Newsletter March 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

- Digital identities: Why this Balkan country aims to match Estonia's successes
  While many western Balkan countries are only in the early stages of developing their digital economies, a few have been taking bold steps. Take, for example, North Macedonia. By teaming up with payments giant Mastercard, it is set to become the first country in the region to implement digital identities, emulating tiny Baltic state Estonia, which has had some success in this area.
- Estonia raises cybersecurity issues at UN for first time
  Estonia raised the issue of the October 2019 Russian cyber attacks on Georgia at the UN Security Council (UNSC) on Thursday, the first time the question has been officially discussed in its own right. Estonia, a non-permanent UNSC member, condemned the attacks and was joined by permanent members the United States and the United Kingdom.
- Dutch government loses hard drives with data of 6.9 million registered donors
  The Dutch government said it lost two external hard disk storage devices that contained the personal data of more than 6.9 million organ donors. The hard drives stored electronic copies of all donor forms filed with the Dutch Donor Register between February 1998 to June 2010, officials from the Dutch Minister of Health, Wellness, and Sport said earlier this week.
- Has Australia just deregulated government cyber-compliance?
  One of the biggest barriers to digital transformation is flexibility or a lack of it — that's often because stringent regulations have to be imposed to satisfy cybersecurity needs and data privacy requirements.
- The EARN IT Act Is a Sneak Attack on Encryption
  A bipartisan pair of US senators today introduced long-rumored legislation known as the EARN IT Act. Meant to combat child sexual exploitation online, the bill threatens to erode established protections against holding tech companies responsible for what people do and

say on their platforms. It also poses the most serious threat in years to strong end-to-end encryption.

Cyber Security

- Coronavirus-linked hacks likely as Czech hospital comes under attack

As countries around Europe enact drastic measures to try to contain the spread of the Covid-19 coronavirus, a hospital in Brno, Czechia, has been forced to cancel all planned operations and farm out acute patients to other hospitals after falling victim to a major cyber attack.

- Tor team warns of Tor Browser bug that runs JavaScript on sites it shouldn't

  The Tor Project warned users about a major bug in its browser that may execute JavaScript code on sites that users have specifically blocked JavaScript from running. Tor developers said they are working on a fix; however, they did not provide a timeline for a patch.
- Push Security to the Edge: Overcoming Edge Computing Challenges

  While most data centers are the focus of cybersecurity hardening, edge computing environments can sometimes be overlooked. Given this, groups like MoneyTaker exploit edge environments to make, or rather take, their money. Working in complete secrecy for over a year-and-a-half in 2016-17, they pulled off over 20 successful attacks and took away an average of $500,000 per incident in the U.S.
- Necurs Botnets Busted

  Eleven Necurs botnets, which infected more than nine million computers since 2012, have been severely disrupted. The botnets were dealt a blow through the joint efforts of BitSight, Microsoft's Digital Crimes Unit (DCU), and by partners across 35 countries.
- Windows Has a New, Wormable Vulnerability

  Word leaked out on Tuesday of a new vulnerability in recent versions of Windows that has the potential to unleash the kind of self-replicating attacks that allowed the WannaCry and NotPetya worms to cripple business networks around the world.

Cyber Warfare, Intelligence and Terrorism

- Russia Is Learning How to Bypass Facebook's Disinfo Defenses

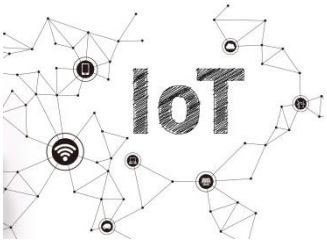
  Since Russia's stunning influence operations during the 2016 United States presidential race, state and federal officials, researchers, and tech companies have been on high alert for a repeat performance. With the 2020 election now just seven months away, though, newly surfaced social media posts indicate that Russia's Internet Research Agency is adapting its methods to circumvent those defenses.
- UK says Russia's GRU behind massive Georgia cyber-attack

A huge cyber-attack which knocked out more than 2,000 websites in the country of Georgia last year was carried out by Russia, according to Georgia, the UK and the US.

