Ambassade de France à Washington
Service pour la Science et la Technologie
4101 Reservoir Road NW, Washington, DC 20007
Tél. : +1 202 944 6246
Mail : info@france-science.org
URL : http://france-science.org

Domaine : Nouvelles Technologies de l'Information, de la Communication et de la Sécurité
Document : Rapport d'Ambassade / Ambassade de France à Washington
Titre : Paysage gouvernemental et scientifique de la cybersécurité aux Etats-Unis
Auteur(s) : Hervé Martin (attache-ntics@ambascience-usa.org)
Clémentine Désigaud (deputy-ntics@ambascience-usa.org)
Xavier Arrom (stagiaire-envt@ambascience-usa.org)
Date : Mars 2018

Mots-clés :	Cybersécurité, sécurité, risques, vie privée, intelligence artificielle
Résumé :	La cybersécurité est un domaine d'activité complexe et pluridisciplinaire visant à empêcher l'accès inapproprié ou malveillant à des objets, systèmes ou infrastructures numériques. Il s'agit de préserver et de faire face aux attaques pouvant affecter l'écosystème numérique, devenu crucial pour le bon fonctionnement des sociétés, gouvernements et entreprises. La sécurité est l'une des priorités principales de l'administration Trump aux Etats-Unis, notamment face aux cyberattaques dont le nombre et la sophistication ont augmenté ces dernières années. Ce rapport présente donc un rapide panorama du paysage de la cybersécurité aux Etats-Unis, en se concentrant sur les initiatives gouvernementales, les grands programmes de recherche et les formations mises en œuvre par les universités américaines. Deux défis majeurs sont également rappelés en début du rapport, celui du manque d'expertise et celui du difficile équilibre entre sécurité et protection de la vie privée dans les relations entre les Etats-Unis et l'Union européenne. Le rapport se termine avec un focus sur une nouvelle orientation scientifique, l'utilisation des techniques d'intelligence artificielle en cybersécurité.

Introduction

La cybersécurité est un vaste domaine d'activité qui vise principalement à protéger tout objet, système et infrastructure numérique connectés à un réseau de tout accès malveillant ou inapproprié. La cybersécurité recouvre donc aussi bien la protection des systèmes physiques, réseaux d'ordinateurs, logiciels et données, que la sensibilisation et la formation des utilisateurs aux règles et procédures liées à l'utilisation de tels systèmes.

La révolution numérique bouleverse profondément le fonctionnement de nos sociétés que ce soit à l'échelle des individus ou de celle des organisations et des institutions. Les citoyens, les entreprises et les administrations dépendent du bon fonctionnement de l'écosystème numérique, qui recouvre aussi bien les moyens de communication, du téléphone à la messagerie électronique et aux techniques de visio-conférence, que les ordinateurs, le stockage des données, le contrôle à distance de dispositifs parfois sensibles, et les services en ligne pour les consommateurs. Garantir que cet écosystème fonctionne en continu, ne soit pas vulnérable et soit à même de faire face à des pannes matérielles ou logicielles ou à tout autre événement (virus, malware, etc.) est donc un enjeu stratégique prioritaire.

Avec l'avènement de l'Internet des objets, qui met en relation le monde physique avec la sphère virtuelle du réseau internet, la cybersécurité devient encore plus complexe, du fait de la diversité et du nombre des utilisations, mais aussi plus critique, du fait de la nature des risques. Nos moyens de transports (avions, voitures, etc.), nos dispositifs médicaux actuels, tels que les pacemakers, ou de demain, avec les lentilles de contact intelligentes et les nano-robots, sont déjà ou seront connectés. La cybersécurité doit permettre de garantir qu'un système malveillant ne puisse provoquer une catastrophe en prenant le contrôle d'un de ces objets ou d'une grande infrastructure connectée, comme une centrale hydro-électrique.

Cette note fait un point non exhaustif sur les initiatives gouvernementales et académiques aux Etats-Unis en matière de cybersécurité, une science complexe et pluridisciplinaire.

