Axe 2 - Cybersecurité, Cybercrime, Cyberdéfense (C3)

Professeurs supervisant l'axe de recherche: Pr. Philippe Baumard (Cnam), Pr. Sandro Gaycken (ESMT - Berlin), Pr. John C. Mallery (MIT)

Chercheurs associés: 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.

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

La forte croissance des attaques informatiques sur la période 2008-2017 soulève la question du**coût du maintien d'un environnement opérationnel**pour l'économie numérique, qui pourrait à terme menacer la croissance et la durabilité des industries dépendantes des infrastructures informatiques. Les attaques ciblées (Advanced Persistent Threats) ont connu une **forte croissance depuis 2010** : 40% de croissance annuelle, 20% des entreprises touchées signalant des dommages financiers (KCS-CERT 2012 & PWC 2011), **dont plus de 50 % des incidents (intrusion, détérioration, espionnage) pour les secteurs de l'énergie (nucléaire, pétrole) et des infrastructures critiques.**
Sur le plan économique, **le coût de la sécurité et de l'élimination des vulnérabilités** est absorbé par **les entreprises, les consommateurs, les gouvernements, les opérateurs de télécommunications et les fournisseurs de services touchés**. L'industrie souffre de l'absence d'un **cadre réglementaire clair**pour partager la charge de la réparation des **dommages causés par les attaques à grande échelle**, tant aux États-Unis qu'en Europe, en Amérique latine et en Asie du Sud-Est.

Au niveau stratégique, le recours aux attaques à grande échelle est entré dans l'arène de la confrontation entre nations (par exemple, les campagnes Stuxnet, Flame) et est devenu plus récemment un vecteur **d'attaques terroristes** et de croissance des activités du **crime organisé**.

Sur le plan technique, les infrastructures critiques des entreprises du G8 souffrent de **vulnérabilités systémiques** et de conceptions liées aux **architectures informatiques héritées des années 1980.**

Les entreprises interrogées déclarent un **niveau élevé d'insatisfaction** par rapport à l'offre existante, avec un **taux d'échec** des solutions de protection **supérieur à 25 %** (voir l'étude nationale CERT US 2017). Le CERT nord-américain et l'ANSSI en France ont tous deux enregistré une croissance exceptionnelle des rapports d'incidents de sécurité.

Projets de recherche associés

Projet de recherche 5 : Situation actuelle des menaces et enjeux de la cybersécurité

Projet de recherche 6 : L'impact disruptif de l'IA et des innovations dans le cyberespace sur la croissance des menaces terroristes et criminelles

Projet de recherche 7 : Le crime organisé : nouvel acteur dominant dans le cyberespace ?

Projet de recherche 8 : Le cyberterrorisme : quels risques, quels scénarios ?

https://esd.cnam.fr/axes-de-recherche/axe-2-cybersecurite-cybercrime-cyberdefense-c3--1117324.kjsp?RH=1561452