Newsletter January 2018

Center for Cyber Security and International Relations Studies

It is a great honour for the Center for #Cybersecurity and International Relations Studies to announce the beginning of its partnership with the Global Forum on Cyber Expertise.
The GFCE is a global platform for Countries, International Organizations and private companies to exchange best practices and expertise on cyber security and cyber capacity building.
We look forward to collaborating with the #GFCE and its inspiring and high-level partners.

CALL FOR PAPERS
The Center for Cyber Security and International Relations Studies is happy to announce its first call for papers devoted to cyber security issues! Check out further details at:
https://www.cssii.unifi.it/upload/sub/Call%20for%Paper%20center%20cyber.pdf

Cyber Policy, Diplomacy & Legal Framework

- Evaluating the US-China Cybersecurity Agreement
- Cyber security a focus of UN Internet governance conference
- Year in Review: The Trump Administration Disrupts U.S. Cyber Diplomacy
- Aspen Cyber Strategy Group holds inaugural meeting to tackle cybersecurity issues
- WannaCry and the International Law of Cyberspace
- Cyber is the new black: Australia's cyber security strategy
- EU cyber chief says expectations exceed resources

Events

- ***Industrial Cyber Security Forum***
  Milano, 20 January 2018
- ***Cyber Security: Last Call***
  Mestre, 25 January 2018
- ***ItaSec 2018***
  Milano, 6-9 February 2018

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

Cyber Security

- Major flaw in millions of Intel chips revealed
- Microsoft: Meltdown and Spectre can cause noticeable performance slowdowns
- Apple releases new update to fix 'Spectre' chip flaw
- Cisco to release patches for Meltdown, Spectre CPU vulnerabilities
- Meltdown and Spectre fixes arrive, but don't solve everything
- Electrum Moves to Patch Bug That Left Thousands of Bitcoin Wallets Exposed
- Hackers have found a way to mine cryptocurrency and send it to North Korea
- Researchers at security firm We Are Segment have discovered a vulnerability in Gmail
- Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip Flaw At the Same Time
- PC security pioneer John McAfee claims his Twitter was hacked
- 2018 Winter Olympics being used as phishing
- Forever 21 Confirms Security Breach Exposed Customer Credit Card Details
- It's a mystery, member of the Lurk gang admits creation of WannaCry ransomware for intelligence agencies
- A security breach in India has left a billion people at risk of identity theft
- New security flaw allows hackers to eavesdrop on your WhatsApp chats

Cyber Warfare, Intelligence and Terrorism

- Russia could cut off internet to NATO countries, British military chief warns
- Cyber attacks on nuclear arsenals 'could lead to inadvertent launches', think tank warns

Cyber Opportunities: Economy, Research & Innovation

- Huawei's expansion plans are floundering
- What's Next for Cybersecurity in 2018?

Newsletter February 2018

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- New global cyber security center announced at Davos
- Pakistan Launches 'Surfsafe' Application to Combat Cyber Extremism
- India is planning steps to ensure cryptocurrencies are illegal within its payments system
- New China Data Privacy Standard Looks More Far-Reaching than GDPR
- Bitcoin dips as South Korea's cryptocurrency rules come into effect
- Rex Tillerson proposes new 'cyber bureau' at the State Department
- Polish electric company looks to Israel as 'partner in fighting cyber-crime'
- Slovakian Parliament passes law on cyber-security

Cyber Security

- Data breach disclosure law will lift Australia's cyber security game
- International crackdown on anti-spyware malware
- Exercise Crossed Swords Practised Cyber-Kinetic Operations in Latvia
- Update on Twitter's Review of the 2016 U.S. Election
- Russians penetrated US voter systems, DHS cybersecurity chief tells NBC
- 'Fancy Bear': Defense Contractors' Email Hacked by Russians
- Lebanese security agency turns smartphone into selfie spycam
- Facebook to roll out new tools in response to EU privacy laws
- Samsung starts making cryptocurrency mining chips

Events

- Tavola Rotonda sulla Homeland Security
- Public sector cyber security 2018
- The European Information Security Summit 2018 (TEISS)

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

Cyber Warfare, Intelligence and Terrorism

- Hezbollah Goes on the Cyber Offensive with Iran's Help
- Cyberwarfare with Russia 'now greater threat than terrorism', warns British Army chief
- Russia says Britain's Defence Secretary's claim of attack threat 'like something from Monty Python'
- A quick look at US cyber warfare preparedness
- Will Trump go nuclear over cyber warfare?
- Four ways to avoid being a victim of Russian cyberwarfare
- Hacking and cyber warfare are top humanitarian concerns

Cyber Opportunities: Economy, Research & Innovation

- Chronicle: a new Alphabet business dedicated to cyber security
- Huawei to invest $800m in 5G research and development
- Cyber offerings and demand for protection to increase in 2018: Fitch
- New cyber training partnership aims to inspire young women
- Israeli cyber security firms raised record $814.5 million in 2017

Newsletter March 2018

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

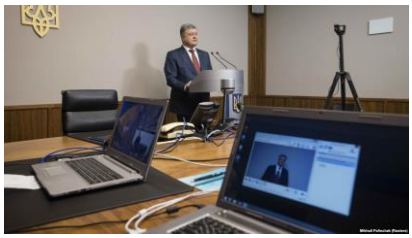
- How Will New Cybersecurity Norms Develop?
  Creating new laws and norms in the cyber domain seems a fundamental yet difficult step to ensure the minimization of the risk posed by electronic warfare to civilians. The multiplicity of governmental and non-governmental policy entrepreneurs involved, coupled 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.

Newsletter April 2018

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- WITH ITS NEW 'WHITE BOOK,' FRANCE LOOKS TO BECOME A WORLD-CLASS PLAYER IN CYBER SPACE
  The French Strategic Cyberdefense Review advocates a more state-centric approach to cybersecurity, contrasting the US private-sector led vision. Recognising the potential dangers of an unregulated cyberspace France aims to become a leading voice in the normative debate on the rules of cyberspace, allowing for, in the most extreme cases, even military responses.
- How Local Governments Can Prevent Cyberattacks
  Local governments all over are embracing modern technologies, but are often not aware of the precautions and policies necessary to defend against attacks. A change in culture is key for a securer future
- Why the CLOUD Act is Good for Privacy and Human Rights
  By streamlining certain foreign countries' access to data concerning their citizens the CLOUD Act will discourage governments from attempting to delocalise data from the US.
- Cambridge Analytica and Facebook: The Scandal and the Fallout So Far
  From the first disclosures to the analysis of the recent hearings involving Mark Zuckerberg in front of the Senate and the House: the New York Times' take on the Cambridge Analytica scandal.
- New West Virginia law targets cyber bullies
  West Virginia legislature has been among the first to create a law which prohibits online harassment, threats, and intimidation, making cyber bullying of kids a crime.

Cyber Security

- Cboe urges U.S. regulators to move forward with bitcoin ETFs
  As investor demand for virtual currencies soars, exchange holding companies such as Cboe Global Markets are putting pressure on the Securities and Exchange Commission (SEC) to allow exchange-traded funds (ETF) that include cryptocurrencies into the market. So far the SEC has been reluctant in accepting such funds, asking for more time to examine the issue
- Thousands of Sears, Delta customers affected by data breach
  Credit card information of tens of thousands of clients were left vulnerable to cybercriminals for more than two weeks due to the hacking of third-party vendors, managing online customer chat services.

