Newsletter October 2021

Upcoming Events

21st Oct Women in Cybersecurity

6th Nov HackinBo

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- US leads world in bitcoin mining after China crackdown sends industry overseas
  The United States has overtaken China to account for the largest share of the world's bitcoin mining, according to data published by researchers at Cambridge University.
- Russia excluded from 30-country meeting to fight ransomware and cyber crime
  Russia was not invited to attend a 30-country virtual meeting led by the United States that is aimed at combating the growing threat of ransomware and other cyber crime, a senior administration official said.
- How Will Japan's Cybersecurity Posture Impact its Relations With China?
  Japan's new Kishida government seeks to bolster the national response to cyber threats from China, the country's largest export market. What could go wrong?
- Thailand's cybersecurity negligence causes personal data breaches
  Thailand's cybersecurity readiness has come under question, after reports that tourists' personal details were recently exposed online, potentially hurting a much-needed recovery of the key sector.
- Put Aside Grand Geopolitical Plans: First Fix Transatlantic Digital Plumbing
  Global tech rules have given birth to a confusing, unproductive and often conflictual alphabet soup of acronyms: DEPA, DFFT, GDPR, CPTPP. Now there's a new acronym: TTC, the transatlantic Trade and Technology Council (TTC), which launches last week in Pittsburgh.

Cyber Security

- European Cybersecurity Month: 'Think Before U Click'

The ninth edition of the European Cybersecurity Month began on 1 October and will run for the entire month of October under the motto 'Think Before U

Click'. This is an annual awareness campaign organized by the Commission, the European Union Agency for Cybersecurity (ENISA) and over 300 partners in the member states, including local authorities, governments, universities, think tanks, NGOs and professional associations.

- Twitch confirms massive data breach
  Game-streaming platform Twitch has been the victim of a leak, reportedly divulging confidential company information and streamers' earnings. More than 100GB of data was posted online on Wednesday (6th October). The documents appear to show Twitch's top streamers each made millions of dollars from the Amazon-owned company in the past two years.
- Opinion: Cyber piracy has hurt Ireland this year - but we can affect change internationally
  To guarantee its cyber security, Ireland needs to join the push for action against rogue states. The ransomware attack carried out in May against the HSE was Ireland's first taste of mass-scale cyber piracy and the severe infrastructural damage it can visit upon states and their citizens
- Google warns of surge in activity by state-backed hackers
  Google has warned of a surge in activity by government-backed hackers this year, including attacks from an Iranian group whose targets included a UK university.

Cyber Warfare, Intelligence and Terrorism

- Microsoft: Russia behind 58% of detected state-backed hacks
  Russia accounted for most state-sponsored hacking detected by Microsoft over the past year, with a 58% share, mostly targeting government agencies and think tanks in the United States, followed by Ukraine, Britain and European NATO members, the company said.
- UK cyber head says Russia responsible for 'devastating' ransomware attacks
  Cyber-attacks which see hackers get inside computer networks and lock the owners out until they pay a ransom present "the most immediate danger" to UK businesses in cyber-space, the head of the National Cyber Security Centre (NCSC) has warned.
- Report: Suspected Chinese hack targets Indian media, gov't
  A U.S.-based private cybersecurity company said Wednesday it has uncovered evidence that an Indian media conglomerate, a police department and the agency responsible for the country's national identification database have been hacked, likely by a state-sponsored Chinese group.
- Belarusian hacktivists claim drone attack on riot police base in Minsk
  Belarusian cyber-activists claim to have targeted a riot police building in northeastern Minsk in a first-of-its-kind drone attack last month. Busly Latsyats (Flying Storks) was formed on

November 13 last year amid an ongoing crackdown on dissent over Belarus' disputed presidential election.

Cyber Opportunities: Economy, Research & Innovation

- Does the NFT craze actually matter?
  The NFT market is still defying reason, but then again that's kind of its thing. But one thing I'm especially unsure about lately as I see JPGs continue to sell for millions of dollars is… does any of this actually matter?
- How Intellectual property could be Transferred through the Blockchain Ecosystem
  While the world has evolved from storing and transferring information from paper to cloud storage, data is still not entirely protected. The existing cloud storage system used for sharing information while encrypted is centralized, and centralized systems have the inherent disadvantage of being vulnerable to hacks and attacks.
- Much 'Artificial Intelligence' Is Still People Behind a Screen
  The practice of hiding human input in AI systems still remains an open secret among those who work in machine learning and AI.

Italian Focus

- How the Mafia Is Pivoting to Cybercrime
  Police in Europe announced Monday that they had arrested more than 100 people connected with Mafia organizations that were employing hackers to support traditional crimes such as extortion and drug trafficking.
- Phishing attacks: Police make 106 arrests as they break up online fraud group
  Police have dismantled an organised crime group linked to the Italian mafia that defrauded hundreds of victims through phishing attacks and other types of online fraud. The joint operation was led by the Spanish National Police, with support from the Italian National Police, Europol and Eurojust and has resulted in 106 arrests across Spain and Italy.
- Our healthcare system is at risk for cyber attacks
  Italian healthcare system has lately attracted the wrong attention; in spite of the efforts during the Covid emergency, digitalization has created many problems to the national infrastructures.
- TA544 threat actors hit Italian firms with Ursnif banking Trojan
  The IT security researchers at Proofpoint have discovered a new malware campaign in which threat actors from a group called TA544 are targeting organizations in Italy with Ursnif banking trojan.

European Focus

- European Parliament calls for increased EU cybersecurity capacity

In a resolution on the state of the EU cyber defence capabilities, the European Parliament called on the European Commission and EU member states to increase spending and staff dedicated to cyber defence.

- Cyberdefence, EU is a patchwork that needs to be solved

The barriers set by the Member States to protect their defense powers, both traditional and cyber, block the use of effective supranational instruments. The EU defence is still based exclusively on a set of coordination, standardisation and suggestions.

- EU and US vow to boost microchip supplies and promote trustworthy AI

  The European Union and the United States have set the stage for a new era of closer cooperation to determine the rules of trade and technology of the 21st century while simultaneously boost their domestic industries and achieve greater self-reliance.
- EU warns Russia over 'Ghostwriter' hacking ahead of German elections

  The European Union has warned it may take action over Russia's involvement in 'malicious cyber activities' against several EU member states.