1. Définition et remarques liminaires

Les 5 dimensions de la cybersécurité

Cinq dimensions caractérisent la cybersécurité :

- Identifier les risques en termes de gouvernance et d'infrastructure matérielle ou logicielle ;
- Protéger les infrastructures, les réseaux et les données et mettre en place une cyber-hygiène pour sensibiliser les différents acteurs du système d'information ;
- Détecter les anomalies et les attaques ;
- Répondre à des attaques pour éliminer ou en diminuer les effets ;
- Rétablir le système dans un état cohérent en cas d'incident.

De nombreux défis scientifiques et technologiques sont à relever sur ces 5 aspects de la cybersécurité, un domaine qui prend une place croissante dans nos sociétés.

Un manque d'experts en cybersécurité

Au-delà des défis scientifiques et technologiques se posent également des défis humains en matière de cybersécurité, dont le principal d'entre eux est la pénurie de talents.

Le monde entier peine à recruter des experts en cybersécurité, les profils disposant des bonnes compétences restant trop rares, y compris aux Etats-Unis. Les analystes de données (*Data Scientists*) font partie des profils les plus recherchés pour s'attaquer aux défis de la cybersécurité. La demande d'ingénieurs formés en la matière dépasse cependant l'offre. Le décret présidentiel américain du 11 mai

2017 sur le renforcement de la cybersécurité des réseaux fédéraux et des infrastructures critiques[1] insiste ainsi sur le besoin de développer une main d'œuvre experte en cybersécurité.

La France possède de sérieux atouts : les étudiants français affichent un bon niveau en mathématiques et en sciences, et la France compte plus de 200 écoles d'ingénieurs formant chaque année près de 40 000 ingénieurs. L'Ecole Polytechnique, l'Ecole Normale Supérieure (ENS) et l'Université Pierre et Marie Curie (UPMC) font partie des meilleures universités au monde en mathématiques. La France compte de plus de nombreux chercheurs et ingénieurs talentueux dont l'excellence est reconnue dans le monde entier. En 2017, le Service pour la Science et la Technologie a notamment organisé un programme sur la cybersécurité à destination des doctorants américains (programme FADEx ou French-American Doctoral Exchange), venus en France pour une semaine de séminaires dans des laboratoires et centres de recherche français reconnus pour leur expertise en matière de cybersécurité (le LORIA2 en Lorraine, l'IRISA3 à Rennes et l'Inria4 à Paris).

Un difficile équilibre entre sécurité et protection de la vie privée

En matière de cybersécurité se pose la question de l'équilibre entre protection de la vie privée, notamment des données personnelles, et sécurité. Les pays européens et les Etats-Unis ne conçoivent pas nécessairement cet équilibre de la même manière. Le département du Commerce américain et la Commission européenne avaient instauré un cadre juridique, le *Safe Harbor*, afin de concilier leurs deux approches du respect de la vie privée lors du transfert de données personnelles de l''Espace économique européen (EEE) vers les Etats-Unis. Ce cadre a toutefois été invalidé par la Cour de justice de l'Union européenne (CJUE) en octobre 2015, considérant que les Etats-Unis n'offraient pas un niveau de protection adéquat. Deux nouveaux instruments ont alors été mis en place :

- Le *EU-US Privacy Shield*, adopté en juillet 2016, qui garantit notamment la protection des données des citoyens européens lorsqu'elles sont transférées aux Etats-Unis ;
- Le *EU-US Umbrella Agreement*, entré en vigueur en février 2017, qui étend aux Européens les protections déjà accordées aux Américains par le *US Privacy Act* de 1974 et leur donne accès aux courts de justice américaine.

Ces deux instruments permettent pour les Européens présents sur le sol américain ou dont les données personnelles sont transférées aux Etats-Unis de maintenir un niveau de protection équivalent à celui dont ils bénéficient sur le sol de l'Union européenne.

