Hacktiviste,
je t'aime moi non plus

GÉNÉRAL D'ARMÉE (2S)
MARC WATIN-AUGOUARD
Fondateur du Forum InCyber

ADÈLE FORVEILLE
Rédactrice en chef InCyber News

SEPTEMBRE 2024

agora
INCYBER FORUM

INTRO-DUCTION

Le titre résume à lui seul l'hétérogénéité du champ de l'hacktivisme, non seulement en raison de la diversité des moyens employés, mais surtout au regard des finalités poursuivies.

Il souligne le caractère subjectif de toute approche du sujet, chacun étant tenté de choisir entre le « bon et le méchant », selon le prisme des ses convictions, de sa situation dans l'environnement géopolitique. L'hacktivisme ne se résume pas au bipôle « cybercriminel ou héros » : des cyber-citoyens sont également actifs. Le droit actuel, concentré sur les faits et parfois les effets, ne prend pas en compte le mobile du *hacker*, qu'il soit éthique ou non. Les négociations dans le cadre de l'ONU, si elles aboutissent, pourraient introduire des nuances sur la base de la gravité des faits et de l'objectif poursuivi. Limiter l'hacktivisme aux atteintes aux systèmes de traitement automatisé de données est réducteur, compte tenu de la multiplication des attaques dans la couche cognitive d'Internet. La « guerre de l'information » constitue désormais un terrain d'action d'autant plus dangereux qu'elle menace nos démocraties et peut devenir une arme en cas de conflit.

Organisé par le Forum InCyber le 26 juin 2024 au Quartier des Célestins, à Paris, un petit déjeuner a rassemblé des experts pour mieux caractériser l'hacktivisme. Cette note, publiée dans le cadre de l'Agora, *think tank* du Forum, retrace les grandes lignes des interventions de :

Karine BANNELIER, directrice du Cyber Security Institute de Grenoble

Damien BANCAL, spécialiste de la lutte contre le cybercrime

Thierry BERTHIER, pilote du groupe « IA, sécurité, robotique » du Hub France IA

Yassir KAZAR, CEO et cofondateur de Yogosha

SOMMAIRE

HACKTIVISTE, JE T'AIME MOI NON PLUS

L'hacktivisme, de quoi s'agit-il ?

Ceux qui espèrent une définition lapidaire seront déçus. Si l'on prend le terme dans son acception la plus banale, l'hacktivisme est, selon **Yassir Kazar,** l'utilisation des techniques informatiques ou du *hacking* à des fins politiques.

Le groupe *Cult of the Dead Cow*, créé en 1984 à Lubbock (Texas), est, dans un échange de mails, à l'origine du terme, contraction de *hacker* et d'activisme. Mais le vocable cache une très grande diversité d'acteurs, dont certains poursuivent des objectifs politiques, voire militaires. On pense à Jester qui défend les intérêts américains, à l'Armée électronique syrienne *(Syrian Electronic Army)*, mobilisée pour défendre Bachar al-Assad. Il en est de même de la *Jewish Internet Defense Force* (JIDF) en Israël, de la *Cyber Army of Russian Reborn* (CARR) qui serait responsable de nombreuses cyberattaques visant les infrastructures européennes.

Thierry Berthier évoque, à propos de l'hacktivisme politique, les actions menées en Afrique, notamment au Burkina Faso, au Mali et au Niger. Ce sont des opérations extrêmement structurées, rationnelles, industrialisées, pensées, qui ont recours à tous les procédés, mêlant sciences cognitives, informatique, *data sciences* et, désormais, intelligence artificielle. Derrière ces opérations se profile une véritable organisation d'entreprise avec des consultants, des spécialistes du marketing, des ingénieurs, etc. Mettre en place une telle opération exige un important investissement financier ; il faut donc des résultats. Cet hacktivisme spécifique, par filière, a été théorisé par la Russie, mais celle-ci n'est pas la seule. La Turquie a, elle aussi, compris le bénéfice de telles opérations et a développé ce que l'on pourrait qualifier de « *soft* hacktivisme » autour de sa diplomatie technologique, en particulier en matière de drones. Les enjeux sont à la fois financiers et géopolitiques. Un cas d'hacktivisme, qui peut sembler anodin ou sans impact, cache parfois un montage complexe.

