

# Cybercrime Digest

Bi-weekly update and global outlook by the  
Cybercrime Programme Office of the Council of Europe (C-PROC)

16-31 October 2016

Source: Council of  
Europe

## Strategic priorities on cybercrime adopted by GLACY countries in Bucharest

Date: 28 Oct 2016

"Countries participating in the project on Global Action on Cybercrime (GLACY) have adopted a set of strategic priorities to address the challenges related to cybercrime and electronic evidence. Representatives of Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga finalised the document during the GLACY closing conference in Bucharest, Romania, on 28 October 2016.

The conference also marked the launch of the new GLACY+ project on Global Action on Cybercrime Extended. GLACY+ will help countries of Africa, Asia/Pacific and Latin America to give follow up to these Strategic Priorities." [READ MORE](#)

### RELATED ARTICLES

Prime Minister's Office of the Kingdom of Tonga, [Launching of the Global Action on Cybercrime Plus](#), 31 Oct 2016

Le Matin, [Participation du Maroc à la conférence de lancement du programme Glacy+](#), 30 October 2016

Jurnalul24, [Lansarea proiectului Acțiunea Globală împotriva criminalității informatice extinsă \(GLACY+\)](#), la București, 31 Oct 2016

Agerpress, [Ioana Albani \(DIICOT\): E mai probabil să devii victima unei infracțiuni informatice decât a unei tâlhării](#), 28 October 2016

Source: Reuters

## Websites free to store IP addresses to prevent cyber attacks - EU court

Date: 19 Oct 2016

"Website owners are free to store users' internet addresses to prevent cyber attacks, the European Union's top court said on Wednesday, rejecting a claim from a German privacy activist who sought to stop the practice. Patrick Breyer, a member of Germany's Pirate Party, had sought to stop the German government registering and storing his Internet Protocol (IP) address when he visited its web pages, arguing that citizens should have a right to surf the web anonymously." [READ MORE](#)

Source: United  
Nations

## UN anti-crime chief urges better use of Convention against Transnational Organized Crime

Date: 17 Oct 2016

"Citing indisputable negative impacts of transnational organized crime on people's lives and societies, the United Nations top anti-crime official today stressed the need to make better use of the existing global convention and its protocols to tackle this illicit act. [...] He also noted that UNODC is working hard to highlight the Convention's unique value in addressing new and emerging crimes, including cybercrime, whether involving criminal use of the internet, cyber-enabled fraud or online exploitation and abuse of children[...]. However, he pointed out, implementation represents a distinct challenge and this gap must be closed." [READ MORE](#)

Source: *Le Monde*

Date: 21 Oct 2016

## Une attaque informatique majeure a paralysé une partie du Web pendant plusieurs heures

“Twitter, Netflix, Reddit ou encore le site du « New York Times»: certains des plus grands sites mondiaux ont été fortement perturbés, essentiellement pour les internautes américains. Une attaque informatique massive a paralysé une partie du Web, essentiellement aux Etats-Unis, depuis vendredi 21 octobre en fin d’après-midi. L’entreprise au cœur des perturbations, Dyn, a annoncé peu après minuit (heure de Paris) que l’incident a été résolu. L’attaque, de type « déni de service», qui consiste à saturer un service de connexion pour le rendre inaccessible, a visé plus spécifiquement les services de Domain Name System (DNS) de Dyn.” [READ MORE](#)

### RELATED ARTICLES

Reuters, [Cyber attacks disrupt PayPal, Twitter, other sites](#), 21 Oct 2016

Krebs On Security, [Hacked Cameras, DVRs Powered Today’s Massive Internet Outage](#), 21 Oct 2016

RT, [Internet denied: What’s behind the massive DDoS attacks](#), 22 Oct 2016

Dyn, [Dyn Statement on 10/21/2016 DDoS Attack](#), 22 Oct 2016

---

Source: *Europol*

Date: 17 Oct 2016

## European Cybercrime Center, 13 countries join the global fight against ransomware

“More than 2 500 victims were able to decrypt their devices thanks to No More Ransom. Just three months after the successful launch of the No More Ransom project, law enforcement agencies from a further 13 countries have signed up to fight ransomware together with the private sector. The new members are: Bosnia and Herzegovina, Bulgaria, Colombia, France, Hungary, Ireland, Italy, Latvia, Lithuania, Portugal, Spain, Switzerland and the United Kingdom. More law enforcement agencies and private sector organisations are expected to join the programme in the coming months.” [READ MORE](#)