Sur le sol européen, la protection des données personnelles est garantie par le règlement général sur la protection des données (RGPD), adopté en avril 2016. Ce texte vise à moderniser, renforcer et unifier la protection des données personnelles au sein de l'UE et aborde également la question du transfert des données en dehors de l'UE. L'une des exigences du RGPD vise à garantir que les pays tiers recevant des données de l'UE disposent de lois adéquates en matière de protection des données. C'est en l'absence de lois adéquates aux Etats-Unis qu'a justement dû être négocié l'accord spécifique *Privacy Shield*.

Le RGPD rentrera en application en mai 2018 après une période de transition de 2 ans. Ce texte réglementaire remplacera ainsi l'ancienne *Data Protection Directive* de 1995. En France, le texte

[1] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure issued on May 11, 2017: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[2] Laboratoire Lorrain de Recherche en Informatique et ses Applications

[3] Institut de Recherche en Informatique et Systèmes Aléatoires

[4] Institut National de Recherche en Informatique et Automatique

adaptant la loi CNIL au RGPD a été adopté en première lecture par l'Assemblée nationale en février 2018.

Plusieurs points ont suscité ou suscitent encore des questions et des tensions entre l'Union européenne et les Etats-Unis :

- Même si la Commission européenne a estimé que les dispositions du *Privacy Shield* garantissaient un niveau de protection des données équivalent à celui appliqué dans l'UE, certains ont toutefois émis des réserves au motif que la surveillance en masse des donnés par les agences de renseignement américaines resterait possible dans le cadre du *Privacy Shield*. Le Contrôleur européen de la protection des données a notamment jugé que le *Privacy Shield* ne serait pas assez robuste pour résister à un nouvel examen de la CJUE.
- Le décret présidentiel américain du 26 janvier 2017[5], axé sur l'immigration illégale, demande aux agences de renseignement américaines de ne pas étendre les mesures de protection de la vie privée aux non-résidents et non-citoyens américains. Si ce décret semble donc aller à l'encontre de ce qui a été négocié dans le cadre du *EU-US Umbrella Agreement*, il a toutefois été considéré que la mention « dans le respect des lois en vigueur » présente dans le décret épargnait les européens.
- Enfin, concernant l'entrée en vigueur du RGPD, les autorités européennes de protection des données ont publié leurs recommandations sur les transferts internationaux de données, notamment des règles d'entreprise contraignantes ou « *binding corporate rules* ». Les Etats-Unis expriment leurs craintes face à ces dispositions qui, si elles seront bénéfiques pour les consommateurs et dans la lutte contre les cybermenaces, pourront avoir un fort impact sur les pratiques des entreprises américaines qui doivent s'y conformer.

2. Initiatives gouvernementales aux Etats-Unis

Les priorités des Etats-Unis en matière de cybersécurité

Le décret présidentiel du 11 mai 2017 sur le renforcement de la cybersécurité des réseaux fédéraux et des infrastructures critiques[6] a pour but de moderniser les capacités en cybersécurité des Etats-Unis et d'encourager les différents départements à s'adapter aux nouveaux enjeux sécuritaires. Ce décret énonce plusieurs éléments clés :

- La responsabilité des risques de cybersécurité incombe aux agences fédérales, qui doivent se conformer aux normes établies par le *National Institute for Standards and Technology* (NIST) pour évaluer les risques. Le décret demandait aux agences de remettre dans un délai de 90 jours un rapport portant notamment sur les risques identifiés, la stratégie de l'agence et son plan d'actions pour assurer la conformité avec le *framework* du NIST.
- Le gouvernement porte une attention particulière sur les risques associés aux infrastructures critiques, et notamment les risques liés aux *botnets* (réseaux de bots informatiques, des programmes informatiques communiquant entre eux pour exécuter des attaques distribuées et automatisées) et les conséquences de coupures électriques prolongées sur ces infrastructures critiques.