Events

- IoT Tech Expo Global 2018 April 18 - 19, 2018 | London, United Kingdom
- Cyber-Crime Conference 2018 April 18, 2018 | Rome, Italy
- IL VALORE DEL DATO PERSONALE April 19, 2018 | Rome, Italy
- Workshop – Hacking mind in the cyber age April 19,2018 | Rome, Italy
- 11th European Workshop on Systems Security (EuroSec) April 23, 2018 | Porto, Portugal
- International Conference on Data Mining (DaMi) April 28 - 29, 2018 | Copenhagen, Denmark
- Workshop – GDPR: Stato dell'adeguamento in Italia e risultati attesi alla scadenza dei termini per la sua applicazione May 31, 2018 | Rome, Italy

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

- [Government websites hit by outage, cyber security chief says it was a technical glitch]
  An apparent cyberattack affected over a dozen official Indian govt. websites, but the National Coordinator of Cyber Security said that the issues were due to hardware failures
- [Atlanta takes down water department website two weeks after cyber attack]
  Two weeks after a ransomware cyber attack targeted the city's computer systems, Atlanta had to take down its water department's website due to ongoing issues
- [Cloudflare's new DNS service speeds up surfing, maintains your privacy]
  Cloudflare announced the release of a new tool aimed at increasing internet connection speeds without allowing internet service providers and the company itself from collecting data.

Cyber Warfare, Intelligence and Terrorism

- [A cyber attack in Saudi Arabia failed to cause carnage, but the next attempt could be deadly]
  The August 2017 attack on a petrochemical plant highlighted the danger posed by cyber attacks to industrial plants. Exact details on the investigation of the attack are closely guarded, but the sophistication of the attack and required funds indicate nation state involvement. Worryingly, the compromised component is used in 18,000 plants globally, including some nuclear plants.
- [Artificial Intelligence: The Next Frontier of Cyber Warfare?]
  Even if the adoption of AI technology it is still in its nascent stages, a report warned that cybercriminals may soon be leveraging AI to increase the scope and efficiency of their attacks.
- [Cyberattack targeted provider of electronic data affecting gas pipeline network]
  In Houston, Texas, a cyber attack interrupted the communications between four natural-gas pipeline operators and their consumers. While gas service was not interrupted, vulnerabilities were highlighted.
- [Marines started to test new information warfare units]
  The Marine Corps is developing a process that will lead to the integration of all information-related capabilities such as cyber, signals intelligence, electronic warfare and information operations.
- [Presumed Russian hacker extradited to the U.S.]
  Yvegeniy A. Nikulin was arrested in 2016 with the accuse of having hacked the systems of three American technology companies. After having being held in in the Czech Republic, the man was extradited to the U.S..

Cyber Opportunities: Economy, Research & Innovation

- [Cyber needs to be centre stage for every world leader, minister and business CEO]
  The Commissioner on the Global Commission for the Stability of Cyberspace, Christopher Painter, underlines the need to demystify cyber policy and make it part of the larger national and economic discourse. Cyber policy should involve leaders, ministers and CEOs to address the threats posed by cyberspace, but at the same time the many opportunities offered by this fifth dimension.
- [It's embarrassingly huge': John McAfee reveals why he charges over $100,000 for each market-moving cryptocurrency tweet]
  McAfee decided to reveal the influence his tweets have on the price of cryptocurrencies as a proof of transparency. In addition, it warned the other promoters to be clear about their dealings with cryptocurrencies firms since they risk facing repercussions
- [What A Cyber Security Firm Can Teach You About Making Your Pitch]
  Liz Maida, co-founder and CEO of Uplevel Security, an early-stage company looking for capital and seeking top

talent to differentiate itself in the crowded marketplace of cybersecurity, shared her experiences about the protection of data.

- $64 million from the state to advance cyber and education
  Georgia invest 64$ million in Augusta University to advance cybersecurity and education. A new Center for Cyber Innovation and Training will open in July as a proof of the partnership between the Central Institutions and the Academia.

Italian Focus

- Una tecnologia nazionale per la cyber security: che può fare l'Italia
  Italy should invest in a national hardware system in some strategic area. Hardware that is not appropriately protected can be the weak link in the chain, becoming a gateway to the system, to its functionality and top the data processed and / or stored in it. It can start from a National Research and Development Center in cybersecurity, which will have as main task advanced research, the development of architectures, applications and actions of various national nature
- F-Secure, 30 anni d'innovazione nella cyber security
  F-Secure celebrates its thirty years and traces the stages of its history. The company's new strategy - Predict, Prevent, Detect, Respond - today guides the entire offer
- Cyber security, Microsoft e Vodafone insieme per Pmi
  Microsoft and Vodafone announce a collaboration to offer Italian companies the solution of Modern Workplace, designed for small and medium-sized businesses to protect corporate data and provide support for the adaptation to the new GDPR
- Cyber crime, operazione congiunta Polizia italiana e rumena
  The "Bruno" operation ordered home and IT searches that put into practice the judicial and coordination cooperation mechanisms provided by Eurojust
- Facebook, l'Antitrust italiana apre istruttoria su raccolta e uso di dati
  Following the Cambridge Analytica scandal, the Italian Antitrust Authority decided to open an investigation against Facebook to determine if there were any improper commercial practices regarding the collection and use of data.

European Focus

- Majority of European businesses unprepared for GDPR - IDC
  Only 29 per cent of European small business and 41 per cent of midsize businesses "have taken steps to prepare" for GDPR, according to IDC.That's despite just a seven-week deadline before the EU's privacy legislation comes into force on 25 May. The potential penalties for failing to meet these requirements are severe: up to £17.5m or four per cent of annual revenues.
- UK cyberskills lagging behind Europe
  UK IT leaders have become increasingly concerned that they do no have adequate levels of expertise in cloud-based security and data protection
- France and Estonia strengthen digital cooperation
  On March 19 Paris and Tallinn have signed an e-government agreement to combat cyberattacks and develop the digital economy
- A Euro Cyber Resilience Board for pan-European Financial Infrastructures
  First meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures. The ECRB's objective is to enhance the cyber resilience of financial market infrastructures and their critical service providers, as well as that of the wider EU financial sector, in line with international standards
- Applied Risk Launches New European Program to Tackle Industrial Cybersecurity Challenges
  Applied Risk, an established leader in industrial security, has today launched a new program to help industrial operators and suppliers across Europe achieve compliance with NIS Directive

Newsletter May 2018

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- The State Department might designate a cyber ambassador
  After the retirement of former Cyber coordinator, Christopher Painter, the US State Department effectively removed his position. The Department of State Authorization Act of 2018 sets the basis for the recreation of this office and even going a step further with the creation of a Bureau for Cyberspace and the Digital Economy, run by a Senate confirmed assistant secretary reporting directly to the under secretary for economic growth, energy and the environment.
- Government to refresh 2015 Cyber Security Strategy and Action Plan
  New Zealand refreshed its approach to cyber security by establishing a CERT NZ, by delivering of CORTEX malware detection and disruption services, by promoting cyber security awareness campaigns and by working to improve the cyber security of small business and developing police skills
- Is it Time to Regulate Cyber Conflicts?
  According to Microsoft President, Brad Smith, Governments should work together with private tech companies to tackle the growing threat of state-sponsored cyber attacks. Encouraged by positive indications in the international legal and diplomacy arena, Smith proposed a program based on three pillars.
- Three critical components of a cyber policy
  Although cyber criminals seem to be one step ahead of the authorities, leading cyber insurance companies are doing a good job of creating broad and forward thinking policies that protect a client in the event of a cyberattack. Here, Insurance Business looks at three of the critical components of a modern cyber policy.
- How Casper Klynge is reinventing diplomacy as the world's first tech ambassador
  Denmark's representative in Silicon Valley has met with scepticism since taking up his post, but he is convinced others must follow his country's lead

Cyber Security

- What Is Telegram, and Why Are Iran and Russia Trying to Ban It?
  Telegram, the cloud-based instant messaging service founded by Russian engineer Pavel Durov, has been recently blocked in Iran and Russia, two of its largest user bases. The social network has already sparked some criticism, when it was disclosed its role as communication tool for terrorists. Now many

Events

- Hack Miami (CFP FL, USA)
  May 18 - 20, 2018 | Miami, Florida, United States
- IT & Digital Leaders Nordics
  May 24, 2018 | Stockholm, Sweden
- International Workshop on Secure Software Engineering in DevOps and Agile Development (SecSE) (CFP Porto, Portugal)
  May 25, 2018 | Porto, Portugal

un-democratic countries are using fear to crack down Telegram and the network of political dissidents, which used it to protect themselves.

