Newsletter September 2018

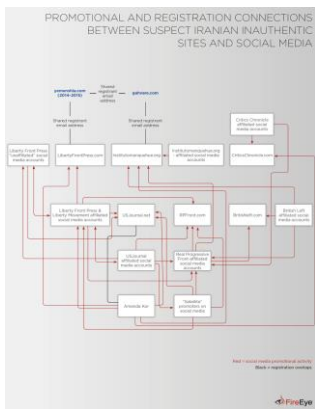**Center for Cyber Security and International Relations Studies**

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

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

Cyber Security

PROMOTIONAL AND REGISTRATION CONNECTIONS BETWEEN SUSPECT IRANIAN INAUTHENTIC SITES AND SOCIAL MEDIA

- **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.