Newsletter March 2018

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

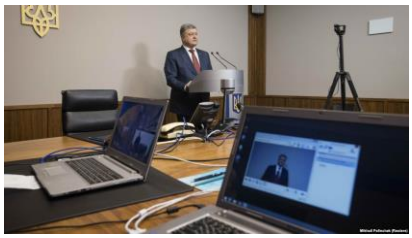
- How Will New Cybersecurity Norms Develop?
  Creating new laws and norms in the cyber domain seems a fundamental yet difficult step to ensure the minimization of the risk posed by electronic warfare to civilians. The multiplicity of governmental and non-governmental policy entrepreneurs involved, coupled with the unprecedented nature of the cyber threats, make the development of a new standardized legislation a treacherous obstacle course.
- Philippines joins the Budapest Convention on Cybercrime
  The Philippines is primary source of child pornography; the signature of the Convention, promoted by the Council of Europe, represents a step forward in the attempt to protect innocent victims of cybercrimes
- When to report a Cyberattack? For companies it's still a dilemma
  Even with the rising number of severe hacks, only a few companies report incidents each year to the Securities and Exchange Commission which has now issued an updated cybersecurity guidance.
- UK cyber security certification pilot launched
  The London Digital Security Centre (LDSC) has announced a pilot of the UK's first police-backed cyber security certification scheme to help organisations protect themselves against common online threats.

Cyber Security

- Satellite Internet and Russia's Control Over Its Cybersphere
  With the aim of making Internet access available to every point in the world, Starlink's upload and download links to thousands of satellites challenges the Russian government's idea of national sovereignty. Russian authorities have in the past several years adapted to the evolution of cyberspace, but at the same time the Government seems to care about setting a clear definition of what "vertical" limits of sovereignty could be.
- China: Big Data Fuels Crackdown in Minority Region
  Chinese authorities are building a predictive policing program based on big data analysis in Xinjiang. The tasked police officers are reluctant to explain the reasons for such data collection, nor give residents a choice to decline to provide the data
- Cybersecurity and Brexit: What does it mean for the fight against hackers?
  The after Brexit is a period filled with uncertainties, one is the future relationship between UK and Europol. In case UK won't be a part of it anymore, there could be possible negative implication for its cybersecurity.

Events

- Cybersecurity competition coming in April
- IoT, DevSecOps & Your Perimeter: The 2018 Cyber Security Digital Summit
- Norwich Brings Leaders in Cybersecurity to Campus for Second Annual Summit
- OURSA conference for cybersecurity diversity set for April 17



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

- Hackers used Outlook for cyberattack on German government: report
  Suspected Russian Hackers broke into a German government network, gaining access by burying hidden coded instructions into emails which they sent to staffers' Microsoft Outlook inboxes.

Cyber Warfare, Intelligence and Terrorism

- Integrating Cyber and Electronic Warfare
  The US Department of Defense has recognized that the synchronization of cyber and electronic warfare is key for US forces to succeed. The priority is to establish an effective governance structure to coordinate a multiservice approach to harmonizing electromagnetic spectrum and cyber activities—and doctrines—in addition to overseeing new investments in offensive and defensive technologies to support these efforts. The US Department of Defense has identified the synchronization of cyber and electronic warfare
- North Korea poses a greater cyber-attack threat than Russia, security expert warns
  Kim Jong-un's regime has been connected to a number of major hacks in recent years. Now North Korea is likely to continue malicious cyber activity against entities in South Korea, Japan and the US.
- What's Ukraine Doing To Combat Russian Cyberwarfare? 'Not Enough'
  Ukrainian authorities attributed the past suffered cyberattacks to Russia, expecting to be a target again. Despite the step forwards in its cybersecurity apparatus, the country would still be unprepared in case of attack.

Cyber Opportunities: Economy, Research & Innovation

- First probabilistic cyber risk model launched by RMS
  Catastrophe risk modelling specialist RMS has launched the first probabilistic cyber risk model, saying that it will help insurers, reinsurers and ILS markets to allocate their capital to cyber risk in a rigorous and quantitative way for the first time. Cyber risk modelling continues to advance, providing tools that can really help reinsurers and ILS managers to evaluate the risks in a more comprehensive way
- Cyber sector tries to shake off 'men in hoodies' image
  Just 11% of cyber security professionals are women. Sponsors to support, guide and mentor them are needed, but might not be enough to fill the gender gap and the expected 3.5m jobs in cybersecurity created by 2021.
- Skills Development Scotland in cyber security drive
  The digital transformation group Atos hosted an event in Forres for students from a Highland school with the aim of raising awareness of the growing career opportunities in the cybersecurity field.
- As cyber risks grow, insurance firms tap business opportunity
  An increasingly large number of Indians are falling victim to fraudulent withdrawals from their savings accounts. As the number of such frauds increases, the cyber insurance market is expected to grow.

Italian Focus

- Emergenza cyber-sicurezza, Italia tra i Paesi più a rischio
  The Chinese cybersecurity company Venustech has identified Italy and Europe as possible targets for hackers cyberattacks. Notwithstanding the increasing attention devoted to the cyberdefence, the dangers coming from the cyber world are still underestimated. While most of the population does not adopt the necessary defensive methods, hackers are developing increasingly sophisticated IT skills.
- Cyber security, intesa tra Leonardo e Nozomi Networks
  The high-tech security and defence company Leonardo has signed an agreement with Nozomi Networks, with the aim of increasing the level of critical infrastructure protection in Europe and in the rest of the world.
- Scuola, Anonymous annuncia lo "scippo" di 26mila dati degli insegnanti
  On the 8th of March one twitter account affiliated with the Hacktivists group Anonymous, announced the leaking of more than 26.000 sensitive data belonging to teachers, professors and school directors.

- Chiusi gli account filorussi dietro i cyber attacchi in Italia
  Three out of five twitter accounts that were reported for pro-Russian propaganda have shut-down. There are still doubts on who really ran them, but the sudden closing after the reporting gives room to suspects.

European Focus

- European Commission wants to make Europe a fintech hub
  The European Commission published on the 9th of March a 23 steps Action Plan to promote and make more easily accessible – especially for startups - the opportunities made available by new technologies like blockchain. This lab aims at involving both European and national authorities to engage with technology providers in a neutral and non-commercial space
- More women in the Digital sector: a key to Europe's successful digital future | International Womens Day 2018
  Challenging stereotypes; promoting digital skills and education and advocating for more women entrepreneurs are the three planned areas of actions to increase women's participation in the digital sector.
- Lithuania calls for an e-Schengen
  The President of Lithuania Dalia Grybauskaite has called for a "cyber Schengen" infrastructure to address online crime and cyberattacks in the European Union with the primary aim of protecting civilian infrastructure.
- A Europe that protects: Commission reinforces EU response to illegal content online
  On the 1st of March the European Commission has recommended a set of operational measures to facilitate removal of illegal content and increase the protection against terrorist content online.