Newsletter January 2019

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- **The government shutdown is affecting US cybersecurity**
  The US Congress shutdown has blocked the development of the newly born Cybersecurity and Infrastructure Security Agency, which is part of the Department of Homeland Security (DHS).
- **The US, Russia and China are managing cyber-war with vodka**
  Last month, former and current officials from US, Russia and China have discussed possible guidelines in case of conflict in the cyberspace
- **Vietnam says Facebook violated controversial cybersecurity law**
  After having passed its new cybersecurity law on January 1, Vietnam has accused Facebook of failing to take down "slanderous content" and thus to violate Vietnamese law in its management of online content, advertising and tax liabilities.
- **In Myanmar the government is considering a new cyber law**
  The Deputy Minister of Transport and Communications U Thar Oo said that a Cyberlaw will be drafted to take action against those who insult the country and people and commit crimes over any communications network.
- **Egypt's Anti-Cyber and Information Technology Crimes Law Protects Investment and Investors**
  In late December, Egypt ratified an Anti-Cyber and Information Technology Crimes Law. The law, made up of 45 articles, revolves around ensuring the safe and secure use of technology.

Cyber Security

- **Hackers Attack Hundreds Of High-Profile German Politicians, Post Private Data Online**
  'Advent calendar-like' hacking attack exposed the weaknesses of the German political world. Private data of many politicians, included Chancellor Angela Merkel's contact information, have been realised by two Twitter accounts.
- **NASA Eyes Blockchain Tech to Secure Aircraft Flight Data**

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

According to experts, blockchain technology can ensure the privacy and security of aircraft flight data in preparation for the release of the new surveillance system, Automatic Dependent Surveillance Broadcast (ADS-B), in 2020.

- [The Biggest Cybercrime Threats of 2019](#)
  Ransomwares, phishing mails, digital ad frauds, violations of cloud technology and criminal use of cryptocurrencies are most likely to be still main cybercrime concerns in 2019.

- [IPv4 vs IPv6: How Two Protocols Run the Internet in 2019](#)
  We are running out of IP addresses. The solution is to pass from the current IPv4 to the now developing IPv6. However, this renovation is already creating some problems as the conversion to the new IP version is slower than estimated.

- [Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war'](#)
  US Mondelez is suing Zurich American Insurance Company for $100m after its claim for cleaning up a massive NotPetya ransomware infection was rejected for being "an act of war" and therefore not covered under its policy.

Cyber Warfare, Intelligence and Terrorism

- [A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps](#)
  ISIS has effectively exploited the power of technology to fuel its rise around the globe. But while major platforms are becoming increasingly inhospitable to terrorists, ISIS is looking for less popular messenger apps.

- [Protecting Democracy In An Age of Cyber-Conflict](#)
  For everything in the real world, there is an online analogy. Internet has increased our connections and created a 'global village', but it has also given us anonymity and an almost indefensible topography.

- [Huawei: who is the businessman arrested in Poland for espionage](#)
  Two men, a Polish citizens expert in cybersecurity and a Chinese business, have been arrested last Tuesday. They are accused of spying for the Chinese secret service and the Polish authorities have also inspected Huawei offices.

- [Technology and Internet. How China is making business in South America](#)
  Chinese tech giants have invested substantial resources in South American countries, overcoming the low purchasing power of the population and the lack of efficient logistic and financial services. The Chinese interest for this region is as much economical as political.

Cyber Opportunities: Economy, Research & Innovation

- **Cryptocurrency analysts predict the end of the Bitcoin bear market**
An independent research boutique specializing in the digital asset market, has studied Bitcoin transaction data and market prices, calculating that Bitcoin investors are (for the most part) done with their selling. Roughly 20% of the global Bitcoin could be lost forever, understanding why is vital

- **5G Is Coming This Year. Here's What You Need to Know**
The transition to new fifth-generation cellular networks will affect smartphones and many other kinds of devices. The high-speed connections will bring positive results on many fields in the future.

- **The Exaggerated Promise of So-Called Unbiased Data Mining**
The 'Feynman trap' explains why ransacking data for patterns without any preconceived idea of what we are looking for is pointless and expensive.

- **How 5G will (also) change the telemedicine**
5G technology will have an impact on the medical field, particularly on the so called telemedicine. Better connection and more efficiency will improve the security and privacy of the IoT medical devices and induce a revolution in the supervision of special patients.

Italian Focus

- **Digital Italy: PAs wasting time and lacking innovation in services and processes will face the Court of Audit**
A Memorandum of Understanding between the Special Commissioner for the Digital Agenda and the President of the Court of Audit has tried to put a stop to the digital inefficiency of the Italian public institutions and offices

- **National cybersecurity: all the open dossier in Italy**
For the Italian government, the 2019 might be the 'year of cybersecurity': the implementation of the European Directives (NIS and GDPR), the application of the Standard Measures for the PAs, the investments for cyber defence, and the focus on future challenges.

- **Cybersecurity: the OESs have been identified**
The interested Ministries have indicated 465 private and public entities as OESs in line with the NIS Directive. Now, it's time to pursue the improvement of the cyber national system

- **ISIS is losing the cyber warfare and in Italy, it is employing young people to covert others**
ISIS is changing its communication strategy online: from mass communication to messages tailored to capture a certain kind of young individuals. It has started to favour quality over quantity.

- [Attacks against critical infrastructures: a national strategy to defend the 'fifth military domain'](#)
  After the cyber-attack of 12th November, in which more than 500.000 e-mail addresses had been violated, the Italian government is focusing on increasing the coordination among its military forces in response to these typologies of threats.

European Focus

- [Draft Ethics guidelines for trustworthy AI](#)
  In March 2019, the final version of these guidelines will be realised by the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG). The guidelines are still open for feedbacks from, AI stakeholders.

- [How can Europe tackle fake news in the digital age?](#)
  Europe is trying to fight against fake news promoting the use of AIs, as well as the education of European citizens to distinguish trustworthy sources.
- [European Banking Authority calls for pan-EU rules on crypto assets](#)
  The patchwork of different rules across the European Union covering crypto assets could be exploited and it leaves the costumers unprotected.