- Twitter users told to change passwords after internal leak
  Twitter's 330 million users got their passwords stored in a easily readable system. The company has encouraged users to change the passwords for caution, since no account result stolen or damaged.
- British and Spanish leaders say Russian trolls meddled in their elections
  Britain and Spain accuse Russian government of pushing respectively for Brexit and Catalonian Referendum, through massive fake news campaign. The leaders have not revealed any evidence and Putin has replicated suggesting that Western countries are using Russia as scapegoat for their internal failures.
- Cybersecurity risks to get worse: Warren Buffett
  Warren Buffet, Berkshire Hathaway CEO, warns that "Cyber is uncharted territory. It's going to get worse, not better". Cybersecurity risk is more difficult to assess than other threats, nowadays.

Cyber Warfare, Intelligence and Terrorism

- Pentagon's Cyber Command Gets Upgraded Status, New Leader
  The Pentagon has recently incremented its cyber warfare and digital unit, indicating an increasingly important role of this sector in the US national defence and security system. Army Gen. Paul Nakasone has been named chief of the Cyber Command, as well as Director of the NSA. This appointment seems to suggest that US are taking more and more seriously the cyber threats, both from non-state actors (ISIS) and from major countries (China and Russia).
- Drones used to disrupt FBI hostage situation
  Criminals reported to use drones to disrupt FBI hostage situation. This is the last of a series of criminal use of UAV, which is worrying police.
- Cyberwarfare, populism top 'black swan' events at Milken conference
  Cyberwarfare and populism are some of the top risks that could threaten global stability and financial markets, investors and policymakers warned at the annual Milken Institute Global Conference.
- What a cyberwar looks like — and what it doesn't
  President and Chief Legal Officer Brad Smith of Microsoft in April told the RSA cybersecurity conference about attacks that don't involve tanks and warplanes, but bytes and bots. And they are aimed at our energy grids, our infrastructure, and even our private financial information
- By staging war games, NATO members prepare for cyber attacks
  The world's largest live-fire cyber defense exercise is helping NATO members prepare for cyber warfare. Over the last eight years, 22 NATO and EU countries have been practicing the scenario of a cyber attack in Locked Shields, a war game run by the NATO Cyber Defence Centre of Excellence.

Cyber Opportunities: Economy, Research & Innovation

- Private Companies Take the Lead on Cyber Security
  The Cybersecurity Tech Accord is a remarkable initiative by a group of 35 key technology and security companies like Cisco, Facebook, Microsoft, Nokia and Oracle. It is a public commitment to protect and empower civilians online and to improve security, stability and resilience in cyberspace.
- Georgia governor vetoes cyber bill that would criminalize "unauthorized access"
  After many weeks of opposition from information security firms and professionals, Georgia Governor Nathan Deal vetoed a bill that would have criminalized unauthorized access of computer systems.
- Facebook publishes new content moderation guidelines
  Zuckerberg's social network implemented the expected new, post Cambridge Analytica, user standards urging the Facebook community to "share responsibly".

- Goldman Sachs to Open a Bitcoin Trading Operation
  Goldman Sachs will finally launch its widely-rumoured bitcoin trading operation after having hired its first digital asset trader
- JPMorgan Chase is doubling down on artificial intelligence.
  The American bank has hired Manuela Veloso, a top researcher from Carnegie Mellon University as its first head of artificial intelligence research.

Italian Focus

- Professioni Ict, fra tre anni in Italia 135mila posizioni scoperte
  The gap between supply and demand in the Italian ICT labour market will rise by up to 18% in 2020. Notwithstanding the clear signals coming from the market, the Italian education system keeps investing in ICT diplomats instead of in graduates.
- Italy joins Hybrid CoE
  On the 24th of April, Italy became the 15th member state in the European Centre of Excellence for Countering Hybrid Threats.

- Cybersecurity: perché stanno raddoppiando gli attacchi nella sanità?
  According to the latest report issued by McAfee Labs on Cyber threats, 2017 has been a terrible year for the health sector: cyber attacks tripled in comparison to 2016
- Recepimento direttiva Nis, Italia è in ritardo ma è allarme cyber crime
  Notwithstanding its relevance, the current Italian political deadlock is slowing the implementation of the new NIS directive.
- Formazione, Poste spinge sulla networking security. E si allea con Juniper
  Network security specialists Juniper Networks and Poste Italiane, will jointly deliver a cycle of university classes on information security for Master's students.

European Focus

- EU to force tech firms to hand over terror suspects' messages
  The European Commission plans to give judges the power to issue transnational production orders for information held by service providers in other EU countries. These come with short time limits for compliance to improve the ability of law enforcement agencies to conduct effective investigations.
- European Commission welcomes new EU-wide cybersecurity laws
  The new NIS Directive is considered by the EU Commissioners as a "turning point". Indeed the Directive is the first legally binding EU instrument concerning cybersecurity.
- Joint Statement by EU Commissioners on the new NIS Directive
  On the 4th of May, several Commissioners including Andrus Ansip, responsible for the Digital Single Market, issued a statement on the first EU-wide legislation on cybersecurity.

Newsletter June 2018

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

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

- 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.

Newsletter July 2018

Center for Cyber Security and International Relations Studies

Cyber insight

Check our last publication on "OSCE. Problems in implementing the CBMs"

Cyber Policy, Diplomacy & Legal Framework

- Putin, Trump need to discuss cybersecurity issues
  Andrei BystritsDaky, Chairman of the Board of the Valdai International Discussion Club's Development and Support Foundation, affirmed that it is absolutely important that cyber security issues are among the topics of the meeting between Russian President Vladimir Putin and his US counterpart Donal Trump, scheduled for the 16th July in Helsinki.
- Russia proposes alternatives to international cyber norms
  Russia will propose two "cyber resolutions" to the UNGA next September with the aim of updating the Code of Conduct (2011) and creating a global treaty on cyber crime to replace the Budapest Convention (2001).
- A Look at Israel's New Draft Cybersecurity Law
  Israeli government presented the Draft of the cyber security law which strengthens the National Cyber Directorate and underlines the need of developing public-private partnerships along with cyber preparedness and resilience.
- China's cybersecurity law is biased and open to abuse, but it may not stop others copying it
  As a stark contrast to Europe's GDPR, China's cybersecurity law gives Chinese companies an unfair edge and raises important privacy concerns. The risk is that other countries could adopt this model instead of the European one.