---

Source: *The Guardian*

Date: 24 Oct 2016

## Curbing cybercrime in Nigeria: Ministry to partner agencies

“As new prospects and emerging trends in cyber security is on the increase globally, the Minister of Communications, Barrister Adebayo Shittu, has expressed the readiness of the ministry to partner with agencies to catalyse and develop worldclass human and institutional capacity in cyber security for the country. In a statement by the ministry, he said the ministry is living up to expectation of sensitising and impacting skills on cyber protection by creating the Computer Emergency Response Team (CERT) to handle computer security incidents and examining the implementation framework of the Cybersecurity Act with amendments where necessary in collaboration with the Office of the National Security Adviser (ONSA).” [READ MORE](#)

### RELATED ARTICLES

The Guardian, [Nigerian Police to create special unit to tackle cybercrime](#), 24 Oct 2016

---

Source: *The Daily Monitor*

## Uganda, Rwanda police chiefs to fight crime

Date: 24 Oct 2016

"The Inspector General of Police, Gen Kale Kayihura and his Rwandan counterpart, Commissioner General Emmanuel Gasana, have laid strategies of combating cross-border crimes. [...] The two heads of the police forces signed a joint communiqué of resolutions. They include enhancing timely exchange of information and intelligence on criminal syndicates, to develop and update a joint watch list of wanted persons, build capacity through development of police doctrine, curriculum, infrastructure, exchange of instructors and students as well as embracing ICT-led policing and conducting simulation exercises." [READ MORE](#)

Source: *Finextra*

## Indian banks hit by massive ATM breach

Date: 20 Oct 2016

"India's top banks are asking customers to change PIN codes and recalling millions of debit cards following reports of a malware-based security breach at a number of unspecified ATMs across the country. State Bank of India, HDFC Bank, ICICI Bank, Yes Bank and Axis Bank have all issued advisories concerning the breach, which may impact up to 3.2 million debit cards." [READ MORE](#)

### RELATED ARTICLES

Business Standards, [Securities and Exchange Board of India steps up effort to tackle cyber crime](#), 24 October

Source: *ORF*

## India and the Budapest Convention: Why not?

Date: 20 Oct 2016

"[...] In 2007 and 2008, India and the Council of Europe cooperated in the reform of India's Information Technology Act. These reforms brought the legislation of India broadly in line with the Budapest Convention. While membership in the Budapest Convention more than doubled since then, India is yet to join this treaty. The reasons are not entirely clear. [...] Given Prime Minister Narendra Modi's vision of a Digital India and considering the surge in cybercrime, it would be beneficial for India to join this treaty." [READ MORE](#)

Source: *Computer World Singapore*

## Philippines' National Cybersecurity Strategy to be launched in December

Date: 19 Oct 2016

"The Philippine government will launch its cybersecurity strategy in December, according to Allan Cabanlong, Executive Director of the Cybercrime Investigation and Coordination Centre (CICC). In a report by GovInsider, Cabanlong said the strategy aims to strengthen the country's cyber core through four key thrusts, including critical infrastructure protection, government, businesses, and individuals." [READ MORE](#)

Source: *The Stack*

## Proposed Thai law would hold ISPs responsible for cyber crime

Date: 25 Oct 2016

"[...] Article 15 of the Computer Crime Act says that any service provider intentionally supporting or consenting to an offence within a computer system under their control shall be subject to the same penalty as that imposed on a person committing an offence." [READ MORE](#)

Source: *Computer Weekly*

## ASEAN countries deepen joint efforts against global cyber threats

Date: 20 Oct 2016

"Member states of the Association of Southeast Asian Nations (Asean) will cooperate more closely to combat cyber threats as part of the recently announced cyber security strategy of the Singapore government. Ibrahim proposed three areas for cooperation among Asean member states: cyber capacity building, cyber space awareness, and cyber norms. "Singapore is committed to these ideas, and we are backing our words with resources and investment," he said." [READ MORE](#)

---

Source: *IntellASIA*

## The Trouble with Vietnam's Cyber Security Law

Date: 24 Oct 2016

"[...] On the one hand, Vietnam's computer networks are among the most targeted for attack in the world, courtesy of rampant cybercrime and legions of Chinese hackers. The July hacking of Noi Bai Airport underlined the scale of Vietnam's cyber woes. Investment in national cyber security efforts must increase drastically. On the other hand, the new law makes it clear the government is antsy about citizens with the cyber savvy to encrypt their online communications." [READ MORE](#)