Des groupes manipulés développent un véritable marketing de malveillance

Damien Bancal

Damien Bancal constate à l'appui le glissement de certains groupes qui, à l'origine, sont des membres actifs des *blackmarkets* et qui, de fil en aiguille, glissent vers les cyberattaques. C'est le cas notamment de *Killnet*, groupe de pirates russes qui ont décidé de soutenir la politique de la guerre en Ukraine. Le fondateur, Killmik[1], aujourd'hui sous surveillance de la Russie, tenait des boutiques où se vendaient des données piratées et des stupéfiants. Ces groupes, clairement manipulés, développent un véritable marketing de malveillance. Tandis qu'ils cherchent à faire un maximum de bruit dans le cadre de leurs opérations, ils continuent d'animer des cyberboutiques qui vendent des outils d'attaque par déni de service (DDoS). Cette communication et la visibilité de leurs opérations permettent d'attirer à eux de nouveaux clients. Tout en poursuivant ses attaques en rançongiciel, *Lockbit* apparaît ainsi de plus en plus endoctriné politiquement.

1 Citoyen russe, de son vrai nom Nikolai Nikolaevich Serafimov ?

L'hacktivisme ne doit cependant pas être perçu uniquement sous l'angle de la cybercriminalité, souligne **Yassir Kazar**. Cela ne doit pas occulter le hacking dit « éthique » et mettre en danger des personnes qui font un travail utile. Certains hacktivistes s'inscrivent en effet dans une approche citoyenne, à l'opposé des groupes précédemment évoqués.

Karine Bannelier rejoint **Yassir Kazar** en soulignant aussi le rôle du « cyber-citoyen », celui qui veut aider. Être « cyber-citoyen, dit-elle, c'est vouloir apporter quelque chose de positif, vis-à-vis de leur pays, de leur famille, ne serait-ce qu'en expliquant à ses proches comment se protéger. Plus professionnels, les *hackers* éthiques qui agissent dans le cadre d'un *Bug Bounty* participent de cette démarche.

Il ne faut pas confondre hacktivisme et activisme numérique

Yassir Kazar

Le spectre de l'hacktivisme est donc très large, complète **Yassir Kazar**, puisqu'il inclut aussi des acteurs qualifiés de cyber-terroristes (comme Cybercalifat, branche cyber de l'État islamique). Il faut donc éviter de confondre hacktivisme et activisme numérique. Dans un article intitulé *« From Clicktivism to Activism: understanding digital activism »*[2], Jordana G. George et Dorothy E. Leidner dessinent ainsi les contours de ce que l'on peut appeler aujourd'hui la mobilisation digitale. Elles ont identifié dix activités d'hacktivisme numérique représentatives : le clicktivisme, le *metavoicing*[3], l'affirmation des opinions en ligne, le financement électronique *(e-funding)*, le consumérisme politique (appel au boycott), les pétitions numériques, le « botivisme[4] », l'activisme des données, la révélation au public d'informations cachées et l'hacktivisme. À la clé : une sorte de pyramide de Maslow[5] avec trois étages, selon le schéma de Milbrath (1965), qui divise l'action sociale en activités de spectateurs, de transition et de gladiateurs. Le premier étage, les spectateurs digitaux, « likent », plussoient, upvotent, retweetent, sans aller au-delà. Le deuxième étage est celui des activistes en transition. Leur niveau d'engagement est plus élevé. Ils vont commencer à créer eux-mêmes du contenu avec des finalités politiques ou pratiquer du « botivisme », c'est-à-dire créer des mini-*bots*. Cet étage comprend aussi les pétitions en ligne, le *e-funding* avec des cagnottes, finançant des initiatives politiques. Le dernier étage est celui des gladiateurs, avec un premier niveau constitué par les hacktivistes qui pratiquent les attaques DDoS, l''intrusion à des finalités politiques, le défacement de sites web, etc. Le niveau suivant a pour objectif l'exposition, c'est-à-dire la fuite de documents sensibles, à l'instar de Wikileaks. Dernier niveau : l'Open Gov, considéré comme le stade de mobilisation ultime. Durant le Printemps arabe, un groupe d'activistes numériques s'est ainsi mobilisé et a initié une démarche d'open gov et de vigilance, sur le modèle de *« Where does my money go? »*, un moteur qui permet à chaque citoyen de suivre les finances publiques d'un État : où l'argent public a-t-il été utilisé, comment a-t-il été utilisé, avec quelle finalité ?