Events

- Summer School "Digitalisation in Transport"
  11-15 June 2018 Trieste, Italy
- International Conference on Information Society
  15-18 July 2018 Dublin, Ireland
- Conference on Data and Applications Security and Privacy
  16-18 July 2018 Bergamo, Italy

- UK & France sign major deal for AI & Cyber Security cooperation
  UK and France signed a five years deal to bolster the development and implementation of fast-moving technologies between the two countries

Cyber Security

- A human-centric approach to better cybersecurity

A recent risk report from the Office of Management and Budget demonstrated that a majority of agencies with cyber security programs in place remain at significant risk of attack. In order to have a better information security programs, agencies should consider developing human-centric, automated and adaptive security responses based on how individual users interact with data

- Cyber attack on Mexico campaign site triggers election nerves

During the last television debate before the Mexican presidential elections, the website of current Mexican opposition party was hit by a DDoS cyber attack with the bulk of traffic to the site nominally coming from Russia and China

- Russian Attacks Against Singapore Spike During Trump-Kim Summit
  During the meeting between US President Donald Trump and his counterpart North Korean Kim Jong-un, Singapore was targeted by cyber attacks, whose 97% coming from Russia
- Exclusive: Ukraine says Russian hackers preparing massive strike
- Ukraine's cyber policy chief affirmed that hackers from Russia are infecting Ukrainian companies with malicious software to create backdoors for a large coordinated attack.
- A cybersecurity fund has returned more than 30 percent since the Equifax data breach
  Since the epic data breach of more than 145 million customers at credit firm Equifax in September 2017, the fund has returned 31 percent, double the return of the S&P 500 over that same period

Cyber Warfare, Intelligence and Terrorism

- Cyber peacekeeping is integral in an era of cyberwar – here's why

While a large proportion of research focuses on how to conduct cyber warfare, there is very little research on restoring peace in the aftermath of an online conflict between nation states. The physical effects of cyber weapons make cyber peacekeeping a key enabler to help bring about lasting peace

- Islamic cyber terrorists trying to target infrastructure

Islamic cyber terrorists are increasing their efforts to carry out cyberattacks against Western countries infrastructure. In addition the United Cyber Caliphate is reorganising itself

- Cyber warfare is grave threat, but India is not yet prepared for it: General Hooda

The Indian General D.S. Hooda said that India was ranked third in terms of facing threats of cyberwarfare, but was at 23rd position when it comes to preparedness to deal with them.

- Congress Pushes For a Clearer Strategy on Cyber Warfare

Congressional lawmakers are calling for a more clearly defined strategy for responding to large-scale cyberattacks–ranging from attacks on infrastructure, to cyber espionage that threatens national security

- Preventing the Global Cyberwar: Why We Need a Digital Geneva Convention

As it stands today, the opportunity for an attacker to target major infrastructure is far too easy. We need to ensure that global attacks have tangible consequences on a global scale.At the RSA conference this year, 34 security vendors signed the Cybersecurity Tech Accord, forming a coalition determined to prevent nation-state cyberattacks. It was a significant step forward in the private sector, but we need to go further.

Cyber Opportunities: Economy, Research & Innovation

- The age of cyber: The private and public sectors must join forces

UK offers a perfect example of the importance of the private and public partnership thanks to the opening of the London Office for Rapid Cyber security Advancement (LORCA). This facility will act to bring together a cohort of the brightest and best innovators, and generate industry-led cyber innovation.

- Innovation in healthcare: A hacker's dream and CISO's nightmare?

Applying AI and machine learning to the healthcare sector has a big positive potential in

pure technological and economical terms, but at the same time it represents a big risk from the cyber security point of view.

- AI and other tech key to post-Brexit success, says Matt Hancock
  Matt Hancok, the British Digital secretary, highlighted the importance of emerging technologies for the future of UK after Brexit, considering the relevance of the opening of London's cyber security innovation centre,
- Top 100 Cyber Security Companies: Ones to Watch in 2018
  The aim of the report is to provide an evaluation of the 100 significant major companies in the global Cyber Security industry by detailing their involvement in the market.
- Not enough CISOs and business leaders cooperate on a cybersecurity plan and budget
  C-suite and IT decision makers need to embrace a different approach to cybersecurity to effectively protect against future cyber risks since nowadays they do not really have influence on the cybersecurity strategies.

Italian Focus

- Chi c'era e che cosa si è detto all'Italy-Israel Cyber Summit 2018
  The importance of the Italian-Israeli cooperation, mainly due to the complementarity of the economic systems, has been at the center of the Italy-Israel bilateral during the Cyber week in Tel Aviv. The two countries agreed on the need to broaden and complete the spectrum of action and intervention in bilateral projects.
- Cyberchallenge, perché ci serve a formare i talenti italiani della cyber security
  The 2018 edition of Cyberchallenge reminds us how important these competitions are to give Italy the cyber security resources we need.
- Ibm: Ecco i tre valori cardine della cyber security, dopo la Nis e il Gdpr
  According to IBM, cognitive technologies, integration of processes and behaviors, and the search for sophisticated and new professional skills are the three core values of cyber security.
- Cyber security, perché Israele e Italia devono cooperare. Parla Zori Kor
  Zori Kor, cyber security expert with an over twenty-year career in the ISI, today vice-president of the consulting firm Asero, is convinced that closer cooperation between the Israeli experience in the field of security and the lively Italian productive system, composed in prevalence from manufacturing SMEs with quality productions, can be an effective remedy to mitigate the dangers of the Net and lead to win-win results.

- Il CIOC per la prima volta alla esercitazione cyber Joint Stars
  The Interforces Command for Cyber Operations (CIOC), set up in 2017, will be part of the "Joint Stars" exercise for the first time in 2019 to test network and information security

European Focus

- Parliament demands EU institutions ban Kaspersky Lab cybersecurity products
  MEPs have called for the EU institutions to put more money into their in-house cybersecurity units and, in a contentious move, also demanded they stop using products from "malicious" Russian firm Kaspersky Lab. This action sets the European Parliament's approach to a European cyber defence policy, an area where EU institutions have been moving to step up their work.
- NATO and EU leaders sign joint declaration
  NATO Secretary General Jens Stoltenberg, European Council President Donald Tusk and European Commission President Jean-Claude Juncker signed a new Joint Declaration on cooperation between NATO and the European Union in a range of areas, including cyber security.
- EU countries sign declaration to form Cyber Rapid Response Teams
  At least 10 member nations of the European Union are expected by the end of the year to sign a Declaration of Intent to form multiple Cyber Rapid Response Teams (CRRTs) designed to react to major cyberattacks
- Cyber firm expands and eyes further growth in EU
  APM, a Scottish cyber security company has expanded into new Edinburgh and London offices as it eyes international growth opportunities.
- Japan, EU strengthen cybersecurity cooperation ahead of Olympics
  Since organizers of pas Gamed faced an enormous number of cyberattacks, Tokyo is expected to face no less of a cyber threat. In order to tackle this risk, Japan has been acquiring knowledge on cybersecurity through cooperation with the European Union.

