

Axe 2 - Cybersecurité, Cybercrime, Cyberdéfense (C3)

Philippe Baumard (PU, CNAM), Sandro Gaycken (PR, EMST- Berlin), John C. Mallery (MIT), Julia Pieltant (MCF Cnam)

Chercheurs associés: Pr. Chris Demchak, Pr. David B. Mussington, Pr. Gary Brown, Pr. Paul Cornish, Pr. Robert Jervis, Pr. Nonyoung Park, Pr. Tim Stevens, Dr. Nadim Kobeissi, Dr. Camino Kavanagh, Dr. Eneken Tikk, Pr. Joshua Walker, Pr. Heli Tirmaa-Klaar, Pr. Martha Finnemore, Pr. Henry Farrell, Dr. Carl Horn, Joseph Cannataci, Brown G .

Experts associés: Rafal Rohozinski, Marcus Willett, Yoko Nitta; Meuel P Klein E Tikk Eneken Kobeissi N.

Doctorants : Marie Devillers ; Marie Garbez ; Bouchra Hasnaoui.

L'étude des menaces liées au cyberspace est un axe prioritaire de toute réflexion stratégique sur la sécurité et la défense d'un territoire et de sa population au XXI^e siècle^[1]. Le cyberspace est avant tout un champ d'expansion majeur pour tous les phénomènes et acteurs criminels. En effet, les réseaux criminels ont très tôt compris la puissance des réseaux de communication cachés (Darknet) pour déplacer massivement et discrètement les flux financiers blanchis, les biens, activités et services illicites, voire pour en créer de nouveaux adaptés à ces nouveaux marchés.

Le cyberspace est ainsi devenu l'un des principaux pourvoyeurs de radicalisation et les communautés d'expérience qui se sont massivement développées sur Internet jouent un rôle central dans l'endoctrinement et le recrutement de futurs djihadistes.

La sécurité du cyberspace est au cœur de nouveaux défis: le Machine Learning est par exemple capable de générer un comportement humain, dissimulé derrière des activités normales et généralement au service des mafias et des cybercriminels; Cette révolution de l'intelligence artificielle, à la hauteur des rêves de Turing, Simon et Newell, devient une menace pour toutes les populations, en raison de la performance accrue des ordinateurs, du crowdsourcing et des outils de Big Data issus des réseaux sociaux et des objets connectés^[2]. Des cas d'attaques via un comportement simulé d'IA sont déjà en vigueur sur les réseaux sociaux. Enfin, ce nouvel espace s'est développé sur des bases fondamentalement informatiques et économiques (modèle d'entreprise GAFAM), avec une quasi-absence des systèmes de régulation traditionnellement présents dans nos sociétés modernes, et sans l'apport des sciences humaines et sociales; la méconnaissance des caractéristiques et du fonctionnement de ce nouvel espace d'échange met en péril la résilience des institutions publiques et privées et a un impact important sur la gouvernance de nos sociétés démocratiques^[3].

Cet axe de recherche aborde les questions de cybersécurité sur l'ensemble de son spectre, depuis son corpus technique (cryptographie, techniques offensives) jusqu'à son corpus social (psychologie, sociologie) et géopolitique (guerre de l'information, opérations de guerre psychologiques, cyberdéfense).

Né d'une coopération avec le CSAIL (Computer Science and Artificial Intelligence Laboratory) du MIT débutée en 2012, cette équipe assure la coprésidence du comité d'organisation d'un groupe de recherche international qui se réunit tous les 3 mois, et compte en son sein 40 chercheurs, décisionnaires civils et militaires traitant la question de la cyberstabilité militaire (Roundtable on Military Cyber-Stability - RMCS). Le volet recherche donne lieu à des formations par la recherche, notamment au sein du CRM 210, cours du M2 portant le même titre. Le programme de recherche est dédié à l'exploration des thèmes encourageant la coopération (inter-États, police, services, industrie et recherche) pour une meilleure résilience et sûreté numérique. L'objectif est de réunir différentes perspectives, européennes, américaines, chinoises ou russes sur les questions de recherche suivantes :

Quel cadre de régulation pour la question de l'attribution des attaques et la prise en charge des coûts des dommages engendrés ? (Assimilation des coûts à la source, WTO, EU, agences internationales de type ENISA ou agences domestiques, etc.).

Quel degré d'extra-territorialité peut-il être toléré dans la mise en œuvre des contre-mesures ? (Arrêt de campagnes offensives, dissuasion). Quels sont les enjeux économiques, au plan européen, d'une possible régulation supranationale de la contre-mesure ? Quels sont les enjeux de compétitivité et de souveraineté nationale associés ?

Quelle métrique utiliser pour mesurer l'impact financier et économique de la cybersécurité en Europe ?

(Discussion des mesures courantes, enjeux du système métrique choisi)

Quelle politique de régulation pour le partage des coûts de résilience de l'industrie numérique et de télécommunications européenne ?

Quelles sont les stratégies viables de monétisation et de création de valeur concernant la sécurisation des modèles économiques des FAI et des producteurs de services ?

Comment pallier la croissance de l'économie grise des incitations à la cybercriminalité ? (Mécanismes, régulations, politiques des fournisseurs de logiciels).

