Newsletter April 2020

Center for Cyber Security and International Relations Studies

Upcoming Events

In the light of the recent developments concerning COVID-19 and the Italian government's decisions, the section will remain blank

Cyber Policy, Diplomacy & Legal Framework

- The US Is Waging War on Digital Trade Barriers
  As digital trade barriers rise throughout the world, so do swings at knocking them down. In the past two months, the US Trade Representative released two reports on China and Russia's World Trade Organization compliance.
- Brazil-EU Cyber Cooperation: Swinging Bridges on the Road to Stability in Cyberspace
  The February 20 Brazil-EU Cyber Dialogue signaled the most recent step taken by Brasília and Brussels to collaborate on advancing responsible state behavior in cyberspace. While there have sometimes been differences in the two parties' approaches to this challenge, their cooperation is crucial in the current geopolitical climate where cyber threats will continue to proliferate.
- China's next plan to dominate international tech standards
  Security experts warn that holes in the Zoom app's technology make user data vulnerable to exploitation. Its CEO, Eric Yuan, has publicly admitted their lacks concerning privacy and security. However, we might have neglected a larger point.
- White House strategy paper to secure 5G envisions America leading global 5G development
  Though light on details, the paper offers clues as to how the US government sees the development and security of 5G communications moving forward.
- Brazilian president shelves plans for surveillance in fight against coronavirus
  The decision was made public by the minister of science, technology, innovation and communications, Marcos Pontes, who posted details on his social networks on Sunday (12), citing concerns over citizen privacy.

Cyber Security

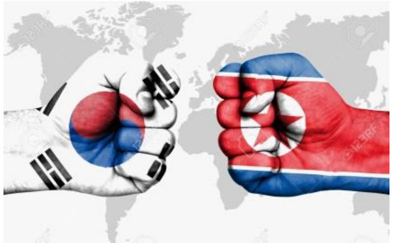
- Hackers are scanning for vulnerable VPNs in order to launch attacks against remote workers
  The number of cyberattacks attempting to exploit the coronavirus outbreak for their own

gain continues to rise as both cyber-criminal groups and nation-state-backed hacking operations attempt to take advantage of the COVID-19 pandemic.

- BlackBerry: Chinese cybercriminals target high-value Linux servers with weak defenses
  Linux malware is real and Advanced Persistent Threat (APT) groups have been infiltrating critical servers with these tools for at least eight years, according to a new report from BlackBerry.
- Firefox gets fixes for two zero-days exploited in the wildFirefox users are advised to update their browsers to patch two bugs that are being exploited in the real world by hackers. The fixes are available in Firefox 74.0.1, released earlier today. This new Firefox version includes fixes for CVE-2020-6819 and CVE-2020-6820, two bugs that reside in the way Firefox manages its memory space.
- Taiwan takes down top piracy site
  One of Taiwan's top movie and TV download sites, 8maple.ru, has been shut down and the assets of two engineers have been frozen on suspicion of infringing intellectual property rights.
- How Microsoft Dismantled the Infamous Necurs Botnet
  At the height of its powers, Necurs was one of the most disruptive forces on the internet. A sort of Swiss Army botnet, over the years it has harnessed more than 9 million computers unwittingly under its control to send spam, distribute ransomware, attack financial institutions, and more. Last week, Microsoft pulled its plug.

Cyber Warfare, Intelligence and Terrorism

- An Elite Spy Group Used 5 Zero-Days to Hack North Koreans
  Most Northern Koreans don't spend much of their lives in front of a computer. But some of the lucky few who do, it seems, have been hit with a remarkable arsenal of hacking techniques over the last year—a sophisticated spying spree that some researchers suspect South Korea may have pulled off.



- WhatsApp’s spyware lawsuit against NSO Group could change cyber espionage laws forever
  Almost six months after it was served with a lawsuit by WhatsApp, the controversial Israeli spyware company NSO Group took its first substantive action in relation to the court case last week – it filed a motion to dismiss it on several grounds.
- Coronavirus: Chinese Hackers APT41 Seek Exploits Amid Pandemic

Security researchers at FireEye have warned of a “widespread hacking campaign” being carried out by APT41, one of the most effective hacking teams backed by the Chinese government.

