Newsletter January 2020

Upcoming Events

January 20

CS4CA

January 28

CyberTech

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- Russia Takes a Big Step Toward Internet Isolation
  Over the holidays, the Russian government said it had completed a multi-day test of a national, internal internet known as RuNet, a bid to show that the country's online infrastructure could survive even if disconnected from the rest of the world. The test underscores Russia's broader campaign to control and censor access to digital information within its borders.

- Can the UK government's efforts solve the cyber skills gap?
  The training and certification body's Cybersecurity workforce study 2019, which was based on interviews with 3,200 professionals around the world, revealed the gap in the number of skilled personnel in the region has almost doubled to 291,000 over the past year..
- New digital asset legislation might do more harm to the crypto industry
  The crypto industry has been around for over 11 years now, and for most of that time, its members kept asking for regulatory clarity around the world. Unfortunately, it never actually arrived, despite multiple countries' attempts to tackle the issue.
- India's answer to GDPR: Data protection legislation set to pass this year
- ndia's answer to GDPR, the EU's data protection law, has achieved quite a feat: drawing the ire of both Big Tech and privacy advocates. A second draft of the Personal Data Protection (PDPA) Act (PDF), approved by Narendra Modi's government on December 4, has retained data localization provisions that critics feel over zealously protect personal data.
- Facial recognition laws are (literally) all over the map
  The potential benefits of facial recognition, and biometric data generally, are just too great for governments and corporations to pass up. Existing bans of public-sector use that are based on its present, inaccurate, and discriminatory implementations likely won't be sustainable long-term as the technology improves. At the same time, completely unfettered use of private biometric systems seems incompatible with American values. We're not China, or at least not yet.

Cyber Security

- 'Serious cyber-attack' on Austria's foreign ministry

Austria's foreign ministry has been targeted by a cyber-attack that is suspected to have been conducted by another country. The ministry said the seriousness of the attack suggested it might have been carried out by a "state actor". The hack started on Saturday night and experts warn it could continue for several days.

- Microsoft and NSA say a security bug affects millions of Windows 10 computers
  The vulnerability is found in a decades-old Windows cryptographic component, known as CryptoAPI. The component has a range of functions, one of which allows developers to digitally sign their software, proving that the software has not been tampered with.
- Is Huawei Really More Dangerous than Facebook?
  US President Donald Trump's campaign against leading Chinese technology companies is driven by legitimate concerns. But are they so different from the worries that democratic societies should have about American social-media and technology companies?
- Two-thirds of UK healthcare organisations breached last year
  Nearly three years after WannaCry laid waste to IT systems across the NHS, an apparent institutional failure to address lax cyber security measures has been highlighted by a new report from Clearswift, which has claimed that 67% of UK healthcare organisations experienced some kind of cyber security incident during 2019.
- Now It's Really, Truly Time to Give Up Windows 7
- wo days ago, I finally gave up Windows 7. I don't dislike Windows 10, but there's just always been something special about Windows 7. It was svelte. It actually ran faster and took up less hard drive space than its predecessor, the much-maligned Windows Vista. It looked great. We Windows users could finally hold our heads a little higher around Mac users. And, well, I didn't know how well Windows 10 would work on that old Windows 7 laptop, or how much time it would take to make the transition.

Cyber Warfare, Intelligence and Terrorism

- Yemen in Focus: Cable damage wipes out 80% of country's internet connectivity
  The Falcon cable, which runs underwater in the Red Sea region, affected some 80 percent of Yemen's internet connections, which already suffers from slow speed and frequent cuts. Messages sent to customers from Yemen's main telecommunications companies YemenNet and TeleYemen, confirmed the outage was due to a damaged underwater cable in the Suez canal, which also hit connectivity in Saudi Arabia, Kuwait, Qatar, Sudan and Ethiopia, reports confirmed.

- [If Russia Hacked Burisma, Brace for the Leaks to Follow]
  The oil firm Burisma sits at the center of the Venn diagram of two of the Kremlin's hacking obsessions: It's in Ukraine, Russia's favorite playground for all manner of cyberattacks. And it's at the core of a political controversy that might further divide the US and aid Donald Trump's reelection campaign..
- [An Iranian Hacking Campaign, Social Media Surveillance, and More News]
  In a new report, the security firm Dragos details hacking activity against American electric utilities and attributes it to a group of Iranian hackers called Magnallium. For the past year, Dragos says, the state-sponsored group has been carrying out a broad campaign of so-called password-spraying attacks, which guess a set of common passwords for hundreds or even thousands of different accounts, targeting US electric utilities as well as oil and gas firms.
- [The Iran Cyber Warfare Threat: Everything You Need To Know]
  When news emerged that Iranian general Qassem Soleimani had been killed in a U.S. airstrike on January 3, speculation about an imminent cyberattack was rife. It quickly led to warnings that Iran would retaliate by hitting the U.S. and its allies with a combination of physical and cyber warfare.
- [Calling app ToTok used as 'spying tool' by UAE: Report]
  ToTok, an app released earlier this year, is tracking "every conversation, movement, relationship, appointment, sound and image of those who install it on their phones," NYT investigators and American officials familiar with classified intelligence claimed in the report on Sunday.

