le cnam
ESDR3C

Security and Defence Research Team

Axis 2 - Cybersecurity, Cybercrime, Cyberdefense (C3)

Professors supervising the research axis: Pr. Philippe Baumard (Cnam), Pr. Sandro Gaycken (ESMT - Berlin), Pr. John C. Mallery (MIT)

Associate researchers: Prof. Chris Demchack, Prof. Gary Brown, Prof. Paul Cornish, Prof. Robert Jervis, Prof. Nohyoung Park, Prof. Tim Stevens, Dr. Julia Pieltant, Dr. Nadim Kobeissi, Dr. Camino Kavanagh, Dr. Enekken Tikk, Prof. Joshua Walker, Ambassador Heli Tirmaa-Klaar, Prof. Martha Finnemore, Prof. Henri Farrel, Dr. Carl Horn.

Associate experts: Anne C. Bader, Nigel Inksten, Rafal Rohozinski, Marcus Willett, Yoko Nitta, Dr. James Andrew Lewis, Dr. Joel Brenner.

The strong growth in IT attacks over the period 2008-2017 raises the issue of the **cost of maintaining an operational environment**for the digital economy, which could ultimately threaten the growth and sustainability of industries dependent on IT infrastructures. Targeted attacks (Advanced Persistent Threats) have experienced a **strong growth since 2010**: 40% annual growth, with 20% of affected companies reporting financial damage (KCS-CERT 2012 & PWC 2011),**including more than 50% of incidents (intrusion, deterioration, espionage) for the energy (nuclear, oil) and critical infrastructure industries.**

Economically, **the cost of security and vulnerability remediation**theis absorbed by affected **businesses**, **consumers** , **governments**, **telecommunications operators** and **service providers**. The industry suffers from the lack of a clear **regulatory framework** for sharing the burden of dealing with **the damage caused by large-scale attacks**, both in the United States and in Europe, Latin America and Southeast Asia.

At the strategic level, the use of large-scale attacks has entered the arena of confrontation between nations (e.g. Stuxnet campaigns, Flame) and has more recently become a vector for **terrorist attacks**and the growth of **organized crime**.

Technically, the critical infrastructures of G8 companies suffer from **systemic vulnerabilities**and designs related to**IT architectures inherited from the 1980s.**

The companies surveyed declare a **high level of dissatisfaction** with the existing offer, with a**failure rate** of protection solutions **exceeding 25%** (see CERT US 2017 national study, above). Both the North American governmental CERT and the ANSSI in France have recorded an exceptional growth in security incident reports.

Associated Research Projects

Research Project 5: Current Status of Cyber Security Threats and Issues

Research Project 6: The disruptive impact of AI and innovations in cyberspace on the growth of terrorist and criminal threats

Research Project 7: Organized crime: the new dominant player in cyberspace?

Research Project 8: Cyber-terrorism: what risks, what scenarios?

https://esd-en.cnam.fr/axis-2-cybersecurity-cybercrime-cyberdefense-c3--1223707.kjsp?RH=1576512148977