- Private Battles Become More Public as China Accuses CIA of 11 Years of Cyber Espionage
  Discussion of state-sponsored advanced persistent threat (APT) groups tends to focus on Russia, North Korea, Iran, and above all China. FireEye currently lists 10 APT groups as being attributed to China, far more than any other country.
- How destructive ransomware attacks could represent the future of cyberwarfare
  The increasingly destructive capabilities of ransomware attacks could provide nation-state hacking operations with a means of attacking infrastructure – and the ability to plausibly deny any sort of involvement in campaigns.

Cyber Opportunities: Economy, Research & Innovation

- Debunking Myths about Quantum Cryptography

Quantum computing has long captured the imagination of the technology industry, and last year’s news of Google reaching a “quantum supremacy” milestone planted a real stake in the ground.

- Irish team’s breakthrough set to boost quantum computer efficiency
  One of the ‘holy grails’ of computer science is to achieve a stable, small-scale quantum computer that would exceed the capability of even the most powerful binary supercomputer.
- G20 Watchdog Warns Nations to Mitigate Risks Posed by Libra-Like Stablecoins
  The Financial Stability Board (FSB) has warned national regulators to review standards and address any possible disruptions caused by global stablecoins such as Libra.
- Zoom data scandal shows blockchain may be the future of communications
  As people around the world started following shelter-in-place orders, popular video conferencing platform Zoom quickly gained new users, noting in a recent blog post that it had reached more than 200 million daily users last month, up from 10 million in December.

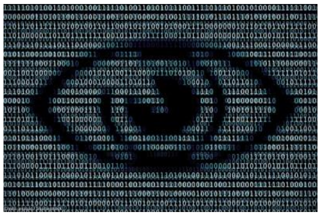
Italian Focus

- DDoS attacks took down Italy’s social security website amid COVID-19 crisis
  Frequent cyber-attacks forced Italy’s social security and welfare department to temporarily shut down its website at a time when thousands of vulnerable citizens were trying to apply for financial assistance in the middle of the crisis.

- Staff mailboxes at Italy's Monte dei Paschi suffer hacker attack: document
  Hackers have accessed the mailboxes of some employees at Italian state-owned bank Monte dei Paschi and sent emails to clients, according to a notice to customers seen by Reuters. Monte dei Paschi told clients in the notice that on March 30 some messages with voice mail attachments had been sent as a result of the cyber attack.
- Sanitary emergency and digital divide: wrecking the bureaucracy to restart
  Because of the sanitary emergency, the country has re-discovered its differences and has gained the willingness to overcome them. Regions need to do their part without depending entirely on national companies and parastatal subjects.
- Online education, the challenge is global: priorities and difficulties
  According to UNESCO, the number of students forced home has increased to a billion. For the first time, many digital instruments have been activated on large scale, but there are still many problems to tackle down. Situation and future strategies.
- Tim, Google, Microsoft and Netflix. Who's helping Italy against Covid-19
  From mobility to school, through finance and insurance companies, as well as entertainment industries: big corporations, tech companies and startups are developing projects to sustain Italy in this tough moment.

European Focus

- Privacy activists on COVID-19 surveillance: Either ineffective or questionable



  To combat the coronavirus pandemic, some governments have been tempted to monitor their citizens using Big Data. In Germany and Austria, there are concrete ideas, but to be truly effective, the methods would have to be deeply invasive, say privacy activists.
  - An EU Committee Calls for Crypto Rules w/ International Standards

  A committee of the European Parliament calls for the end of crypto-related regulatory arbitrage - a way to use loopholes in regulatory systems to avoid unfavorable regulations - proposing that crypto regulation should be made at the international level.
- How the 5G coronavirus conspiracy theory tore through the internet
  From an interview with an obscure Belgian doctor to apparent arson attacks in the UK, the conspiracy theory that 5G is somehow linked to the coronavirus pandemic has spread unlike any other
- EU under pressure to broker online terrorist content agreement
  The European Council and Commission are under pressure to make headway on rules to stamp out online terrorist content, the substance of which could provide a precedent for the upcoming Digital Services Act, an MEP involved with the matter has said.

- Call for common EU approach to apps and data to fight COVID- 19 and protect citizens' rights
  The European Commission has responded to the regional scramble for apps and data to help tackle the coronavirus crisis by calling for a common EU approach to boost the effectiveness of digital interventions and ensure key rights and freedoms are respected.