Newsletter August 2018

Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- Trump revoked Obama's cyber offense order.
- Israel launches three-year program to boost cyber industry
- When China Rules the Web
- Australia: Public consultation commences on new Assistance and Access Bill
- Cubans cheer as internet goes nationwide for a day
- NATO's Advancement in Cyber

Cyber Security

- Iran hacks Israel in cyber attack
- Cyber security threat to Britain's oil and gas sites as attack could cause 'unprecedented damage'
- Facebook uncovers disinformation campaign to influence US midterms
- The state of cybersecurity at small organizations
- AI in cybersecurity: what works and what doesn't

Cyber Warfare, Intelligence and Terrorism

- China aims to narrow cyberwarfare gap with US.
- Is Singapore ready for cyber warfare?
- The age of cyberwar is here. We can't keep citizens out of the debate
- Russia to boost cooperation with BRICS countries in fighting against cyber terrorism
- The Role Al Qaeda Plays in Cyberterrorism
- Battlefield Internet

Events

- **International Workshop on Autonomics and Cloud Security (ACS)** Trento, 3-7 September 2018
- **11th Conference on Security and Cryptography for Networks (SCN)** Amalfi, 5-7 September 2018
- **International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)** Venice, 16-20 September 2018

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

Cyber Opportunities: Economy, Research & Innovation

- IBM Security Opens Network of Four Secure Testing Facilities Globally
- Facebook Issues $1M in Cyber-Security Defense Awards
- Georgia Cyber Center opens new doors for Augusta mom pursuing cybersecurity degree
- A new model for cyber risk management

Italian Focus

- Investire in cyber difesa può fare la differenza
- Che cosa deve fare l'Italia per rafforzare le sue difese cyber

European Focus

- China, EU seize control of the world's cyber agenda
- Internet overseer ICANN loses a THIRD time in Whois GDPR legal war
- Proposed EU Cybersecurity Act Released
- How does ENISA help EU member states with their cybersecurity strategies?

Newsletter September 2018

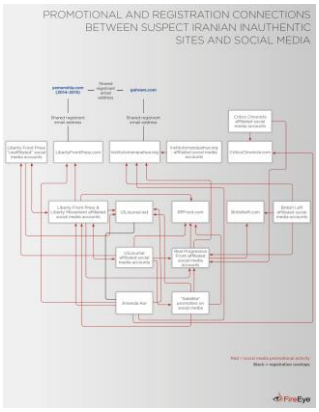
Center for Cyber Security and International Relations Studies

Cyber Policy, Diplomacy & Legal Framework

- U.S. government seeks Facebook help to wiretap Messenger
  The U.S. government is trying to force Facebook Inc (FB.O) to break the encryption in its popular Messenger app so law enforcement may listen to a suspect's voice conversations in a criminal probe.
- Tech giants warn Australia Coalition bill opens customers up to cyber attack
  Facebook, Google, Twitter and Amazon are worried that the new bill that force them to assist law enforcement agencies in decrypting private communication would open customers to cyber threats.
- Australia Government Provides 5G Security Guidance To Australian Carriers
  The Government wants to create an environment that allows Australian businesses to be at the forefront of seizing the benefits of 5G across the economy and therefore is fostering a policy and regulatory environment to support a more efficient rollout.
- Germany, seeking independence from U.S., pushes cyber security research
  Germany announced a new agency on Wednesday to fund research on cyber security and to end its reliance on digital technologies from the United States, China and other countries.
- NATO's Tallinn-based Cyber Defence Centre of Excellence gets new director
  Colonel Jaak Tarien has taken the helm at NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Tallinn, replacing Merle Maigre

Events

- **CyberTech Europe**
  Rome, 26-27 September 2018
- **Cybersecurity Europe**
  London, 3-4 October 2018
- **ICS Cybersec 2018**
  Rishon LeTzion, 11 October 2018



Cyber Security

- Five Eyes threatens to force encryption backdoors, says 'privacy is not absolute'

According to the recently issued Statement of Principles on Access to Evidence and Encryption, it seems the government intelligence alliance (representing the U.S., the U.K., Canada, Australia and New Zealand) is ready to bring the pain by pursing "technological, enforcement, legislative or other measures to achieve lawful access solutions."

- Chinese Cyberespionage Originating From Tsinghua University Infrastructure

Recorded Future's Insikt Group identified a novel Linux backdoor called "ext4," deployed against a Tibetan community attributable to one of the Chinese best universities.

- Hackers could cause havoc by Internet connected irrigation systems

  Israeli university researchers discovered that hackers could mess with a city's water supplies without attacking its critical infrastructure, but targeting the internet connected sprinklinkers.
- Google published an update on state sponsored activities

  Google has invested in robust systems to detect phishing and hacking attempts, identify influence operations launched by foreign governments, and protect political campaigns from digital attacks through our Protect Your Election program.
- Back to School: COBALT DICKENS Targets Universities

  Despite indictments in March 2018, the Iranian threat group is likely responsible for a large-scale campaign that targeted university credentials using the same spoofing tactics as previous attacks.

Cyber Warfare, Intelligence and Terrorism

- Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East

  FireEye has identified a suspected influence operation that appears to originate from Iran aimed at audiences in the U.S., U.K., Latin America, and the Middle East. This operation is leveraging a network of inauthentic news sites and clusters of associated accounts across multiple social media platforms to promote political narratives in line with Iranian interests

- Japan to beef up anti-cyberattack operations with China in mind

  The Japanese Defense Ministry plans to strengthen steps against cyberattacks by setting up its first regional cyberspace defense unit, as China bolsters its own cyber capabilities.
- Removing Myanmar Military Officials From Facebook

  Since the ethnic violence in Myanmar has been truly horrific and it wants to prevent the spread of hate and misinformation, Facebook removed a total of 18 Facebook accounts,

one Instagram account and 52 Facebook pages of individuals and organization of the country.

- Nigerian Army has established a Cyber Warfare Command to combat terrorism, banditry and other attacks by criminal groups in the country.
  The cyber warfare command, the Daily Sun gathered, is charged with the responsibility of monitoring, defending and attack subversive elements in the cyberspace. It will also be expected to provide real-time information to fighting troops and commanders in the field from the highly sophisticated equipment so far installed to checkmate the counter terrorism fight, herdsmen/militia killings, armed banditry, pipeline vandalism among others.
- Turkish group hacks Egypt's state news agency
  Egypt's state news agency was hacked Sept. 11 by a Turkish group condemning mass death sentences given by the country on Sept. 8.The group replaced MENA's front page with a picture of Mohammed Beltagy, the father of Asmaa, who was shot dead during protests in Cairo in 2013.

Cyber Opportunities: Economy, Research & Innovation

- Microsoft is taking new steps against broadening threats to democracy
  Microsoft's Defending Democracy Program launched a new initiative called Microsoft AccountGuard. This initiative will provide state-of-the-art cybersecurity protection at no extra cost to all candidates and campaign offices at the federal, state and local level, as well as think tanks and political organizations we now believe are under attack. The technology is free of charge to candidates, campaigns and related political institutions using Office 365
- Google tracks users even with location history turned off
  An American Agence Press, along with Princeton University researchers, found that Google services such as Google Maps and the Google search engine record Android and iPhone users' locations without their permission.
- Tech Companies Are Gathering For A Secret Meeting To Prepare A 2018 Election Strategy
  Representatives from a host of the biggest US tech companies, including Facebook and Twitter, have scheduled a private meeting for Friday to share their tactics in preparation for the 2018 midterm elections.
- China launches official online rumor information platform
  In late August, China launched a national-level platform to alert the public about online rumors and refute slander. The platform allows the public to quickly discover and debunk rumors floating around online, while at the same time throwing light on pseudoscientific theories.

Italian Focus

- Cybersecurity, Mattarella: allarmante Stati ostili dietro attacchi web
  States have an obligation to defend their fellow citizens from virtual attacks ". This was underlined by President Sergio Mattarella talking about cybersecurity from Latvia, on the occasion of the "Arraiolos" summit among 13 European heads of state.
- L'Italia ha un futuro cyber (non solo nella difesa europea). L'idea di Tofalo
  In Seoul, where Defense Dialogue 2018 was held, Undersecretary of Defense Angelo Tofalo re-launched the idea of a peninsula that should play a leading role in innovative and high-tech sectors, without asking geographical limits.
- Intelligenza artificiale, l'Italia ci prova. E il Mise chiama a raccolta gli esperti
  The Ministry of Economic Development will select thirty experts to elaborate an Italian strategy to get to know, deepen and deal with the issue of artificial intelligence, with the aim of increasing public and private investments in this direction and technologies closely related to it.