L'agenda de recherche de cette équipe est l'étude de la convergence des capacités numériques Étatiques, militaires et issues du crime organisé, et leur impact sur la stabilité stratégique des organisations d'intérêt vital (OIV), des institutions régaliennes (services du 1er cercle), ou des intérêts de la nation au sens large. Il ne s'agit donc pas, au sens strict, d'une équipe dédiée à la cybersécurité (au sens technique), mais à l'intersection des relations internationales, des sciences politiques, du renseignement et des systèmes capacitaires numériques (tout moyen offensif, depuis le spectre physique, jusqu'à la guerre cognitive et les opérations de déstabilisation) :

Sur le plan économique, le coût de la sécurité et de la correction de vulnérabilités est absorbé par les entreprises affectées, les consommateurs, les États, les opérateurs de télécommunications et les fournisseurs de services. Le secteur souffre de l'absence d'un cadre de régulation clair quant au partage de la prise en charge des dommages causés par les attaques de grande échelle, aussi bien aux Etats-Unis, qu'en Europe, Amérique Latine et Asie du Sud Est.

Sur le plan stratégique, le recours à des attaques de large échelle est entré dans l'arène de confrontation entre nations (ex : campagnes Stuxnet, Flame), et plus récemment, devenu un vecteur d'acteur d'attaque terroriste et de croissance de la criminalité organisée.

Les incitations économiques de l'économie grise de la sécurité informatique, et les défaillances des modèles économiques en présence sur le marché, sont les principaux vecteurs de la montée en puissance des attaques sur le plan global. Ces éléments nouveaux comprennent :

La forte croissance des marchés parallèles - et légitimes - des exploits (découvertes de failles pouvant être exploitées pour mener une attaque). Le paiement des découvertes de faille a connu, en valeur, une croissance sans précédent (selon les estimations, entre 200% et 300%) ;

La location de capacités offensives s'est de son côté démocratisée, avec la possibilité de louer des botnets pour des coûts inférieurs à 500\$;

La détérioration de la perception de ce qui est « légitime » par les consommateurs (perception de la paternité, de la propriété du numérique, du libre usage, du « droit » de visionner des matériaux en streaming, etc.) ;

La croissance des modèles économiques adossés aux réseaux sociaux, qui crée une réserve de valeur marchande au sein de cibles particulièrement mal protégées. La monétisation des réseaux sociaux constitue une incitation forte pour la petite criminalité informatique (vols d'identité, vols d'identifiants CB, etc.) ;

La délocalisation des données, l'accès à distance (cloud) et la numérisation des monnaies constituent une autre incitation économique à la criminalité informatique, créant un transport de données susceptible d'être monétisé sur le marché gris ou illicite de la cybercriminalité (vols d'identifiants en masse, extorsions, chantage aux données auprès de marchands ou d'opérateurs OIVs).

L'émergence de capacités IA très faiblement régulées (grands modèles de langage : LLM, IA génératives), qui génèrent de nouvelles capacités offensives, mais élargissent également les surfaces d'attaques en créant des vulnérabilités cognitives globales.

Cet état des lieux distingue un ensemble de déterminants cruciaux de l'économie et des enjeux de sécurité :

La continuité d'opération des fournisseurs d'accès à Internet et la stabilité des infrastructures numériques ;

La résilience de services aussi bien pour les opérateurs d'infrastructures vitales (santé, hôpitaux, services publics, énergie, etc.) que pour des services publics et régaliens (administrations, défense) ;

La sécurité des paiements et des transactions électroniques, qui encouragent la criminalité numérique en lui offrant une incitation à la consommation de biens numériques obtenus illégalement (torrent, streaming illégal, contrefaçon de logiciels, vols d'accès, usurpation d'identité) ;

L'investissement de renouvellement et de progression générationnelle des infrastructures numériques (fibre, très haut débit) qui repose sur le maintien d'une rentabilité et d'une visibilité des coûts d'investissement à long terme.

[1] Nye, Joseph S., Jr. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly*, December 2011. Accessed January 1, 2017. <http://www.au.af.mil/au/ssq/2011/winter/nye.pdf>.

[2] Schneier, Bruce. *Data and Goliath: the hidden battles to collect your data and control your world*. New York, NY: W.W. Norton & Company, 2016. Page 27

Questions de recherche associées

Comment la résilience des services, à la fois des opérateurs d'infrastructures critiques (santé, hôpitaux, services publics, énergie, etc.) et des services souverains et publics (administrations, défense) est-elle affectée par l'utilisation accrue des outils numériques et de l'intelligence artificielle? Quels sont les scénarios d'évolution de la vulnérabilité de ces institutions à travers l'UE?

Comment les liens croissants entre les cyber-mercenaires, les groupes criminels, les djihadistes et les groupes armés paraétatiques représentent-ils une nouvelle menace pour la souveraineté et la sécurité des États de l'Union européenne?

De quels outils l'Union européenne dispose-t-elle, notamment par l'intermédiaire d'institutions spécialisées telles que Eurojust et Europol, pour mieux protéger la sécurité de ses propres infrastructures critiques et de celles de ses États membres face à ces nouvelles menaces cybernétiques?

Mener des études transversales, allant de la psychologie à l'ingénierie sociale et sociétale, et en particulier concernant le modus operandi des cybercriminels afin d'étudier leurs profils, leurs chemins de recrutement et de guérison, mais aussi d'identifier leurs vulnérabilités et les meilleurs moyens de les combattre.

<https://esd.cnam.fr/axes-de-recherche/axe-2-cybersecurite-cybercrime-cyberdefense-c3--1117324.kjsp?RH=15614528>