- Hackers Join Forces Against U.S. And Israeli Targets: This Is What An Iranian Cyber Attack Looks Like In 2020
  Ever since the 2010 Stuxnet worm attack on the Natanz nuclear plant that was eventually attributed to the U.S. and Israeli governments, Iran has been taking "cyber" seriously.
- CIA Accused of Mounting 11-Year Cyber-Attack Against China
  A security company has accused America's Central Intelligence Agency (CIA) of waging an 11-year campaign of cyber-espionage against critical industries in the People's Republic of China.
- U.S. targets North Korean hackers, money sources as talks sputter
  U.S. officials are engaged in an intense behind-the-scenes campaign with foreign allies to cripple North Korea's cyber-hacking and fundraising capabilities, as consensus grows in the Trump administration that nuclear talks with Pyongyang will remain stalled for the coming year.
- State-sponsored hackers are now using coronavirus lures to infect their targets
  Government-backed hacking groups from China, North Korea, and Russia are not letting a global pandemic go to waste and have begun using coronavirus-based phishing lures as part of their efforts to infect victims with malware and gain access to their infrastructure.

Cyber Opportunities: Economy, Research & Innovation

- Why internet of things security is surprisingly on the decline
  espite years of attention to the dangers of insecure internet-connected devices, internet of things security is declining, "leaving organizations vulnerable to new IoT-targeted malware as well as older attack techniques that IT teams have long forgotten," Palo Alto Networks said in an IoT report out.



- Amazon announces four new projects to make its data centers greener
  Amazon is launching four new renewable energy projects across the globe in the next couple of years, designed to supply green power for the data centers operated by its cloud computing subsidiary AWS.
- Most Medical Imaging Devices Run Outdated Operating Systems
  You'd think that mammography machines, radiology systems, and ultrasounds would maintain the strictest possible security hygiene. But new research shows that a whopping 83 percent of medical imaging devices run on operating systems that are so old they no longer receive any software updates at all.
- AI is an Ideology, Not a Technology

Without the constraints on data collection that liberal democracies impose and with the capacity to centrally direct greater resource allocation, the Chinese will outstrip the West. AI is hungry for more and more data, but the West insists on privacy. This is a luxury we cannot afford, it is said, as whichever world power achieves superhuman intelligence via AI first is likely to become dominant.

Italian Focus

- How The Coronavirus Is Forcing Italy To Become A Digital Country, At Last
  It's certainly a small thing, compared to the grief and losses of many, but the Coronavirus emergency is forcing citizens and institutions to come to terms with digital technologies, at last.

- Italy without high-speed Internet, the damages of wrong political decisions
  At a moment when Internet is capital for economy, education, and institutional and human relations, too many Italians are discovering the damages of the infrastructural digital divide. The development of high-speed Internet arrived too late to turn the trend.
- Italy's new Digital Services Tax is now in force
  With the 2020 Budget Law, the Italian government has reshaped Italy's digital services tax (DST), mirroring the EU Commission proposal of March 2018. The revised version of the Italian DST is now in force effective January 1, 2020.
- New Cyber Security Framework: tools and procedures to protect private infrastructures
  The development of cybercrime and the introduction of new norms have modified our approach to information security. Now, business companies need to adapt to these changes and embrace an approach based on threat detection and response.

European Focus

- Europe's digital vision, explained
  In the global fight for tech supremacy, Europe is taking its gloves off. The EU's executive arm on Wednesday unveiled a series of proposals laying out the bloc's approach to data, artificial intelligence and platform regulation over the next five years and beyond.

- European electricity association warns of office network breach
  An association of European electricity companies has confirmed that hackers have breached its office network. "ENTSO-E has recently found evidence of a successful cyber intrusion into its office network," the association said in a statement. It

added that a risk assessment had been performed and contingency plans are now in place to reduce the risk and impact of any further attacks.

- The ePrivacy Regulation saga three years on
  The Croatian Presidency is the latest member state with responsibility to resolve the ePrivacy Regulation conundrum. The latest texts clarify the scope of the Regulation to include machine-to-machine communications and the internet of things as well as introduce "legitimate interest" as grounds for processing metadata and utilising the user's terminal equipment.
- Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace
  On 28 October 2019, Georgia was the victim of a targeted cyber-attack causing damage to their social and economic infrastructure. The European Union and its Member States express their concern about the cyber-attack, which showed disregard for security and stability in cyberspace and undermines the development of political, social and economic benefits provided by the Internet and the use of Information and Communication Technologies (ICTs).
- Google confirms plans to move UK users' accounts outside EU jurisdiction
  Google is planning to move its British users' accounts out of the control of European Union privacy regulators, placing them under US jurisdiction instead, the company confirmed late on Wednesday