Newsletter November 2020

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- **What's behind China's Big Tech crackdown and what does it mean?**
  China's government published draft antitrust rules this week aimed at curbing monopolistic behaviour by its giant internet platforms, a move that analysts believe will lead to increased scrutiny of e-commerce marketplaces

- **India to regulate online news and social media sites**
  India's government has issued an order bringing the regulation of online news portals and content providers such as Netflix under the authority of the Ministry of Information and Broadcasting in a first step to regulate digital media.

- **Singapore to work with UN to help nations implement norms for responsible cyber behavior**
  One of the highlights of this year's conference was an agreement between Singapore and the United Nations (UN) to develop a norms implementation checklist, which comprises a series of steps that countries need to take in order to implement a set of cybersecurity norms for responsible state behaviour in cyberspace.

- **The encryption war is on again, and this time government has a new strategy**
  We could soon be in for a new round of the encryption wars, but this time governments are taking a different approach. Seven governments from across the world have started a new campaign to try and persuade big tech companies to reduce the level of security they offer to customers using their services.

Cyber Security

- **UN warns of impact of smart borders on refugees: 'Data collection isn't apolitical'**
  Robotic lie detector tests at European airports, eye scans for refugees and voice-imprinting software for use in asylum applications are

UNIVERSITÀ DEGLI STUDI FIRENZE | DSPS Dipartimento di Scienze Politiche e Sociali | Centro interdipartimentale Studi Strategici Internazionali Imprenditoriali

among new technologies flagged as "troubling" in a UN report.

- [Ransomware attack on top Brazilian court encrypts files, backups](#)
  The ransomware attack was carried out by unknown operators who are now demanding a ransom for the decryption key.
- [Microsoft says three APTs have targeted seven COVID-19 vaccine makers](#)
  Microsoft says it detected three state-sponsored hacking operations (also known as APTs) that have launched cyber-attacks on at least seven prominent companies involved in COVID-19 vaccines research and treatments.
- [This hacking group is using previously unknown tools to target defence contractors](#)
  Researchers at McAfee first detailed Operation North Star earlier this year, but further analysis reveals additional tactics and techniques of the campaign that has almost identical elements to Hidden Cobra – AKA The Lazarus Group – a hacking operation which the US government and others say is working out of North Korea on behalf of the government in Pyongyang.

Cyber Warfare, Intelligence and Terrorism

- [US charges Russian GRU officers for NotPetya, other major hacks](#)
  A federal grand jury returned an indictment against six alleged Russian intelligence officers who, collectively
- [US plans to 'vigorously defend' TikTok ban order despite ruling](#)
  The United States Department of Commerce says it will "vigorously defend" an executive order that seeks to bar transactions with Chinese-owned short video-sharing app TikTok after a federal judge halted the action.
- [Cyberattack strikes media-monitoring company used by Australian government](#)
  A media-monitoring and analytics firm used by the federal government has been hit by a cyberattack, prompting the involvement of the nation's leading cybersecurity agency.
- [Russia planned cyber-attack on Tokyo Olympics, says UK](#)
  Russian military intelligence services were planning a cyber-attack on the Japanese-hosted Olympics and Paralympics in Tokyo this summer in an attempt to disrupt the world's premier sporting event,

Cyber Opportunities: Economy, Research & Innovation

- [What's quantum computing? CERN's new free online course offers you the answer](#)
  Sweden has banned telcos from using Huawei or ZTE network equipment for their 5G rollouts as the nation joins a growing list of western countries that have restricted the Chinese companies' involvement due to security

concerns.

- [IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain](#)
  Supply chains are currently facing a broad range of threats, from physical threats to cybersecurity threats. Organisations are becoming more dependent than ever before on third parties. As organisations cannot always control the security measures of their supply chain partners, IoT supply chains have become a weak link for cybersecurity.
- [Google patches two more Chrome zero-days](#)
  Google has released today Chrome version 86.0.4240.198 to patch two zero-day vulnerabilities that were exploited in the wild. These two bugs mark the fourth and fifth zero-days that Google has patched in Chrome over the past three weeks.
- [Computer Scientists Achieve the 'Crown Jewel' of Cryptography](#)
  All cryptographic protocols rest on assumptions. A cryptographic protocol is only as secure as its assumptions. The new protocol of indistinguishability obfuscation, by contrast, depends on security assumptions that have been widely used and studied in the past.

Italian Focus

- [Reading about Intelligence](#)
  A new bibliography of Intelligence, six years after the first edition. A necessary update, of course. But to adapt not only to editorial news: also, and even more, to the world that is reflected in them, in the perennial game of mirrors between reality and its interpretation without which we would be unable to face the time we are given to live.
- [Italian beverage vendor Campari knocked offline after ransomware attack](#)
  Campari Group, the famed Italian beverage vendor behind brands like Campari, Cinzano, and Appleton, has been hit by a ransomware attack and has taken down a large part of its IT network.
- [Italian watchdog investigates Google over alleged advertising market abuse](#)
  The watchdog said it suspects Google of using enormous amounts of data collected through its own applications to prevent rival operators from competing effectively. It said it carried out inspections of some Google offices on Tuesday (28 October).
- [Cyber and 5G, newly founded Italian Institute of Cybersecurity](#)
  A foundation for cyber-security, coordinated by Prime Minister Giuseppe Conte and intelligence. Among the folds of the draft budget, in article 96, the birth of the "Italian Institute of Cybersecurity" (IIC) is announced.

European Focus

- [EU aid funding surveillance regimes, privacy campaigners claim](#)

  EU bodies are providing border and migration authorities in non-member countries with surveillance tools, including wiretapping systems and other phone surveillance products, in a bid to 'outsource' the EU's border controls, says PI.

  - [Europe lays out antitrust case against Amazon's use of big data](#)

  The European Commission has laid out a first set of antitrust charges against Amazon focused on its dual role as a platform for other sellers but also a retailer itself on its own platform

- [What's all this about Europe wanting crypto backdoors?](#)

  There have been discussions ongoing between Member States on the topic of encryption — and whether/how to regulate it — for several years now.

- [Data sharing services must be 'established in the EU,' leaked regulation reveals](#)

  In the establishment of EU common data spaces as part of the bloc's forthcoming data strategy, providers of new data sharing services must be established in the EU and should avoid 'conflicts of interest' in collecting new troves of data.