2 Du clicktivisme à l'hacktivisme : Comprendre l'activisme numérique, ScienceDirect

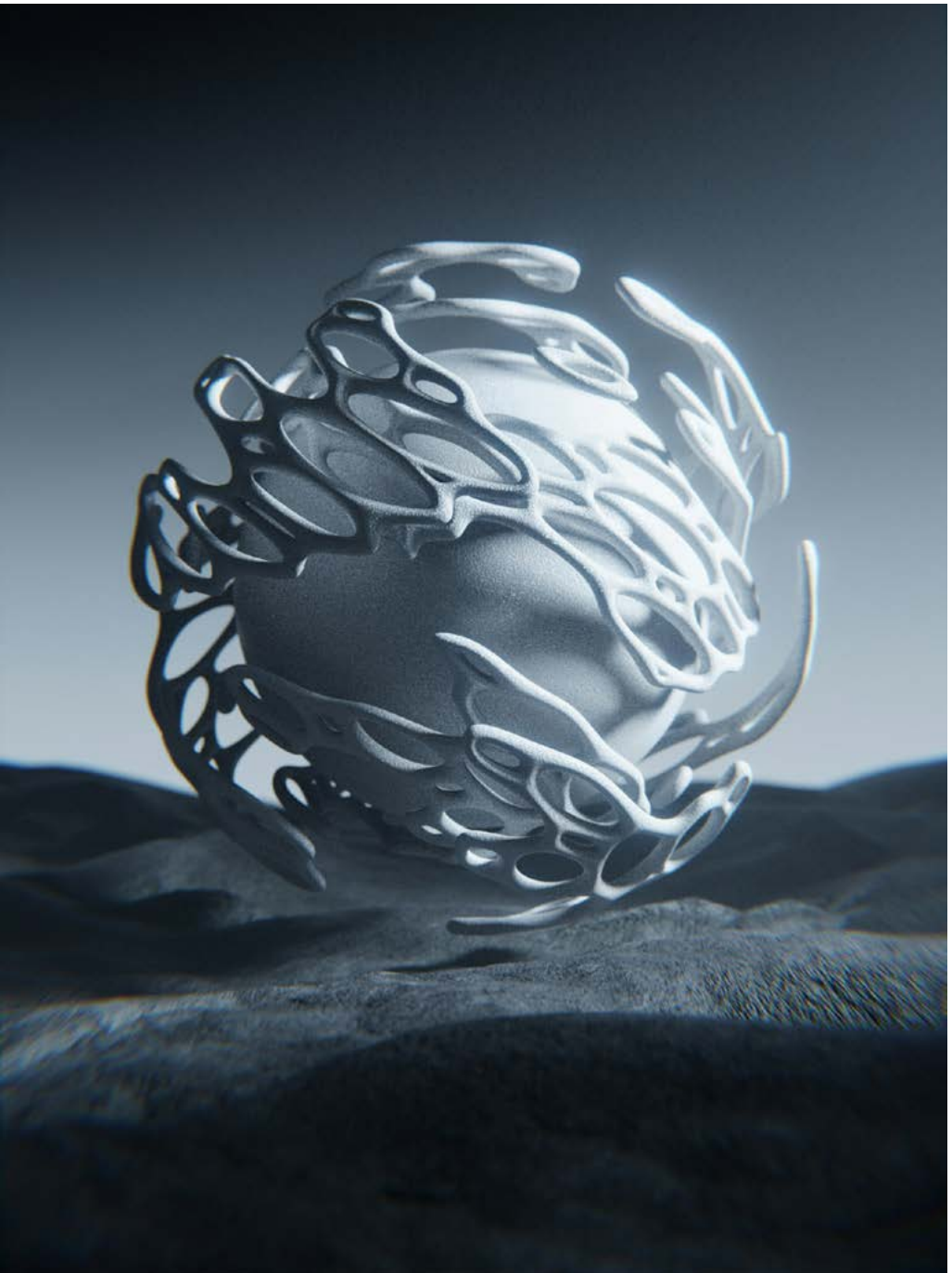
3 *Metavoicing* : expression d'opinions ou de critiques sur des plateformes en ligne, telles que les commentaires sur les articles de blog ou les forums. Cela permet aux individus de participer au débat public sans nécessairement s'engager dans des actions concrètes.

4 L'utilisation de *bots* (programmes informatiques automatisés) pour soutenir une cause en ligne. Les *bots* peuvent être utilisés pour diffuser des informations, partager des messages ou même mener des actions de protestation.

5 La pyramide de Maslow est une représentation pyramidale de la hiérarchie des besoins qui interprète la théorie de Maslow, *A Theory of Human Motivation,* 1943.

Thierry Berthier confirme l'extrême relativisme de la notion dhacktivisme en citant l'exemple d'un hacktivisme à l'échelle ultra-locale avec ses propres dynamiques. Le Limousin, dit-il, se situe dans la « diagonale du vide » et il y a encore une zone encore plus ancrée dans la « diagonale du vide », dans la Creuse, où se manifeste de l'hacktivisme. Ce sont notamment deux villages qui se sont « radicalisés », au point de mener de véritables opérations, à la fois sur Internet, mais aussi sur le plan matériel, comme sur le plateau des Millevaches, où ils donnent beaucoup de fil à retordre aux forces de police locales. Ces hackivistes anti-numérique vont jusqu'à brûler des antennes de télévision, en pensant que c'est de la 5G, tout en menant en parallèle des opérations d'activisme numérique sur les réseaux sociaux, par le biais de sites internet qui sont référencés.