European Focus

- Juncker goes to war against disinformation and online terrorist content
  The European Commission is set to pursue a crackdown on the spread of online terrorist content and disinformation, its president Jean-Claude Junker announced in his state of the union address on Wednesday (12 September).
- EU Elections 2019: Critical cyberattacks loom, Estonia warns
  The 2019 European elections could be hit by a spate of cyberattacks, which could even prevent the new European Parliament from convening, a report led by the Estonian Information System Authority has warned.
- Non solo Italia. L'Europa e la task force per l'etica dell'intelligenza artificiale
  The EU Commission has chosen a group of 52 experts to outline the development and use of AI in Europe, not only by promoting its development in an innovative and responsible way in the various fields of application, but also by helping Europe to become the reference on AI in the world.
- Pubblicato il Decreto Legislativo di armonizzazione al GDPR: novità in materia di Lavoro, sanzioni e piccole e medie imprese
  On 4 September 2018 the Legislative Decree 101/2018 of harmonization of the national legislation to the EU Regulation no. 679 of 2016 ("GDPR")was published on the Official Journal.

Center for Cyber Security and International Relations Studies

Newsletter October 2018

Cyber Policy, Diplomacy & Legal Framework

- Russia accused of cyber-attack on chemical weapons watchdog
  Netherlands expelled four GRU officers after alleged attacks on OPCW and UK Foreign Office
- UK exposes Russian cyber attacks
  The UK National Cyber Security Centre has identified a campaign by the Russian military intelligence service of indiscriminate and reckless cyber attacks.
- AggregateIQ Hit With First GDRP Enforcement Notice
  UK regulators have hit Canada's AggregateIQ (AIQ) with the country's first GDPR enforcement notice, giving the Vote Leave-associated data company 30 days to comply with data regulations or face a fine of up to €20 million.
- U.S. Hosts Ministerial Meeting at UNGA on Advancing Responsible State Behavior in Cyberspace
  On September 28, 2018, Deputy Secretary of State John J. Sullivan hosted a ministerial meeting on advancing responsible state behavior and deterring malicious activity in cyberspace.

32 amid concerns and objections from journalist community and other rights bodies.

- Aadhaar: India top court upholds world's largest biometric scheme
  India's Supreme Court has ruled that the country's controversial biometric identity scheme is constitutional and does not violate the right to privacy.

Cyber Security

- Facebook revises number of accounts hacked, says 29 million were affected
  Facebook says hackers accessed data from 29 million accounts as part of the security breach disclosed two weeks ago, fewer than the 50 million it initially believed were affected
- Russia cyber-plots: US,UK and Netherlands allege hacking
  Russian spies have been accused of involvement in a series of cyber-plots across the globe, leading the US to level charges against seven agents.
- A Recent Startup Breach Exposed Billions of Data Point
  The sales intelligence firm Apollo sent a notice to its customers last week disclosing a data breach it suffered over the summer.
- Apple chief says firm guards data privacy in China
  Apple chief executive Tim Cook said the company is devoted to protecting people's privacy, with data encrypted and locked away on servers even in China.
- Google Exposed User Data, Feared Repercussions of Disclosing to Public
  Google exposed the private data of hundreds of thousands of users of the Google+ social network and then opted not to disclose the issue this past spring, in part because of fears that doing so would draw regulatory scrutiny and cause reputational damage
- Russian State-Sponsored Operations Begin to Overlap
  Kaspersky Lab security researchers have uncovered new evidence that shows overlaps between the activity of infamous Russian cyber-espionage groups Turla and Sofacy.

systems.

- Critical Vulnerability in Telegram Leaks User IP Addresses
  A vulnerability was found in messaging app Telegram due to a voice call bug. The IP addresses of users appeared in the logs stored in telegram servers for hours instead of being encrypted

Cyber Warfare, Intelligence and Terrorism

- US to Offer Cyber Warfare Technology to NATO
  A United States official says the U.S. military is offering its cyber warfare technology, including computer software tools, to the North Atlantic Treaty Organization (NATO), in order to help the 69-year-old alliance better deal with cyber threats from Russia and China
- Australia: Cyber-warfare and its threat to elections
  Interview with Professor Matthew Warren from the Centre for Cyber Security Research at Deakin University to talk more about cyber-warfare and if he thought there'd been any foreign interference in Australian elections.
- Britain FIGHTS BACK: Cyber warfare capabilities expanded amid threat from Russia and Iran
  Britain's cyber warfare capabilities are to receive a major boost as military and spy chiefs expand their offensive operations to counter growing threats posed by Russia, Iran and North Korea.
- Cyberwarfare is the new frontier in the Gulf
  Cyberwarfare has become the new frontier with very few rules. This is especially true across borders. Countries with limited resources, such as Iran and North Korea, have developed cyberwarfare capabilities to compensate for their lack of sophisticated weapons.
- Russian hackers are taking their cyber warfare to the next level
  Researchers with the cybersecurity company ESET have discovered what is believed to be the first known UEFI rootkit malware used in a cyber attack.

Cyber Opportunities:

Economy,Research & Innovation

- Here's how to see if your personal data was stolen in the recent Facebook hack
  Hackers stole personal data from 29 million Facebook users in a recent hack, including information like phone numbers, emails, gender, hometowns and even relationship data. Was your data stolen?
- Market Growth: Global Enterprise Cyber Security Market Research Report 2025: Venustech, Westone, Huawei, Sangfor
  This report studies the global Enterprise Cyber Security market size, industry status and forecast, competition landscape and growth opportunity.
- How cyber security opens tech opportunity for New York City
  According to James Patchett, 30 million$ seed investment in Cyber NYC could build out the city's tech presence while protecting vital institutions.
- Can smart cities prevent cyber risk?
  At the rate smart city initiatives are being hatched in every corner of the globe, the real estate sector is racing to embrace technology to catch up with the new requirements of an industry that has gone digital almost overnight.

Italian Focus

- L'Italia in futuro potrebbe avere una Forza Armata cyber
  The Italian Undersecretary of Defense(Tofalo) said at Cybertech Europe 2018 that he is working on the project of a cyber-armed force that will have both offensive and defending capabilities
- L'Italia della cyber security si presenta a Londra.
  Companies, diplomacy and universities gathered to discuss opportunities and cooperation during a forum organized by the Embassy of Italy in London, the ICE and the Center for Cyber Security and International Relations Studies of the University of Florence
- La roadmap verso la Cyberawareness: intervista a Pier Luigi Rotondo (CLUSIT)
  As stated in the last annual report on ICT Security edited and published by CLUSIT and related to the threats of the year 2017, over one billion individuals have been hit by computer scams, theft of money and personal data, for a total estimated damage in over 180 billion dollars.
- Italia, in corso una massiccia campagna phishing che coinvolge le banche
  New massive campaign of phishing cyber attacks in Italy. Cyber criminals use fake bank sites to steal credentials to access victims' accounts.
- Cyber security, nazionale italiana hacker in ritiro a Lucca
  Italy will participate at the European Cyber Security Challenge (Ecsc), the European cybersecurity championships. The task of forming the Italian national team of Cyberdefender was entrusted given to Cini.

