Newsletter May 2020

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- France to impose digital tax this year regardless of any new international levy
  France will tax big digital businesses this year whether there is progress or not towards an international deal on a levy, its finance minister said on Thursday (13 May), adding such a tax had never been more legitimate or more necessary.
- New US-Poland 5G pact: Will it help loosen Huawei's grip on Europe?
  The US and Poland have just signed a deal to strengthen cooperation on 5G technology, in a bid to challenge Chinese giant Huawei's growing influence over Europe's mobile infrastructure. The agreement was signed on Monday by US vice president Mike Pence and Polish prime minister Mateusz Morawiecki.
- China's Cybersecurity Reviews Eye 'Supply Chain Security' in 'Critical' Industries [Translation]
  The final Cybersecurity Review Measures for 'critical information infrastructure' come three years after the Cybersecurity Law went into effect
- Dealing with Russia's brazenness in cyber space
  Western governments recently attributed to Russia a massive cyber-attack against Georgia. In this and other situations, the brazenness of the attack was seemingly a goal in itself. But Russia is not the only cyber threat. Structural political incentives for better security practices and international solidarity and assistance are needed.
- Poland plans revenue surcharge on Netflix and others
  Poland plans to introduce a 1.5% surcharge on the revenue of video-on-demand platforms such as Netflix, Finance Minister Tadeusz Koscinski said on Wednesday (29th April).
- Australia served Microsoft nearly 900 data access requests in six months
  Under Australian laws such as the Telecommunications (Interception and Access) Act 1979 and the Mutual Assistance in Criminal Matters Act 1987, government authorities can issue foreign companies that operate in Australia, like Microsoft, with requests for data.

Upcoming Events

The Center is pleased to announce a collaboration with the Embassy of the Unit States of America in Italy. The initiative aim raising awareness on risks and opportunitie cyberspace to build a resilient society.

We are hiring! To learn more about our internship opportunity, click here

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

Cyber Security

- Interpol declares WannaCry anniversary the Anti-Ransomware Day

May 12 will now be regarded as the global Anti-Ransomware Day, a day dedicated to raising awareness about the potent danger that cybercrime poses. The global awareness campaign was announced by Interpol in partnership with cybersecurity company Kaspersky.

- Hackers who stole data from entertainment law firm threaten to release Trump's 'dirty laundry'

  Hackers who have stolen data from a major entertainment law firm have threatened to release Donald Trump's "dirty laundry" unless they receive $42m (£35m) in ransom.
- Supercomputers hacked across Europe to mine cryptocurrency

  Multiple supercomputers across Europe have been infected this week with cryptocurrency mining malware and have shut down to investigate the intrusions.
- Companies wrestle with growing cyber security threat: their own employees

  As cyber criminals and hackers ramp up their attacks on businesses amid coronavirus-related disruption, companies are also facing another equally grave security threat: their own employees.
- The Lack of Women in Cybersecurity Leaves the Online World at Greater Risk

  Women are highly underrepresented in the field of cybersecurity. In 2017, women's share in the U.S. cybersecurity field was 14%, compared to 48% in the general workforce.

Cyber Warfare, Intelligence and Terrorism

- FBI, DHS Confirm China-Backed COVID-19 Hacking Activity

  The FBI and the Cybersecurity and Infrastructure Agency on Wednesday said they were probing attempts by Chinese government-aided hackers and others to target U.S. organizations conducting research on vaccines, treatments and testing related to the COVID-19 pandemic
- Blind faith in technology diverts EU efforts to fight terrorism

  If there is one thing the coronavirus crisis proved to us is that automated tools used by big social media companies completely fail to provide a suitable online space for the exchange of vital health-related information.
- Huawei's surveillance system in Serbia threatens citizens' rights, watchdog warns

  Serbia wants to use technology to improve public safety in its capital, Belgrade. To that end, it has decided to implement Huawei's Safe City Solution – a surveillance system that includes the installation of thousands of security cameras.
- Telegram — a free speech Russian platform is a haven for far-Right terror groups

In recent years, Telegram, a point-to-point communications app, has seen an influx of extremist channels using the platform's "public channel" feature to foster online communities. These range from channels dedicated to sharing "politically incorrect" jokes and memes to more virulent channels explicitly aligned with far-right terror groups.

