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.

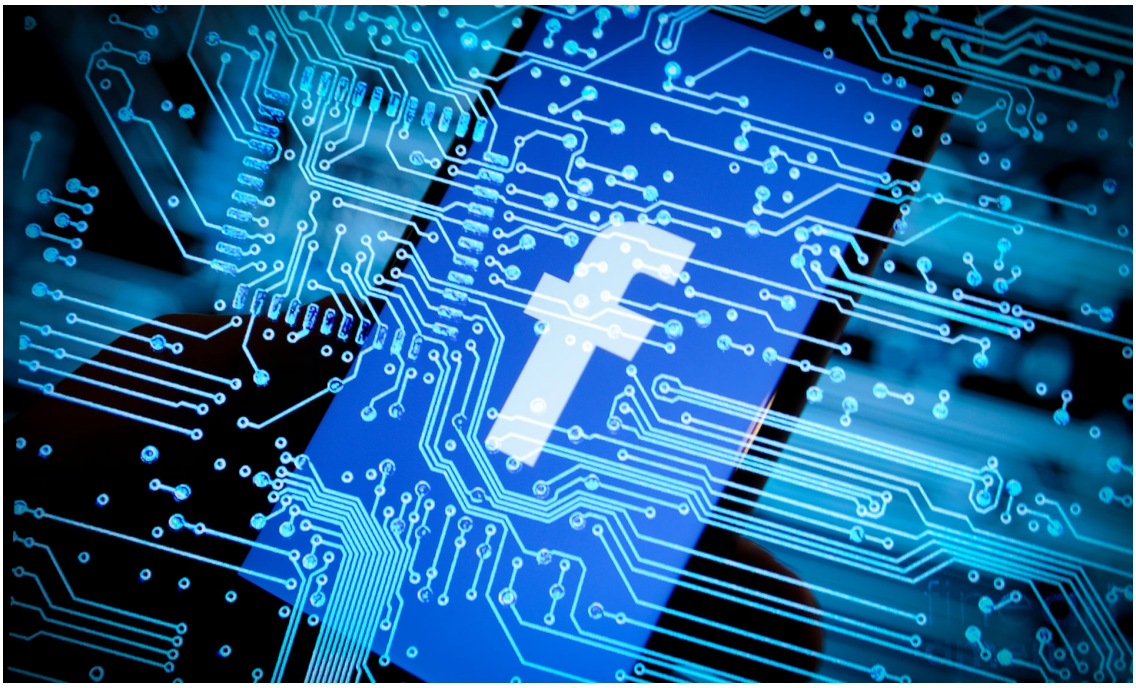
Equifax Inc. failed to modernize its technology security to match the company's aggressive growth strategy and data gathering, a shortcoming that left it open to the 2017 hack that compromised the information of 148 million people, according to a House Oversight Committee report.

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.