European Focus

- EU lawmakers push for cybersecurity, data audit of Facebook
  European Union lawmakers appear set this month to demand audits of Facebook by Europe's cybersecurity agency and data protection authority in the wake of the Cambridge Analytica scandal.
- Il bilancio di Cybertech Europe 2018
  More than 100 companies, thousands of participants from over 40 countries worldwide: these are the numbers of the third edition of Cybertech Europe 2018, the most important European event dedicated to the cyber security sector organized in collaboration with Leonardo and with the innovation partner Accenture , which took place in Rome on 26 and 27 September.
- Come costruiremo l'Europa della cyber security. Parla Campora (Leonardo)
  The European Union aims to become, like the United States and the Asian giants, one of the world leaders in the strategic sector of cyber security. To do so, it is promoting a series of initiatives and Italy and its national champion in the fields of defense, security and aerospace, Leonardo, have also played a major role.
- Europe needs urgent cybersecurity action
  With at least seven parliamentary elections scheduled for in the European Union in 2019, plus European Parliament elections, the continent's leaders are in a frenzy of damage control. The European Commission has launched initiatives to harden information technology infrastructure and fight fake news and it is organising a high-level conference in October on Election Interference in the Digital Age.

Upocoming Events

- October 25
  Conflitti ed Alleanze nello Spazio Cibernetico (Milano)

- October 31

  Cloud Security Summit

Further information at

https://www.cssii.unifi.it

Contact us at

cyber@cssii.unifi.it

In relazione alle disposizioni del D.lgs del 10/08/2018 n° 101 La informiamo che i suoi dati verranno trattati da Center for Cyber Security and International Relation Studies al solo fine dell'invio della presente comunicazione e non verranno fatti oggetto di divulgazione o comunicazione alcuna. In ogni momento Le sarà possibile richiedere la rimozione del proprio indirizzo di posta elettronica, dalla mailing list di cyber@cssii.unifi.

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

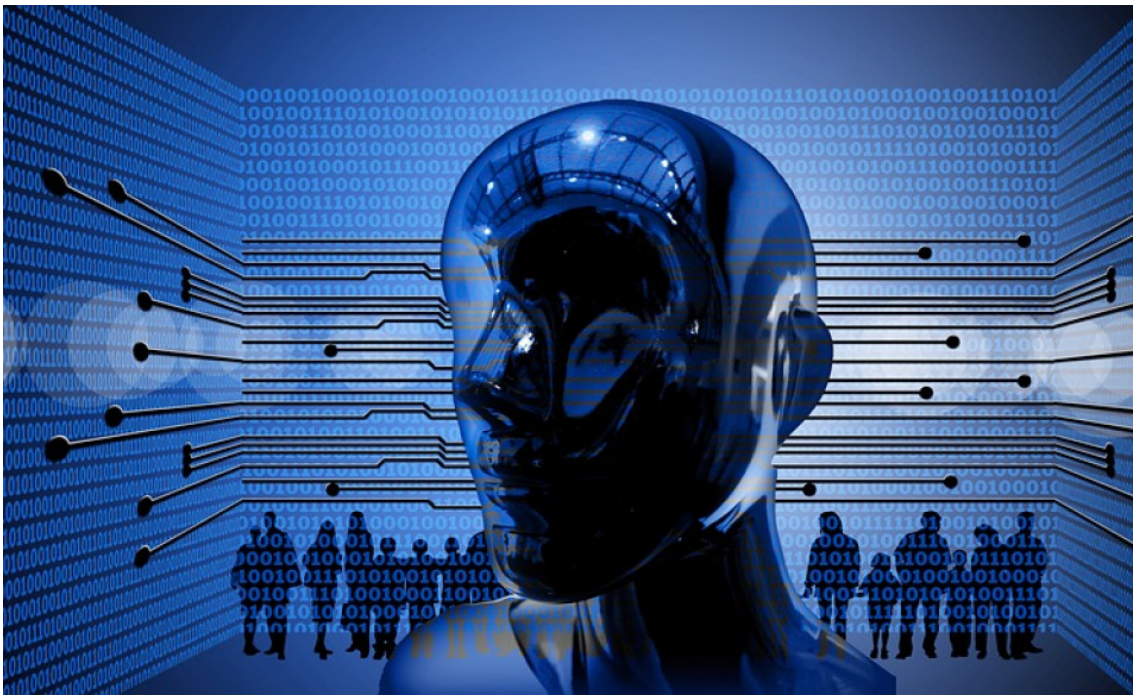
- Cyber security, come cambiano conflitti e alleanze nel quinto dominio

  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

Center for Cyber Security and International Relations Studies

Newsletter December 2018

Cyber Policy, Diplomacy & Legal Framework

- Sen. Warner calls for national cyber-policy overhaul
  During his speech at the Center for New American Security, the senator proposed a new "Cybersecurity Doctrine" to secure American networks and data. The vice chairman of the Senate Intelligence Committee, suggests the U.S. has been asleep at the keyboard while our adversaries were launching cyber attacks with relative impunity.
- Australia approved data encryption laws
  The Australian government passed into law a piece of legislation that would require tech companies to provide law enforcement access to users' encrypted communications. Cybersecurity experts say the new law will open people's communications up to spies and hackers.
- Trump is ready to fight Chinese hacking
  The Trump administration is seeking to show in a range of ways that China has not operated in good faith on cybersecurity. The Trump administration is preparing actions this week to

computers, according to U.S. officials.

- NATO and the European Union work together to tackle growing cyber threats
  On December 10, senior officials from the European Union and NATO met yesterday to discuss recent cyber security and defence developments at the EU and NATO along with perspectives on EU-NATO cooperation on cyber defence.

Cyber Security

- Marriott discloses massive data breach affecting up to 500 million guests
  Hackers stole data from as many as 500 million guests who made reservations at Marriott's Starwood properties, including some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.
- "Malicious" Quora Data Attack Compromises 100 Million Users
  Quora, the Q&A website, said data for about 100 million user accounts were compromised, including usernames, email addresses, password hashes, and more. Quora said about 300 million people use the website each month.
- Amazon hit with major data breach days before Black Friday
  Amazon has suffered a major data breach that caused customer names and email addresses to be disclosed on its website, just two days ahead of Black Friday. The tech giant said it has contacted customers that have been affected.
- Super Micro says review found no malicious chips in motherboards
  An external audit of Supermicro, the IT firm at the center of a widely disputed Bloomberg Businessweek report that alleged the presence of Chinese spy chips on the motherboards the company sells, said it found no such malicious implants. Independent investigators turned up no evidence of eavesdropping equipment in their review of current and former models of Supermicro devices.