- Iran Is Increasing Its Military and Cyber Activity, Report Says
  Few countries were hit as hard by the COVID-19 pandemic as Iran, which has seen more than 114,000 confirmed cases. But in recent weeks, open-source intelligence gleaned from Persian- and Arabic-language sources, as well as commercially available location data from mobile devices, suggests that Iranian military activity did not drop off as severely as civilian activity, according to data analytics company Babel Street.
- Cyber threats and hybrid war. The NATO strategy
  On 20th February, US, UK and other NATO states have publicly accused Russia of the October cyberattack against Georgian infrastructures. The attacks have compromised the governmental and private websites and endangered Georgian national security.

Cyber Opportunities: Economy, Research & Innovation

- Zoom acquires Keybase to get end-to-end encryption expertise
  Keybase, which has been building encryption products for several years including secure file sharing and collaboration tools, should give Zoom some security credibility as it goes through pandemic demand growing pains.
- Microsoft patches 111 vulnerabilities in May 2020 Patch Tuesday
  May Patch Tuesday update is the third-largest in Microsoft's history. The other two large updates were released in March and April this year, in which the company patched 115 and 113 bugs, respectively.
- The introduction of blockchain in the supply chain
  With new technologies such as AI, Big Data and blockchain at companies' fingertips, there is an increasing importance to adopt new processes into operations to maintain a proactive supply chain approach.
- Artificial intelligence is struggling to cope with how the world has changed
  From our attitude towards work to our grasp of what two metres look like, the coronavirus pandemic has made us rethink how we see the world. But while we've found it hard to adjust to the new reality, it's been even harder for the narrowly-designed artificial intelligence models that have been created to help organisation make decisions.

Italian Focus

- Italian CSIRT is on: how it will change national cyber defence
  The Computer Security Incident Response Team will protect our country from cyberattacks and coordinate the responses within a Crisis Management framework
- Immuni, COPASIR stopped the Italian tracking app
  The report from COPASIR depicted a grave scenario. Italians' data could be exposed to the Chinese society Nuo Capital and therefore potentially to the Chinese government. Too many procedural errors have been highlighted so far.
- Power grid operators launch blockchain for home and car batteries
  European electricity grid operators TenneT, Swissgrid and Terna have launched a cross-border blockchain platform, saying it will help stabilise the grid while allowing households to earn "a few hundred euros per year" from their home and car batteries.
- Digital PA, the pandemic has 'pushed' the digitalization: now it's up to us
  As citizens and employers, we had to face a new way to conceive our work in a world more and more digitalized. Now we need to embrace these newly found instruments and exploit their potentialities, even beyond the quarantine period.
- Smart working, Linkem and Kaspersky allied for cybersecurity
  The deal was struck to meet the private business and private citizens' needs. Francesco Sortino: "We will give them the instruments to protect personal and business data from cyberattacks"

European Focus

- Commission seeks 'largest possible participation' of EU citizens for COVID-19 apps

"The largest possible participation of EU citizens is necessary to exploit the full potential of tracing apps," stated one Commission document addressing a series of questions on the measures announced on Wednesday (13 May).

- France gives online firms one hour to pull 'terrorist' content

The one-hour deadline applies to content that French authorities consider to be related to terrorism or child sexual abuse. Failing to act could result in fines of up to 4% of global revenue - billions of euros for the largest online firms. But critics say the new law could restrict freedom of expression.

- Sharing is caring: technical cooperation across CSIRTs, LE and the judiciary
  In an effort to estimate the degree of maturity of the technical cooperation across national and governmental CSIRTs, law enforcement agencies (LEAs) and the judiciary when it comes down to cybercrime investigation, ENISA has prepared a report that focuses on the tools of these communities to cooperate among themselves and counter cybercrime.

- Council extends cyber sanctions regime until 18 May 2021
  Over recent years, the EU has scaled-up its resilience and ability to prevent, discourage, deter and respond to cyber threats and malicious cyber activities in order to safeguard European security and interests.
- Austrian ministry could face GDPR penalty after publishing personal data online
  Austrians' personal data has been publicly accessible on the ministry of economy's website since 2009. The liberal party NEOS and NGO epicenter.works call it the "biggest data protection scandal of the Second Republic."