NewsletterFebruary 2021

Center for Cyber Security and International Relations Studies

Upcoming Events

March 4

The European Cybersecurity Summit

March 17

Security Summit

Cyber Policy, Diplomacy& Legal Framework

- Communications Minister touts the opportunities of a Google-less Australia
  Paul Fletcher said Microsoft is at the ready to replace Google Search with Bing in Australia, while Treasury pointed to the existence of codes in the dairy and sugar industries as justification for pushing forward with the Media Bargaining Code.
- Singapore passes bill governing police use of contact tracing data
  Singapore has passed new legislation detailing the scope of local law enforcement's access to COVID-19 contact tracing data. It does so amidst questions whether the bill offers sufficient clarity and if police access should be excluded in the interest of public health.
- An International response to offensive cyber operations is long overdue
  Recent cyberattacks underscore the need for international norms of responsible behavior, and an institutionalized process to support them.
- India-Japan cyber cooperation: From strength to strength
  Fifth generation internet technology — 5G — is emerging as an important tool of strategic cooperation. Many countries across the globe are in the middle of intense discussions in deciding vendors and ensuring cybersecurity in their 5G services.

Cyber Security

- NetWalker infrastructure taken down by authorities in the U.S. and Bulgaria
  A Canadian national has been indicted in the U.S. for using the NetWalker ransomware to target organisations worldwide, earning at least over $27.6 million, and using a dark web resource to blackmail ransomware victims.
- Top Cybersecurity Threats to Watch in 2021
  The pandemic has brought more than an economic and health crisis, but a cybercrime crisis as well. The explosion of online activities opened a new world of opportunities for cyber criminals. Phishing scams, frauds, and data breaches that

exploit the pandemic are at the order of the day.

- Social media activity exposes many users to cyber threats – report
  Nearly three quarters of people post information on social media that could make them vulnerable to a cyberattack, according to a new report from security company Tessian.
- Bad patching practices are a breeding ground for zero-day exploits, Google warns
  Customers of major software vendors take comfort whenever a vendor issues a security fix for a critical software vulnerability. The clients expect that software update to keep attackers from stealing sensitive information.

Cyber Warfare, Intelligence and Terrorism

- Myanmar coup: How the military disrupted the internet
  The military takeover in Myanmar of the last weeks resulted in internet disruption in large parts of the country. The Authority said was for the sake of "stability".
- Hezbollah linked hackers hit companies in global malware attack
  It is a fact that hackers from Hezbollah and Hamas have carried out successful cyberattacks against Israel including hacking security cameras installed in government buildings or Hamas hacking smartphones of IDF soldiers using seductive images.
- Bangladesh bought mass spying equipment from Israeli company
  Documents and statements obtained by Al Jazeera's Investigative Unit show that the Bangladesh army purchased the Israeli equipment in 2018 using a Bangkok-based middleman and Bangladeshi military intelligence officers were trained in Hungary by Israeli intelligence experts.
- Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources
  Suspected Chinese hackers exploited a flaw in software made by SolarWinds Corp to help break into U.S. government computers last year, five people familiar with the matter told Reuters, marking a new twist in a sprawling cybersecurity breach that U.S. lawmakers have labeled a national security emergency.

Cyber Opportunities: Economy, Research & Innovation

- The risk of giving in to quantum progress

Over the next few years the tech industry has a roadmap to overcome the challenges facing quantum computing. This will pave the way to growth in mainstream quantum computing to solve "hard problems".

- [Google's mega-capacity new transatlantic submarine cable is ready for action]
  Google's Transatlantic Dunant submarine cable system is ready for service, almost two-and-a-half years after announcing the project to bolster network capacity and resilience for Google Cloud customers.
- [Switzerland ushers in new era as blockchain law takes effect]
  Switzerland has ushered in a new era for the digital assets industry after the tokenized securities law took effect on February 1. Known as the Blockchain Act, it sets a firm legal basis for digital asset exchange and tokenization while tackling the threat of digital currency money laundering.
- [Is ethical risk getting the better of artificial intelligence?]
  Beneath the exciting tide of artificial intelligence (AI) applications permeating industries and consumers' daily lives, there has been an undercurrent growing in strength over years: the question over whether we can trust the decisions of morally-void autonomous systems, informed by and interpreting only the datasets they receive.

Italian Focus

- [TikTok will recheck the age of every user in Italy after DPA order]
  TikTok has agreed to re-verify the age of every user in Italy and block access to users who state they are younger than 13, the country's data protection agency said today.

- [Cyber attacks must be reported within an hour. It won't be easy for companies]
  The Dpcm on the Cyber National Security Perimeter, which regulates notifications and security measures in case of accidents, has arrived in Parliament. Experts report the impact on businesses
- [Cyber security, this is what the new Decree provides (on standby because of the crisis)]
  The DPR on the Cyber National Security Perimeter is ready but its approval process in the CDM crosses government crises and consultations.
- [Fake MISE e-mail, new bait to steal data: the details of the scam]
  A new malspam campaign is underway aimed at Italian users to spread Ursnif/Gozi banking malware through a fake e-mail from the MISE with tax breaks and aid to businesses.

European Focus

- [EU claims court errors in bid to overturn €13 billion Apple tax judgment]

EU antitrust enforcers have claimed a court made legal errors when it scrapped their order for iPhone maker Apple to pay 13 billion euros in Irish back taxes, in a filing to have the verdict overturned.

- Businesses, be warned: There is 'no guarantee' to the free flow of data from Europe
  Businesses in the UK should be preparing now for the looming prospect of personal data transfers from the EU becoming unlawful in a matter of months, which could cause major headaches for any company importing information from the continent, whether that's HR files, customer details or advertising data.
- A network of Twitter bots has attacked the Belgian government's Huawei 5G ban
  Social media research group Graphika has published a report today exposing a small network of 14 Twitter accounts that engaged in a coordinated campaign to criticize the Belgian government's plan to ban Huawei from supplying 5G equipment to local telecommunications providers.
- Europol on defensive as concerns raised over 'illegal' Big Data tactics
  The European Data Protection Supervisor (EDPS) slammed Europol in September after a probe had unearthed evidence of national law enforcement agencies increasingly transmitting 'large datasets' to Europol, as opposed to 'targeted data' proportionate to specific criminal investigations, thereby breaching standards set out in the 2016 Europol Regulation.