Center for Cyber Security and International Relations Studies

Newsletter November 2018

Cyber Policy, Diplomacy & Legal Framework

- Midterms Security Watch: A cyber policy success?
  Election officials and federal cybersecurity agents successfully collaborated to confront and deter efforts to tamper with elections
- The Cybersecurity 202: Democrats promise their control of House means cybersecurity policy changes
  During their electoral campaign, Democrats promised that their control of the House of Representatives would bring some serious changes to cybersecurity policy.
- Learning from Israel's cyber playbook
  Israel, which has been always considered a cybersecurity powerhouse, could become a model for countries like Australia to develop a long-term policy of investment in cyber education, as opposed to just focusing on the tertiary sector
- NSA official: China violating agreement on cyber economic espionage
  Senior National Security Agency official Rob Joyce accused China of having violated a 2015 agreement with the U.S. to end cyber economic espionage.
- Paris Call of 12 November 2018 for Trust and Security in Cyberspace
  At the UNESCO Internet Governance Forum, Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace, an high-level declaration on developing common

Cyber Security

- Data Privacy And Cybersecurity Issues In Mergers And Acquisitions
  Data confirm that privacy, cybersecurity, and data breach risks are considered as key elements in mergers and acquisitions.According to one report, more than a third of acquiring companies discovered a cybersecurity problem during the post-acquisition integration.
- Failing cyber security test to cost Mislatel P26B
  A cabinet official said that provisional third telco player Mislatel Consortium may lose P25.7 billion at the minimum should it fail to deliver on its commitments or if it is found to have caused cyber security breaches that infringe on national security or sovereignty.
- Microsoft wants to work with Trump and Congress on cybersecurity
  Microsoft president Brad Smith told CNBC the tech firm hopes to work with Trump as it did with Obama in the attempt to pursue the company mission: to protect people from cyber threats without being affected by a divided Congress.
- Global cyber security skills gap widens to three million
  Based upon feedback from almost 1,500 ICT workers around the world, the Cybersecurity Workforce Study revealed that the worldwide cyber security skills gap currently stands at almost three million.
- Regionally-oriented national school for cyber security opens in Dakar, Senegal
  The French Minister for Europe and Foreign Affairs, Jean-Yves Le Drian, opened a new school in Dakar that will start offering courses from 2019 in Senegal, to train African officials on cyber security issues.

Cyber Warfare, Intelligence and Terrorism

- Top banks in cyber-attack 'war game'
  Some 40 firms, including leading banks like the Bank of England, are taking part in a one-day "war-gaming" exercise designed to assess their resilience.
- In Cyberwar, There Are Some (Unspoken) Rules
  Cyberspace continues to lack a set of norms that regulates aggressive tendencies. But states are acutely aware of the consequences of overly aggressive cyberoperations and therefore actively attempt to limit the impact of their activities.
- Australia joins international cyber war panel
  Australia's ambassador for cyber affairs has attended a meeting at which the Global Commission on the Stability of Cyberspace (GCSC) presented a new normative package concerning the disruption of elections through cyber attacks on electoral infrastructure and a call to protect the public core of the internet.
- NSA official: new U.S. cyberwar policy isn't the 'Wild West'
  Rob Joyce, former White House cyber coordinator and a senior official at the National Security Agency, defines the new U.S. policy governing cyber warfare as "thoughtful" notwithstanding what its critics might think.
- Microsoft boss warns terrorists and rogue states are WINNING the cyber wars against the West
  Microsoft's president Brad Smith claims that the internet has become a battlefield, urging for a digital Geneva Convention' to be signed to prevent a global arms race.

- UK business secretary announces five new AI technology centres

  The UK government announced in a press release the opening of 5 new centres of excellence for digital pathology and imaging, including radiology. All the centers will use advanced AI devices
- Experts predict a “price explosion” in the cryptocurrency market

  Overstock CEO Patrick Byrne, who was behind the online retail giant becoming one of the first places to accept bitcoin back in 2014, said that he still expects the mass adoption of cryptocurrency.
- Intelligence, perché l’uomo conta (molto) anche nell’era cyber

  The Humint (Human Intelligence) - information research conducted through human sources - represents the most important and valuable cognitive tool of 21st century intelligence services, despite the development of increasingly powerful and innovative spy technologies in fields such as Sigint (Signals Intelligence), Geoint (Geospatial Intelligence), Masint (Measurement and Signature Intelligence), Cyber-Intelligence (Cybint).
- DHS Reveals New Cyber Research Strategy

  DHS revealed the approach for the Cyber Risk Economics Capability Gaps Research Strategy in a blog post Tuesday. The study looks at the business, behavioral and legal factors that affect cyber risk by focusing on four broad themes: why and how cybersecurity investments are made, the impact investments have on risk and harm, the relationship between cybersecurity risk and business risk, and incentives to encourage cyber risk management.