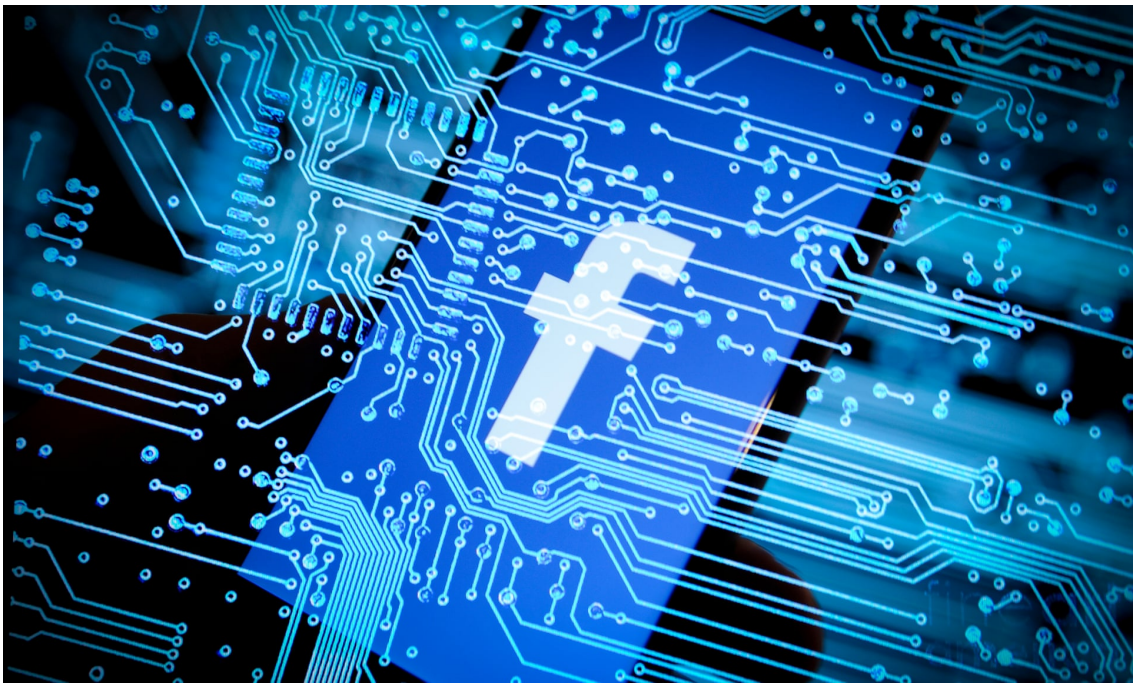
Equifax Inc. failed to modernize its technology security to match the company's aggressive growth strategy and data gathering, a shortcoming that left it open to the 2017 hack that compromised the information of 148 million people, according to a House Oversight Committee report.

Cyber Warfare, Intelligence and Terrorism

- The Nigerian Cyber Warfare Command: Waging War In Cyberspace
  The Nigerian Army has established a Cyber Warfare Command to combat terrorism, banditry and other attacks by criminal groups in the country. The cyber warfare command is charged with the responsibility of monitoring, defending and attack subversive elements in the cyberspace.
- The hacker that became the World's Most Dangerous Terrorist
  The 21-year-old was one of the architects behind a wave of plots and attacks under the ISIS banner, stretching back to 2014.He swapped Kings Heath for the terror group's then de-facto capital of Raqqa in Syria, landing himself on the US Government's most wanted list. The propagandist was considered a "top threat" at the Justice Department.
- Microsoft is fighting to stop a cyber world war
  The tech industry is becoming more worried about a cyberwar arms race. According to Microsoft's President Brad Smith, technology was advancing at an enormous pace in the first decades of the twentieth century, but human institutions failed to keep up. This is why he called governments to stand up for the protection of the civilians and civilian infrastructure, and safeguard the internet in general from cyber attacks.
- Cyber Terrorism and its Securitization in Pakistan
  Pakistan is the second most spied on country and NSA has intercepted more than 13.5 billion pieces of information from Pakistan. Absence of strong filters and blocking mechanisms is helping criminal and terrorist organizations to carry on their malicious

place in realm of cyber space.

- Spying and propaganda are now greater challenges than terrorism, Canada's spy chief says
  Canadian spy chief David Vigneault said this week his agency is more consumed by fighting foreign interference, spying, and cyber threats than terrorism, marking a major shift in challenges since the 9/11 attacks upended national security priorities in 2001.
- The threat of cyberattacks on satellites
  The satellites today are a vital part of our lives and they are essentials for the management of telecommunications and Internet. But they are not exempt from risks of hacking and cyber threats. They can be used as a vector for cyber attacks of different kinds as they have different points of vulnerability.



Cyber Opportunities:
Economy,Research & Innovation

- Facebook defends Mark Zuckerberg's exposed emails
  Facebook has faced several scandals over the course of 2018, and among these, on December 6, Facebook had some 250 pages worth of internal emails released to the public by the UK Parliament. The documents reveal previously unknown details around the company's internal behaviour.

- Consumer location-tracking: are the data really anonymous?
  New York Times investigation dug into the shady economy of consumer location-tracking. Reporters discovered they could easily—and with fine granularity—monitor people's movements as they traveled to their offices, homes, doctor appointments, and schoolyards.

- BlackBerry bets on AI and cybersecurity with $1.4 billion deal for Cylance
  The once-dominant smartphone maker known for producing mobile devices offered $1.4 billion in cash to Cylance, a cybersecurity firm that specializes in machine learning-enabled threat detection. Pending regulatory approval, expected by February, the purchase will deplete more than half of BlackBerry's cash pile.

according to a new survey of risk managers and nonrisk professionals by the Depository Trust and Clearing Corp. Geopolitical risk and trade tensions was the second most-cited risk.

- US vs Huawei: The security concerns
  Western intelligence agencies believe that Huawei could pose a significant threat to global security. This is a key element to take into consideration when analysing the resons behind the detention in Canada of Meng Wanzhou, Huawei's CFO and the daughter of its founder.

Italian Focus

- An anti-cyberbullism library opens in Rome
  The initiative aims to shed light on a overlooked phenomenon by organizing events and workshops to raise awareness among the youngsters. The idea has been developed by the Italian police, the Cini consortium and several public libraries in Rome.

- Italian accounts on the dark net: how to solve the problem
  To reduce the risk of cyber attacks that can put government credentials at risk, we need to act both at the technical level, but also at the human level. At the same time, there is the need to activate all the processes that could enhance threat identification.

- The Italian Hacker team met Cybaze
  On the 29th of November at the Hotel Gallia in Milan, coaches and players of the Italian National Hackers Team met the President and the CEO of the Italian cybersecurity company Cybaze to talk about information sharing and education in the cybersecurity field.

European Focus

- EU agrees new cyber security policy after Wannacry 'wake up call'
  European Union negotiators have agreed on a cyber security act to defend against large-scale data breaches after the "wake up call" from Wannacry and NotPetya
- EU leaders agree on ground-breaking regulation for cybersecurity agency ENISA
  ENISA welcomes the political agreement on the Cybersecurity Act reached on 10 December 2018 by the European Parliament, the Council of the European Union, and the European Commission. Henceforth, ENISA will be known as 'the EU Agency for Cybersecurity'.
- New ENISA report on the economics of vulnerability disclosure
  A new ENISA report published on the 14th of December aims to provide a glimpse into the costs, incentives, and impact related to discovering and disclosing vulnerabilities in information security.
- New Eu guidelines for assessing security measures in the context of net neutrality
  Within the context of the EU's net neutrality regulation, called the Open Internet Regulation, which came into force in 2016, internet providers should treat all internet traffic to and from their customers equally. The power to assess whether or not security measures are justified lies with the national telecoms regulatory authorities (NRAs). ENISA developed a guideline to support NRAs in their assessment.

Upocoming Events

- January 8
  HICSS Symposium on Cybersecurity Big Data Analytics
- January 11-13
  IEEE International Conference on Consumer Electronics
- January 16-18
  International Conference on Global Security, Safety & Sustainability

Further information at

https://www.cssii.unifi.it

Contact us at

cyber@cssii.unifi.it

In relazione alle disposizioni del D.lgs del 10/08/2018 n° 101 La informiamo che i suoi dati verranno trattati da Center for Cyber Security and International Relation Studies al solo fine dell'invio della presente comunicazione e non verranno fatti oggetto di divulgazione o comunicazione alcuna. In ogni momento Le sarà possibile richiedere la rimozione del proprio indirizzo di posta elettronica, dalla mailing list di cyber@cssii.unifi.