Cyber Opportunities: Economy, Research & Innovation

- [2020: The year of seeing clearly on AI and machine learning]

Late last year, I complained to Richard Socher, chief scientist at Salesforce and head of its AI projects, about the term "artificial intelligence" and that we should use more accurate terms such as machine learning or smart machine systems, because "AI" creates unreasonably high expectations when the vast majority of applications are essentially extremely specialized machine learning systems that do specific tasks -- such as image analysis -- very well but do nothing else.

- [New year, new Facebook: Here's what Mark Zuckerberg has promised for the 2020s]
  Ten years ago, Facebook's CEO Mark Zuckerberg made a fresh start to the new decade by publicly pledging that he would learn Mandarin Chinese. The following year, he promised to only eat meat from animals that he had killed himself. Since then, the Zuckerberg new year resolution has been an event eagerly anticipated by fans – but now Facebook's boss has announced that 2020 will mark the end of his year-to-year challenges.
- [How AI is Revolutionizing the Banking Sector]

Artificial Intelligence (AI) is becoming ubiquitous in recent years and its uses are seen in every industry from health, to travel, to banking, to hospitality and finance

- Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates
  This paper offers real-world insights from the UAE blockchain ecosystem to provide decisionmakers with the awareness of challenges and success factors they may face during blockchain implementation.
- Clear standards required for development and use of AI in healthcare
  With digital technologies set to irrevocably change the face of our healthcare systems, the ethical concerns surrounding the use of artificial intelligence (AI) are increasingly gaining prominence in policy circles.

Italian Focus

- sLoad malware is back to strike Italian PEC with fake requests of payement: how to protect our data
  

  A vast malspam campaign is diffusing a variant of the infamous sLoad malware which attacks the Italian PECs. Here's the technical aspects to recognise the infected e-mails and the suggestions to improve the security of personal data.
- Tensions over data privacy cast shadow over potential Greens-Five Star alliance
  A leading Green lawmaker in the European Parliament has hit out at Italy's Five Star Movement (M5S) following revelations that Facebook is investigating the party over potential data misuse. The ongoing tensions between the Greens and M5S over data privacy have poured cold water over speculation that the Italian party could one day join forces with the Greens in the European Parliament.
- Logic security: what is it and how to implement it to protect business data
  Logic security requires a precise set of few rules in order to define the access credentials and the log-in information and to organise the business structure to manage correctly these processes. How to develop a plan for the protection of business data
- Strategic Communication Security
  From the Center Inter-Forces for the management and control of Sicral, the Italian Defence department keeps in check its networks and guarantees the military communications, two capital assets to face international operations or national emergencies
- Cyber security, 2019 in brief according to the Postal Police data
  Phishing, online scams, attacks against critical infrastructures, xenophobic cases, and others are just some of the criminal acts perpetrated online, that the CNAIPIC have studied for the past year.

European Focus

- Make Europe Relevant Again

The competition between the US and China for technological supremacy has revealed Europe's fundamental weakness in the twenty-first century. A community of nation-states built around a shared project to ensure regional peace and prosperity is now surrendering its economic power and autonomy to foreign firms.

- Study says Grindr, OkCupid, and Tinder breach GDPR
  Dating apps Grindr, OkCupid, and Tinder are allegedly spreading user information like sexual preferences, behavioural data, and precise location to advertising companies in ways that may violate privacy laws, according to a study conducted by the Norwegian Consumer Council (NCC).
- ECJ opinion backs EU data transfer contracts
  The European Commission's standard contractual clauses (SCC), used for data transfers between EU and non-EU countries, are "valid", according to a non-binding opinion from an advocate general at the Court of Justice of the European Union (CJEU). The opinion is a symbolic victory for social media giant Facebook, who use SCCs in an bid to safeguard privacy standards for European users of the platform.
- Airbnb wins EU property rules fight
  U.S. homesharing site Airbnb on Thursday won its battle to remain exempt from onerous European property regulations.
- Germany's plans for automatic facial recognition meet fierce criticism
  Germany's Interior Minister Horst Seehofer plans to use automatic facial recognition at 134 railway stations and 14 airports, according to a news report published on 3 January. Although official confirmation of the plan is still missing, an alliance between civil society and politicians has called for the banning of this surveillance technology.