[5] Executive Order: Enhancing Public Safety in the Interior of the United States, issued on January 25, 2017 https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/

[6] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure issued on May 11, 2017: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

- La responsabilité de la cybersécurité sur les systèmes touchant à la sécurité nationale (renseignements, chiffrement, forces armées, armement, etc.) se fera en collaboration avec le Département de la Défense, un rapprochement qui avait été refusé par le Président Obama par crainte d'une surveillance accrue et d'une militarisation du net.
- La dimension internationale de la cybersécurité est abordée au travers de l'identification des menaces, de leur provenance et des collaborations envisageables notamment en terme de partage d'informations.
- Le décret insiste sur l'importance de la formation des acteurs et des futurs spécialistes de la cybersécurité ainsi que sur la veille à effectuer sur les efforts liés à la cybersécurité entrepris par les grands acteurs à l'international.

La sécurité fait partie des cinq priorités en recherche et développement de l'administration Trump, dévoilées dans un mémo du 17 août 2017[7]. Ce mémo évoque la nécessité pour le gouvernement fédéral de développer les technologies nécessaires pour renforcer la sécurité et la résilience des infrastructures critiques des Etats-Unis, face aux menaces physiques et aux cyber-menaces dont le nombre et la sophistication ont augmenté ces dernières années. Le mémo invite à prêter une attention particulière aux activités de recherche et de développement qui contribuent à l'intégration fiable et sûre des nouvelles technologies dans la société (on pense évidemment à la technologie blockchain qui présente quelques atouts pour faire face à certains cyber-risques).

Sous l'administration Obama, un décret présidentiel du 12 février 2013 portait également sur l'amélioration des infrastructures critiques de cybersécurité[8]. Il soulignait notamment les grands principes de la politique de cybersécurité des Etats-Unis : *"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."*

Standardisation des pratiques de cybersécurité

Le *NIST Cybersecurity Framework* (NIST CSF) est un cadre formalisant de grands principes en matière de sécurité numérique. Originellement publié en 2014, une nouvelle version du CSF (version 1.1) a été soumise aux commentaires du public en 2017. Ce *framework* adopte une approche pragmatique : il propose un ensemble de standards, de procédures et une méthodologie, qui en font un guide des bonnes pratiques à adopter en matière de cybersécurité. Les mesures et contrôles qu'il inclut permettent d'aider les opérateurs en charge d'infrastructures de données à identifier, évaluer et gérer les risques liés à la cybersécurité. Ce *framework* permet notamment aux entreprises d'évaluer et d'améliorer leur capacité à prévenir, détecter et répondre à des cyberattaques. L'adoption de ce *framework* se généralise et le NIST a pour objectif qu'il soit adopté par 50% des entreprises à l'horizon 2020.

Le NIST vient également de publier son rapport final sur la standardisation de l'Internet des objets en matière de cybersécurité. Ce rapport fait suite à l'établissement d'un groupe de travail spécialisé en 2015, le *Interagency International Cybersecurity Standardization Working Group*, afin de renforcer la

[7] Memorandum for the Heads of Executive Departments and Agencies on Administration Research and Development Budget Priorities, August 17, 2017:
https://www.whitehouse.gov/sites/whitehouse.gov/files/ostp/fy2019-administration-research-development-budget-priorities.pdf

[8] Executive Order -- Improving Critical Infrastructure Cybersecurity, February 12, 2013:
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

participation des agences fédérales américaines dans la définition de standards de cybersécurité au niveau international. Ce rapport a pour but d'informer et de guider les décideurs politiques et les autres acteurs qui cherchent à développer et utiliser des standards de cybersécurité pour les composants, systèmes et services de l'Internet des objets.

Les programmes mis en œuvre par les différents Départements ministériels

Le Département de la Défense (DoD) est particulièrement concerné par les problématiques de cybersécurité du fait de l'importance stratégique et de la taille de son réseau informatique. Les principales mesures prises par le DoD sont les suivantes :

- Développement d'une architecture réseau commune à l'ensemble du département, pour passer d'une politique de protection service par service à une protection globale ;
- Identification, évaluation et protection des systèmes clés, vitaux aux missions principales ;
- Développement de la coopération entre agences et entre pays afin d'anticiper les menaces et d'accélérer les réponses ;
- Evaluation et développement de la dissuasion, afin de diminuer en amont le nombre de menaces.

