Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- **The impact of GDPR on US cybersecurity policy**
  The EU GDPR marks a turning point in the cyber policymaking arena due to its explicit focus on privacy and data ownership. Considering the clashing differences with the American policy paradigm in the same field, the GDPR is expected to arise a debate involving US private businesses that have costumers in Europe.
- **Trump gets cyber diplomacy and workforce advice from agencies**
  After an executive order issued by President Trump in 2017, Federal agencies with cybersecurity portfolios including the Departments of Homeland Security and Commerce, transmitted reports stressing key challenges for the American government.
- **Qatar state news agency's hacking linked to Riyadh**
  An Al Jazeera investigation has revealed that the hacking of Qatar News Agency's website on May 24, can be attributed to a Saudi piracy cell.
- **Lavrov notes US not interested in cooperating with Russia on cybersecurity**
  During his speech at the Public Administration Academy in Minsk, Russian Foreign Minister Sergey Lavrov's speech focused on the open issue of establishing universal rules of cyber activity, which requires both Russian and American efforts.
- **Four Principles To Build A Healthy Cyber Security Policy**
  Enhancing internal processes, creating a healthy culture from the top down, including customers, and remembering external partners, are the necessary steps to follow to create an effective cybersecurity plan.

Cyber Security

- **Ukraine cyber police aware of possible new threat: police chief**
  Sergey Demedyuk , Ukraine's cyber police chief, said in a statement that it was possible the hackers planned to strike during large-scale events, confirming the suspected Russian plan to attack Ukraine warned by Cisco Systems Inc.
- **German intelligence head warns of cyber attacks on critical infrastructure**
  The head of Germany's domestic intelligence service warns that the country's critical infrastructure could be the targets of cyber attacks. He also claimed that Germany has readily available anti-sabotage measures.
- **According to Domino's CISO, cyber security focus too much on tech**
  Despite the biased focus on technology, it should be remembered that security also includes other key elements involving people and processes.

Events

- **Cyber Week Tel Aviv**
  June 17 - 21, 2018 | Tel Aviv, Israel
- **IEEE Smart Industries Workshop**
  June 18, 2018 | Taormina, Italy
- **The Tenth International Conference on Evolving Internet INTERNET 2018**
  June 24-28, 2018 | Venice, Italy

- [As cyber security needs become an overriding concern, China works on an impenetrable shield](#)
  With the aim of strengthening its cyber defence, China called white hat hackers from all over the world to work on its Cyber Mimic Defense (CMD), a domestically-developed cyber defense system.
- [Cyber security: Nation-state cyber attacks threaten everyone](#)
  Robert Hannigan, who served as director general of GCHQ from 2014 to 2017, said that nation-state cyber attacks are now a problem that concerns the entirety of the population.

Cyber Warfare, Intelligence and Terrorism

- [There will be no 'Cyber Cuban Missile Crisis'](#)
  Modern technology has outpaced the ability of shared familiar metaphors to describe it. Trying to tie modern threats, executed with code over a global network infrastructure that didn't exist decades ago, to historical analogies is a perilous activity.
- [Cyber Mission Force Achieves Full Operational Capability](#)
  Having US Cybercom achieve full operational capability early is a testament to the commitment of the military services toward ensuring the nation's cyber force is fully trained and equipped
- [The new face of the Syrian Electronic Army](#)
  Once responsible for Assad's offensive cyber operations, the Syrian Electronic Army is back. Its new mission, to reconquer Syrian cyberspace for the regime, may prove impossible.
- [China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare](#)
  In January and February Chinese government hackers have compromised the computers of a US Navy contractor, stealing massive amounts of highly sensitive data related to undersea warfare
- [Google bars uses of its artificial intelligence tech in weapons](#)
  Google will not allow its artificial intelligence software to be in weapons or unreasonable surveillance efforts under new standards for its business decisions in the nascent field, the Alphabet Inc (GOOGL.O)

Cyber Opportunities: Economy, Research & Innovation

- [Addressing the challenges of rapid technological advancements in cyber defence](#)
  To ensure that the work on cyber defence is entirely aligned with member states' needs and requirements, the EDA Project Team Cyber Defence (PT CD) was established in 2011 – a group of governmental representatives responsible for driving a portfolio of activities coming out from the cyber defence strategic context case and endorsed by the EDA's Steering Board – its governing body.
- [US Energy Department's new cybersecurity agency is a game-changer](#)
  With energy systems now massively digitized and interconnected, with attackers at all levels becoming more capable and aggressive, and with current approaches to cyber defense observably not keeping pace, something must give
- [Industry must do more to open up cyber security profession](#)
  James Lyne reveals that he fell into security more by accident than design, and says training and recruitment must change to find and develop talented individuals
- [Google Staff AI Revolt Jeopardizes Pentagon Cloud Deals](#)
  Google employees had signed a petition to cancel a company contract with the Pentagon. The decision capped a furious debate inside Google over whether the Alphabet Inc. unit should use its AI to help the military.

Italian Focus

- **L'Italia alla sfida cyber security. Ma bisogna fare fronte comune**
  In Cividale del Friuli, the annual convention of the Radio Square has brought together experts and representatives of institutions, companies and the university world to debate the state of the art but above all to discuss the actions necessary to push the mass to point of a country strategy.
- **Il digitale per lo sviluppo del Sud, quattro punti per il nuovo Governo**
  Resolve from the South with determination, placing digital at the center of development policies with a systemic redevelopment plan.
- **Italy Turns to Postal Police to Fight Fake News**
  Italy's leaning on crime fighters of yesteryear in its battle against fake news: the postal police. It has expanded its expertise to the web, catching pedophilia, hacking, money-laundering, credit-card fraud, copyright violations by monitoring other platforms.
- **Ecco come alla Farnesina si punta sulla cyber diplomacy. Parla l'ambasciatore Talò**
  The Italian Foreign Ministry is gradually developing the peculiarities of its cyber diplomacy, based on three main elements: the defensive aspect, the diplomatic side and the exploitation of opportunities.
- **Cyber security, spesa media delle imprese ferma a 4.500 euro**
  It is now up to the Bank of Italy to highlight the delay of Italian companies in the field of cyber security. Many are victims of attacks and few industries have an adequate level of insurance

European Focus

- **First EU cybersecurity law takes effect—with new fines for misbehaving companies**
  The first EU cybersecurity law went into effect on the 9th of May, as negotiators continue to hammer out details of a second bill that will create even more rules in the area. The new law will require firms running "essential" services, including water, energy, transport, health and banking operations, to inform national authorities if they are hit with serious cybersecurity breaches.
- **Cybersecurity: Joint Statement by Vice-President Ansip and Commissioner Gabriel on political agreement from the Council**
  The European Commission welcomes the political agreement reached by the Telecommunications Council on a general approach on the Cybersecurity Act, which was presented by President Jean-Claude Juncker in his annual State of the Union Address in 2017.
- **A Europe that protects: EU works to build resilience and better counter hybrid threats**
  the European Commission and the High Representative are today proposing further steps to build on the work already carried out in response to hybrid threats as cyber security
- **EU can become a leading player in cyber security**
  The Commission's proposal on cybersecurity is a good start, but it requires certain additional elements to ensure it works, writes Angelika Niebler.