

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

### Contexte

Aux États-Unis, en mai 2018, le nouveau document cadre de la stratégie du *Homeland Security Department* indique que **d'ici 2020, plus de 20 milliards d'objets seront connectés à Internet**, un nombre qui augmente parallèlement à **l'augmentation exponentielle des menaces à la sécurité**. Il convient de rappeler ici que la **transformation numérique** ne repose pas uniquement sur des **infrastructures géantes (cloud)** [1], mais également sur les **petits objets numériques** qui accompagnent dans leur vie quotidienne la majorité des activités des employés, des collaborateurs et même des dirigeants et dirigeantes de ces secteurs et institutions.

Toutes les industries de l'agriculture, de la fabrication et des infrastructures publiques numérisent des secteurs entiers de leur activité: **leur compétitivité en dépend**. Leurs services informatiques destinés aux **opérateurs d'infrastructures vitales** (santé, hôpitaux, services publics, énergie, etc.) ainsi qu'aux **services publics et régaliens** (administrations, défense) sont ainsi de plus en plus équipés d'**outils numériques** et d'**intelligence artificielle (IA)**. Cette évolution concerne également les **armées modernes**, car l'utilisation de l'intelligence artificielle offre une possibilité supplémentaire de **déstabiliser**, de **compromettre** ou même de **détruire les infrastructures essentielles d'un pays**, y compris ses **systèmes de défense et de renseignement** [2]. Cependant, cette **numérisation accrue** crée en même temps de nouvelles vulnérabilités.

### Evolution et enjeux des cybermenaces à venir

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<sup>e</sup> siècle [3]. 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**. Deuxièmement, le cyberspace est devenu l'un des principaux **pourvoyeur 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**. Troisièmement, 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 [4]. 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<sup>[5]</sup>.

Cependant, les États doivent assumer immédiatement la responsabilité de cette rupture, cette évolution ultra rapide se déroulant dans le cyberspace, car les cyberattaques les menacent directement<sup>[6]</sup>. Il est donc notable que les **attaques ciblées** (Menaces Persistantes Avancées/ Advanced Persistent Threats) ont fortement augmentées depuis 2010: croissance annuelle de 40%, 20% des entreprises concernées signalant des **dommages financiers** (KCS-CERT 2012 et PWC 2011), dont plus de 50% des **incidents** (intrusion, détérioration, espionnage) ont concerné les **industries énergétiques** (nucléaire, pétrolière). Par exemple, le service du personnel administratif des États-Unis a été piraté en 2015 et a perdu les données confidentielles de 4 millions d'employés à travers le pays. En Allemagne, l'Agence centrale pour la cybersécurité nationale a récemment dû reconnaître que ses experts n'étaient en mesure de contenir que les attaques et les dysfonctionnements créés par les virus de nouvelle génération Spectrum et Meltdown, notamment en termes d'accès et de diffusion de données personnelles et confidentielles.<sup>[7]</sup>

Ces dangers soulèvent des questions sur la manière dont nous pouvons **mieux protéger nos infrastructures critiques, nos infrastructures publiques, nos citoyens et nos sociétés**, tout en assurant la continuité d'activité des fournisseurs de services Internet et la **stabilité des infrastructures numériques**. En effet, afin de mieux garantir la **cybersécurité de nos infrastructures publiques**, une **approche analytique systémique et transversale des nouveaux cyber-aléas** devrait également permettre de développer une meilleure connaissance des **vulnérabilités** de nos adversaires, des nôtres et des moyens de combattre-les en équipant nos systèmes de défense d'**algorithmes renforcés d'intelligence artificielle et d'innovation**. Ces recherches devraient permettre, par exemple, de comprendre les opportunités criminelles, mais aussi de lutter contre ces phénomènes créés par la sécurité accrue des paiements et des transactions électroniques (torrent, streaming illégal, contrefaçon de logiciels, vol d'accès, usurpation d'identité).

## Questions de recherche associées

Quels sont les **risques de perturbation des infrastructures critiques** générés par les **nouveaux moyens cyberoffensifs** allant de la fabrication et du déploiement d'attaques persistantes avancées (APT) aux vecteurs de compromission de l'opinion publique à l'aide d'**algorithmes** d'apprentissage?

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 para-étatiques** 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**?

---

[1] Gaycken Sandro, "[Does not not compute - old security vs new threats](#)". *Datenschutz und Datensicherheit* 36(9): 666-669 (2012)

[2] [Statement for the record: Worldwide threat assessment of the US Intelligence Community](#), Senate Armed Services Committee, 9 février 2016

[3] Nye, Joseph S., Jr. "[Nuclear Lessons for Cyber Security](#)." *Strategic Studies Quarterly*, décembre 2011. Accessed January 1, 2017.

[4] 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

[5] Baumard Ph. "The behavioral paradigm shift in fighting cybercrime: Counter- measures, innovation and regulation issues", *International Journal on Criminology*, 2(1), 2014, pp.11-22

[6] Gaycken Sandro, "[Does not not compute - old security vs new threats](#)". *Datenschutz und Datensicherheit*36(9): 666-669 (2012)

[7] Andrea Shalal (Berlin) and Stephen Nellis (San Francisco), "[Germany calls on chip and hardware makers to tackle processor flaws](#)", editing by Alexander Smith and Diane Craft, Reuters, 18 mai 2018

<https://esd.cnam.fr/projets-de-recherche-cooperation-scientifique/projets-de-recherche/projet-de-recherche-n-6-l-impac>