En parallèle, le DoD encourage et forme à la cyber-hygiène afin d'améliorer les pratiques des utilisateurs de systèmes informatiques. Pour accompagner cette évolution, 133 équipes devraient être opérationnelles en septembre 2018.

Le Département de l'Energie (DoE) vise la sécurisation du réseau énergétique d'ici à 2020. L'action du DoE se fait en collaboration étroite avec de nombreux acteurs, 90% des infrastructures énergétiques étant privées. Elle s'articule autour de 3 points :

- Préparation : du fait de l'évolution rapide des menaces, leur évaluation systématique et rigoureuse est nécessaire afin de permettre une réponse rapide et efficace. En partenariat avec les acteurs privés, le Département développe des outils tels que le CRISP (*Cybersecurity Risk Information Sharing Program*), qui a pour but de faciliter et d'accélérer l'échange de données concernant les éventuelles menaces, et le C2M2 (*Capability Maturity Model*), qui facilite l'évaluation de la qualité des capacités de réponses des acteurs vis-à-vis de celles-ci.
- Coordination : développement de procédures de réponse et d'assistance, en coopération avec les autres branches du gouvernement et les partenaires privés.
- R & D : le réseau électrique est très hétérogène (vétuste en certains endroits, équipé de technologies avancées mais incompatibles en d'autres). Il est donc nécessaire de développer de nouvelles solutions d'ingénierie permettant le déploiement de solutions de cybersécurité sur l'ensemble du réseau.

Le Département de la Justice (DoJ) a créé en décembre 2014 une unité de cybersécurité. Cette unité revêt un rôle d'expert, s'assurant que les outils légaux sont utilisés au mieux afin d'identifier les attaquants, tout en préservant la vie privée des américains. Elle assiste également les acteurs privés ainsi que les particuliers en faisant la promotion des pratiques autorisées en termes de cybersécurité.

Le département de la Sécurité intérieure (*Homeland Security*) propose notamment un appui technique des différents acteurs grâce à des outils tels que l'AIS (*Automated Indicator Sharing*) qui permet une communication en temps réel des menaces. Si une menace est détectée, l'ensemble des partenaires sont informés, leur permettant ainsi de limiter rapidement leurs vulnérabilités.

3. <u>Recherche et enseignement supérieur en cybersécurité</u>

Les grands programmes de recherche de la NSF

La National Science Foundation (NSF) finance des recherches fondamentales et de nombreux projets pluridisciplinaires associant sciences sociales et technologie dans le domaine de la cybersécurité. En 2015, 257 projets impliquant 37 Etats américains ont été financés pour un total de 75,5 millions de dollars. En 2017, le programme *Cybersecurity Innovation for Cyberinfrastructure* (CICI) a reçu 8,5 millions de dollars. Ce programme se concentre sur le développement et le déploiement de technologies matérielles (*hardware*) et logicielles (*software*) capables de protéger les cyber-infrastructures de la recherche à l'heure où les chercheurs s'appuient sur une variété de technologies en réseau et d'outils logiciels (instruments scientifiques, capteurs, programmes logiciels, bases de données, systèmes de stockage, etc.). Une vingtaine d'autres programmes tels que le programme *CyberCorps(R) Scholarship for Service* (SFS), qui dispose d'une enveloppe de 25 millions de dollars pour traiter des aspects formation en cybersécurité, sont actuellement actifs à la NSF.