---

Source: *The Daily Star*

## Bangladesh Digital Security Act: how does it affect freedom of expression and the right to dissent?

Date: 28 Oct 2016

"The draft Digital Security Act 2016, intended to address the need for cyber-crime legislation, according to the authorities, was approved on August 22, 2016, by the Cabinet. But members of civil society, media and activists have already expressed their concerns over the draft law impinging upon people's freedom of expression." [READ MORE](#)

---

Source: *Prensa Libre*

## No hay ley contra los ciberataques en Guatemala

Date: 23 Oct 2016

"Guatemala carece de una ley para delitos cibernéticos, lo que permite que el país sea vulnerable a diversas prácticas del cibercrimen y que a la vez no exista castigo para los ataques contra páginas gubernamentales o privadas. [...] Wálter Girón, viceministro de Tecnologías, del Ministerio de Gobernación, señaló que ya se trabaja en la Política Nacional de Seguridad Cibernética y que está por terminar el borrador de una iniciativa de delitos informáticos, la cual elaboran con el apoyo de la Unión Europea y la Organización de Estados Americanos, ya que debe cumplir con ciertos principios que establece el Convenio de Budapest." [READ MORE](#)

---

Source: *Media Update*

## South Africa, fears persist over 'internet censorship' Bill

Date: 19 Oct 2016

"Despite a consultative process and public debate, stakeholders are still losing sleep over the Film and Publication Board's (FPB) draft Online Regulation Policy and the Department of Communication's proposed Film and Publications Amendment Bill. Critics see a catastrophe in the making. In a recent panel discussion facilitated by IAB South Africa, FPB CEO defended the position of the Board, explaining the need for the Amendment Bill, and heard counter-arguments from representatives of Google, Uber, and a consultant to the Internet Service Provider's Association (ISPA)." [READ MORE](#)

---

Source:  
DeepDotWeb

## Austrian Government Wants A Federal Trojan To Patrol The Dark Web

Date: 26 Oct 2016

"Austrian Interior Minister Wolfgang Sobotka is preparing to implement a "federal trojan" to patrol the dark net. With this state spying software, Austrian law enforcement authorities hope they can prevent cybercriminal activity on the dark web. "The Interior Ministry lacks the necessary technical and legal requirements in order to operate with the perpetrators on an equal footing," Sobotka said on Tuesday during a debate in the National Council." [READ MORE](#)

---

### Latest reports

- Europol, [EUROPOL Review 2015](#), 28 October 2016
- Europol, [Mobile Malware - Stop. Think. Connect.](#), 24 October 2016
- IEEE Spectrum, [What Is a Distributed Denial-of-Service Attack?](#), 21 October 2016
- OAS, [Inter-American Cooperation Portal on Cyber-Crime](#), updated in October 2016
- Action Fraud UK, [Fraud & cybercrime cost UK nearly £11bn in past year](#), 18 Oct 2016
- Checkpoint, [September's top wanted malware list](#), 21 October 2016
- Kaspersky, [Kaspersky DDOS intelligence report for Q3 2016](#), 31 October 2016
- Panda Software, [27% of all recorded malware appeared in 2015](#), 26 October 2016
- IT Governance, [List of data breaches and cyber attacks in October 2016](#), 27 October 2016

### Upcoming events

- 2 – 3 November 2016, Chisinau, Moldova - On-site expert mission to support assessment of the package of amendments to various laws, [EAP III](#)
- 2 – 3 November 2016, Tbilisi, Georgia – Workshop on legislative amendments related to data preservation, [EAP II](#)
- 4 November 2016, Kyiv, Ukraine - Review of procedural law: presentation of findings, [EAP III](#)
- 7 – 8 November 2016, Yerevan, Armenia – Review of procedural law: presentation of findings, [EAP III](#)
- 9 – 11 November 2016, Tbilisi, Georgia - Public-Private cooperation: Solutions for improved sharing of subscriber information (combine with GITI Information Security Day), [EAP III](#)
- 14 – 15 November 2016, Strasbourg, France (Council of Europe) – Participation in the 16<sup>th</sup> plenary session of the Cybercrime Convention Committee (T-CY), [EAP II](#), [GLACY+](#), [iPROCEEDS](#)

The Cybercrime Digest appears bi-weekly. News are selected by relevance to the current areas of interest to C-PROC and do not represent official positions of the Council of Europe. You receive this digest as you have taken part in Council of Europe activities on cybercrime. It is not intended for general publication.

For any additional information, contributions, subscriptions or removal from this distribution list, please contact: [cybercrime@coe.int](mailto:cybercrime@coe.int)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE