore the concerns for cybersecurity and the level of risk remains the same everywhere and for every sector, said Vicente Diaz, Principal Security Analyst at Kaspersky lab.

"Poorly secured Industrial Cybersecurity Solutions (ICS) is nothing new but now attacking them provides direct benefit to the hackers. There will be more attacks in ICS sector," Diaz told reporters here.

He added that Advanced Persistent Threat (APT) had learnt from mistakes and now their deployment would be more silent in those poorly monitored systems.

APT usually refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity.

Cyber Skills

22.01.17

China's internet users grew in 2016 by the size of Ukraine's population to 731 million

China's internet users increased at the fastest pace in three years as the abundant availability of internet-enabled smart phones spurred usage and increased the penetration rate in the world's most populous nation, according to a report by the state agency responsible for the industry.

The Chinese internet market expanded 6.2 per cent in 2016, gaining 43 million internet users --equivalent to the population of a Ukraine or Argentina -- to put the total number of users at 731 million, according to data by the China Internet Network Information Centre. Penetration rate rose by 3.1 percentage points to 53.2 per cent, the CINIC data showed.

The 2016 growth pace has slowed from the double-digit clip that was recorded five years ago, when smart phones first became the engine driving the country's internet usage.

Already, 95.1 per cent of China's users, or 695 million people, access the internet through their phones, with the growth rate rising to a plateau.

The increasing penetration rate marks the end of the era when internet companies can simply rely on the growth of the overall user population to bolster their traffic and usage. Now they have to work harder to attract visitors to their sites, or to download their applications, requiring billions in development, marketing and subsidy dollars.

Cyber Privacy

No new items of relevance

Rest of the World

24.01.17

100% increase in DDoS highlights growing scale of attacks across EMEA

A 100 percent increase in F5 DDoS customers was spotted in Q1 (October through December 2016), compared to the same period in 2015.

New figures from F5 Networks' EMEA Security Operations Centre (SOC) highlight the growing scale of DDoS attacks across the EMEA region.

In 2016, the SOC based in Warsaw handled and mitigated 8536 DDoS instances alone.

The most commonly observed type of DDoS attack in Q1 were user datagram protocol (UDP) fragmentations (23 percent) followed by DNS reflections and UDP floods (both 15 percent), syn floods (13 percent) and NTP reflections (eight percent).

During Q1, Web Application Firewall (WAF) customers were up 136 percent and anti-fraud rose by 88 percent.

One of the attacks featured among the largest globally, a 448 Gbps UDP/ ICMP fragmentation flood using over 100,000 IP addresses from multiple regions. IP attack traffic originated largely from Vietnam (28 percent), Russia (21 percent), China (21 percent), Brazil (15 percent) and the US (14 percent). This incident highlights a growing trend for global coordination to achieve maximum impact.

24.01.17

Labor accuses Malcolm Turnbull of putting politics ahead of cyber security

Labor has accused Malcolm Turnbull of putting his own political purposes ahead of national security by publicising plans for a secret briefing for political parties to head off "Russian-style" cyber attacks.

The prime minister had told the Australian newspaper about his plans to invite opposition parties to secret classified briefings – but did not inform them except through the media.

Turnbull said such briefings were necessary following evidence of Russian efforts to influence the American elections.

Turnbull said the briefing invitation list included Bill Shorten and Labor's national secretary, Noah Carroll, the Liberal party federal director, Tony Nutt, Pauline Hanson, Nick Xenophon and the Greens.

25.01.17

New Report Pokes Holes in Uganda's Cyber Security Capacity

A new report by the Global Cyber Security Capacity Centre (GCSCC) has exposed loopholes in Uganda's cyber security capacity; indicating that it's at an embryonic state and that no concrete action has been taken to help the situation.

The report was compiled after a three day consultation with different government and private sector stakeholders who included; Government Ministries, National Information Technology Authority, Uganda (NITA-U); Academia; Civil society; Law enforcement; Internet governance representatives; Internet Society chapters; Criminal Justice; Intelligence Community; National Security representatives; CSIRT team; Commercial sectors and SME's; Finance Sector; and Telecommunications Companies.

According to the report, all Uganda's indicators lie in the start-up and formative levels that are the lowest on the indicators chart.

The consultations were based on the GCSCC's Cyber Security Capacity Maturity Model that is composed of five distinct areas of Cybersecurity Capacity:

25.01.17

Ghana adopts policy on cyber security

Ghana now has a Cyber Security Policy and Strategy that seeks to protect the country from attacks on its cyberspace.

The policy, which was approved by cabinet in 2016, is a road map on what should be done to ensure that the country's cyberspace is secure.

The policy also talks about issues within the cybercrime law enforcement area, which currently is difficult for the law enforcement to implement because of the lack of capacity and necessary tools.

It has, therefore, outlined areas such as building the capacities of law enforcement bodies, as well as the legal fraternity such as the Attorney General, judges and lawyers to empower them to deal with cybercrime-related issues.

Briefing the Daily Graphic, the Manager of the Computer Emergency Response Team (CERT)-Ghana, Mr Eric Akomiah, explained that the policy was to secure and protect individuals from cyber fraud.

Global Institutions

23.01.17

PTI Board Adopts FY18 Budget and Publishes Report of Public Comments

The PTI Board has adopted its FY18 Operating Plan and Budget, following a seven-week Public Comment period on a draft published in October 2016. The ICANN Board will consider PTI's Budget at its March meeting, to be held during the ICANN58 meeting in Copenhagen, Denmark.

ICANN and PTI have also published the Report of Public Comments on PTI's draft FY18 plans. This detailed report responds to each of the 21 individual comments submitted. The report has been structured thematically and is accompanied by a sortable spreadsheet, to help readers find the comments and responses they are most interested in.

The FY18 PTI Operating Plan and Budget is the result of months of collaborative work by the community and staff. It includes:

- Highlights of all PTI operations
- Overview of the PTI Implementation Costs
- Overview of PTI's FY18 budget
- Detailed FY18 operating plan

PTI's fiscal year runs from 1 July through 30 June and the adopted Operating Plan and Budget will run from 1 July 2017.

Diary Dates

CyberTech Israel 2017 – 31.01.17-01.02.17

January 31 - February 1, 2017 | Tel Aviv, Israel

ENISA evaluation and review

Open from 18 January to 12 April 2017.

3rd International Conference on Information Systems Security and Privacy – ICISSP 2017 – 19.02.17-21.02.17

Porto, Portugal

European Information Security Summit 2017 (TEISS) – 21.02.17-22.02.17

London, UK

Singapore Cyber Security R&D Conference (SG-CRC 2017) - 21.02.17-22.02.17

Singapore

Emerging issues in building the European data economy

Foreseen for 1st quarter of 2017

European Dialogue on Internet Governance – 06.06.17-07.06.17

Tallinn, Estonia