La structuration des grandes universités en matière de cybersécurité

Côté recherche, plusieurs grandes universités ont mis en place des centres dédiés à la cybersécurité avec une approche holistique mêlant sciences dures (mathématique, cryptographie, informatique) et sciences sociales pour aller de la cryptographie aux mécanismes liés à la vie privé et à la réglementation. On peut notamment citer :

- Le *Center for Long-Term Cybersecurity* de l'Université de Berkeley qui s'intéresse au lien homme/technologie en matière de sécurité en soutenant les collaborations entre le monde universitaire et le monde industriel ;
- Le programme *Stanford Cyber Initiative* qui a reçu une dotation de 15 millions de dollars de la Fondation Hewlett pour traiter de ces sujets ;
- Les initiatives du Massachusetts Institute of Technology (MIT) avec le groupe *Cybersecurity@CSAIL*, le *MIT Cybersecurity and Internet Policy Initiative* et le *Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity* $(IC)^3$;
- Et les nombreux centres spécifiques qui ont vu le jour dans des universités telles que Georgia Tech, l'Université du Maryland ou encore l'Université George Washington.

De plus, pour faire face à une rapide hausse de la demande, de la part des employeurs comme des étudiants, les universités s'adaptent en proposant de nouvelles offres. L'ensemble des initiatives pourrait toutefois gagner en lisibilité et en cohérence. C'est pour faciliter la lecture de ce nouveau catalogue d'offres de formations que la National Security Agency (NSA) et le Department of Homeland Security (DHS) ont créé le label *Center of Academic Excellence in Cyber Defense*, qui définit un certain nombre de cours essentiels à l'enseignement de la cybersécurité (analyse de données, cryptographie, cyberdéfense, implications légales, éthiques et politiques). Ce label facilite l'orientation des étudiants et les recrutements des entreprises. L'université Johns Hopkins propose notamment un cursus universitaire complet agréé par ce label. Georgia Tech propose également un master en cybersécurité. Des laboratoires de recherche tel que le *Security and Privacy Research Group* de Princeton sont également agréés. Certaines universités proposent toutefois des cursus en cybersécurité qui ne disposent pas du label, comme Université de Californie Berkeley.

De manière générale, le nombre de grandes universités américaines à proposer un cursus complet en cybersécurité reste encore limité. L'université Harvard et le MIT, par exemple, ne proposent que des certificats, notamment à destination des professionnels. Les grandes universités traditionnelles (MIT, Stanford, Carnegie Mellon, UC Berkeley, Harvard, Princeton) restent bien sûr toujours en tête des classements internationaux en informatique, mais en matière de cybersécurité en particulier, des universités moins connues se font remarquer pour leurs programmes et spécialisations (spécialisation en *infosecurity* à l'Université Purdue, création du *Maryland Cybersecurity Center* en

2010 à l'Université du Maryland). A noter également que beaucoup des universités moins reconnues proposent de suivre des certificats, licences et masters de cybersécurité en ligne (Utica College, Arizona State University, Maryville University, Champlain College, Syracuse University).

Les entreprises recrutent de plus en plus d'autodidactes s'étant formés seuls à la cybersécurité, notamment dans les villes qui peinent à attirer des diplômés d'universités prestigieuses face à la Silicon Valley. Cette hausse des recrutements basés sur les compétences plutôt que sur les diplômes pourrait constituer une opportunité pour les *Community Colleges* (établissements professionnels). Le 5ème *Community College Cyber Summit* (3CS) s'est déroulé ainsi en août 2018 à Portlandavec l'objectif d'aider les *Community Colleges* à développer de nouveaux cursus et à améliorer leurs pratiques pédagogiques.

4. <u>Focus sur une nouvelle orientation scientifique : cybersécurité et intelligence artificielle</u>

De nouvelles cybermenaces dues aux progrès de l'IA

Les progrès en intelligence artificielle (IA) offrent de nouveaux outils au service des cybercriminels, plus puissants et efficaces, aux conséquences potentiellement désastreuses pour les infrastructures critiques (hôpitaux, transports, réseaux de communication) et la vie publique. Plusieurs exemples d'attaques intégrant l'automatisation ont déjà fait la démonstration de leur impact.