Italian Focus

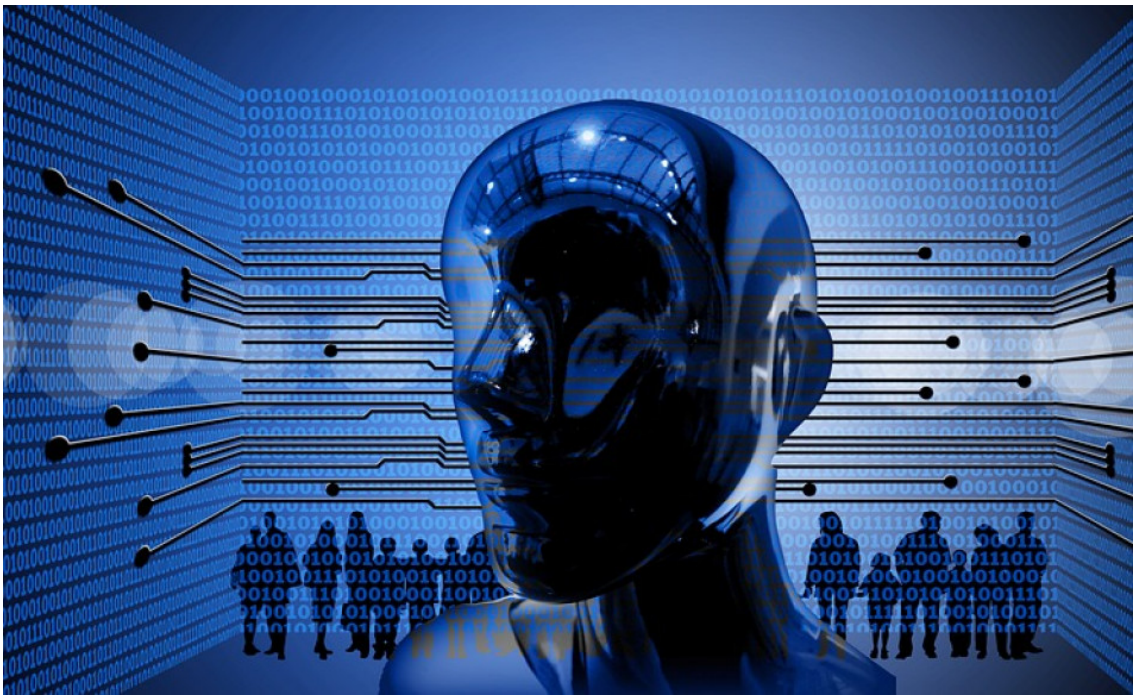
- Cyber security, come cambiano conflitti e alleanze nel quinto dominio

  The Center on cyber security of Ispi and Leonardo presented during an event in Rome, a report that analyzes the main "state sponsored" threats identified in the new American

- Generali lancia una funzione interamente dedicata alla Cyber Insurance e la start-up CyberSecurTech

  CyberSecurTech, created by Generali, will offer customers innovative solutions to assess IT risk through its own online platform. The new function will develop and coordinate the Group's activities in the field of IT insurance at the global level
- L'industria navale in Italia è sotto una campagna di cyber attacchi mirati

  "MartyMcFly", is a malware used in a timed attack, planned in 2010 and executed in 2018, against a company operating in the naval supply sector. After the discovery of the malware, Yoroi and the Fincantieri SOC created a cyberforce to analyze cyber threats to the naval industry in Italy.



European Focus

- Così l'intelligenza artificiale controllerà (anche) le frontiere europee

  iBorderCtrl is testing a system whose aim is to verify the sincerity of travelers by crossing their responses and their facial movements. The pilot project, coordinated by George Boultadakis of the European Dynamics in Luxembourg, will start in Hungary, Latvia and Greece.
- Cyber security, al vertice Ue la proposta di sanzioni per attacchi informatici

  The traditional European Council of October had a strong focus on internal security, including IT security. The primary stated objective is to counter cyber attacks - often of Russian origin according to Western intelligence agencies - with concrete measures.
- Così l'Europa (con gli Usa) può rilanciare il dibattito sul futuro del cyber spazio

  In the analysis of the possible debate on the future of the cyberspace, Floriana Giannotti calls for the prevention of a cybernetic conflict and for the relaunching of the role of Europe as a mediator.
- EU cybersecurity organisations agree on 2019 roadmap

  On 6 November 2018, the four Principals of the Memorandum of Understanding (MoU) between the European Union Agency for Network and Information Security (ENISA), the

Upocoming Events

- November 20
  Conference: Towards the EU Cybersecurity Certification Framework
- November 22
  Cyber London Conference II
- November 30
  NBU/ENISA workshop on the NIS Directive and Critical Information Infrastructure Protection

Further information at

https://www.cssii.unifi.it

Contact us at

cyber@cssii.unifi.it