Du côté des infrastructures critiques, la multiplication des objets connectés (*Internet of Things* – IoT) offre autant de nouveaux vecteurs d'attaques. En octobre 2016, une attaque du logiciel malveillant Mirai a paralysé une partie de l'Internet américain en visant l'infrastructure de l'entreprise Dyn, qui gère les noms de domaines (*Domain Name System* – DNS) de nombreux sites Internet notamment américains. Mirai a infecté plusieurs centaines de milliers d'appareils connectés, y compris des caméras de surveillance, formant ainsi un botnet (un réseau de bots informatiques) à l'origine de cette attaque par déni de service distribué (*Distributed Denial of Service Attack* – DDoS). A la suite de cette attaque, les autorités américaines et européennes se sont mises à rechercher des solutions rapides pour sécuriser les millions d'objets connectés.

Les attaques automatisées peuvent également cibler l'opinion publique. Les attaquants peuvent créer des bots à visée politique, qui génèrent automatiquement des messages sur les réseaux sociaux pour soutenir ou critiquer un candidat, manipulant ainsi l'opinion publique à des périodes politiques clés. Lors des débats télévisés entre les deux candidats pendant l'élection présidentielle américaine de 2016, près d'un tiers du trafic sur Twitter à ce sujet était généré par des comptes automatiques[9].

Mais aussi de nouvelles méthodes plus efficaces pour détecter et lutter contre les cybermenaces

Les méthodes d'intelligence artificielle permettent d'améliorer la détection des cyber-menaces. Les applications de sécurité intègrent de plus en plus l'intelligence artificielle afin de faciliter la détection des menaces et des anomalies. Pour détecter et stopper à temps des cyberattaques, les technologies de type *machine learning* sont capables de collecter et d'analyser de larges volumes de données complexes en très peu de temps, reconnaissant ainsi le moindre changement dans leur environnement. Les algorithmes de *machine learning* sont particulièrement efficaces lorsqu'il s'agit de créer des profils de comportement dits « normaux », et peuvent ainsi distinguer des comportements normaux et anormaux en temps réel. Cela est particulièrement pertinent lorsqu'il s'agit de reconnaître des attaques basées sur un modèle similaire à des attaques passées.

[9] Bots and Automation over Twitter during the Third Presidential Debate, The Computational Propaganda Project, University of Oxford, October 31st, 2016: http://comprop.oii.ox.ac.uk/research/working-papers/bots-and-automation-over-twitter-during-the-third-u-s-presidential-debate/

Néanmoins, les machines se montrent moins efficaces lorsqu'il s'agit de reconnaitre de nouvelles formes d'attaques. L'expertise humaine reste donc cruciale, et ce à plusieurs à niveaux. Les Humains restent plus efficaces que les logiciels lorsqu'il s'agit de mettre en place des stratégies, de négocier et de dialoguer avec d'autres Humains. La technologie a ses limites (taux d'erreur, faux positifs, difficulté à identifier des attaques innovantes) que l'Humain peut aider à corriger et à compléter. Les Humains sont capables de réfléchir plus stratégiquement et d'identifier des attaques sophistiquées, quand des machines pourraient être induites en erreur si les criminels développent des méthodes d'*adversarial machine learning*. La perception et la capacité à contextualiser humaine restent enfin essentielles lorsqu'il s'agit de déterminer le niveau de la menace détectée par la machine et la meilleure façon d'y répondre, notamment lorsque la réponse peut avoir des conséquences sérieuses.

L'IA pour déjouer des attaques physiques organisées en ligne

Au-delà d'une aide à la prévision des cyberattaques, l'intelligence artificielle peut permettre de déjouer les attaques qui se déroulent dans le monde physique mais ont été préparées en ligne. La plupart des groupes utilisent en effet Internet pour planifier des attaques physiques, communiquer, diffuser de la propagande, recruter et former leurs membres et réunir de l'argent. Les progrès en matière de *machine learning* et d'intelligence artificielle peuvent jouer un rôle : la fouille de données (*data mining*) et l'analyse de données sont des outils puissants pour les agences de renseignement qui combattent le terrorisme.