L'hacktivisme n'est donc pas un phénomène monolithique. Les faits, comme les objectifs poursuivis peuvent être illégaux, comme ils peuvent être respectueux du droit.



L'hacktivisme à **l'épreuve du droit**

La loi Godfrain, quoique déjà ancienne (1988), garde toute son actualité. Elle a incriminé la pénétration et le maintien frauduleux dans un système de traitement automatisé de données, l'entrave ou l'altération de son fonctionnement, la suppression, la modification, l'introduction ou l'extraction de données. L'atteinte à la volonté du maître du système est le dénominateur commun. La loi, au fil de ses modifications, a aggravé l'action en bande organisée ou l'atteinte à un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat. Plus récemment (2023), elle a pris en compte l'effet de la cyberattaque en portant à la frontière du crime une infraction ayant pour effet d'exposer autrui à un risque immédiat de mort ou de blessures, de nature à entraîner une mutilation ou une infirmité permanente, ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes. La loi est donc neutre au regard du mobile, c'est-à-dire de l'intention coupable. Seul l'article relatif au terrorisme évoque les infractions à la loi Godfrain commises dans le but de troubler gravement l'ordre public par l'intimidation ou la terreur. Idem pour celui sur le sabotage qui a pour but de porter atteinte aux intérêts fondamentaux de la Nation.

La loi ne prend donc pas en compte l'objectif recherché par les hacktivistes, sans doute parce que le législateur veut éviter une approche subjective qui peut susciter des interprétations politiques, là où le droit doit demeurer neutre.

Vouloir appliquer la loi Godfrain à l'ensemble du spectre du hacktivisme serait ainsi réducteur, tant la diversité des comportements est évidente. Le droit doit dessiner des cadres qui permettent de réguler l'hacktivisme. Parfois, il régule une « zone grise ». Ainsi, la loi pour une République numérique, dite loi Lemaire, a introduit en 2016 une disposition dans le code de la défense qui prévoit que « Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données ». Si l'article 40 est évoqué, c'est bien parce qu'une infraction est supposée avoir été commise. C'est une forme de repentir qui est instaurée.

La frontière entre « le bon et le méchant » est difficile à établir. Ces actions se déroulent la plupart du temps sur plusieurs pays. Il faut donc pouvoir agir à l'échelle internationale sous peine d'être décalé.

Karine Bannelier

La frontière entre « le bon et le méchant » est difficile à établir, constate **Karine Bannelier**. D'autant que ces actions se déroulent la plupart du temps sur plusieurs pays. Il faut donc pouvoir agir à l'échelle internationale sous peine d'être décalé.

Participant aux négociations relatives à une Convention de l'ONU sur la cybercriminalité[6], **Karine Bannelier** est une observatrice directe des accords et des tensions qui se manifestent, à Vienne ou à New York, lors des sessions.

Comme à Dubaï, en 2012, lors du sommet de l'Union internationale des télécommunications, le monde est clivé entre ceux qui parlent de « gouvernance de l'internet » et ceux qui veulent imposer une « gouvernance sur l'internet ». La lutte anti-cybercriminalité apparaît, elle, plus consensuelle. En 2001, a été adoptée la Convention du Conseil de l'Europe sur la cybercriminalité[7]. Soixante-huit États l'ont ratifiée, mais, si l'on compte ceux qui l'ont intégré dans la leur législation par « copier-coller » ou qui l'appliquent sans pour autant ratifier le texte, ce sont aujourd'hui plus de cent cinquante États qui l'appliquent ou s'en inspirent. Comme on s'en doute, ni les Iraniens, ni les Chinois, ni les Cubains, ni les Coréens du Nord et les Russes ne la reconnaissent. La Russie a d'ailleurs proposé un traité à l'ONU dans le but de lui nuire. La Convention de Budapest, rappelle **Karine Bannelier**, criminalise des actes de *hacking* dont pourraient relever des actions menées par des hacktivistes : l'interception illégale de données, l'accès illégal à des systèmes, l'atteinte à l'intégrité de systèmes, l'atteinte à l'intégrité de données, mais elle ne s'est jamais intéressée aux motivations fondamentales, au but poursuivi.

C'est là toute la difficulté des négociations en cours au sein de l'ONU. Alors que le projet de convention de l'ONU sur la cybercriminalité reprend les incriminations de la Convention de Budapest, presque mot pour mot, les ONG, un certain nombre de membres d'organisations de protection relative au droit humain, à la liberté d'expression se sont interrogés sur la question de savoir comment faire la part des choses entre des cybercriminels et des hacktivistes qui souhaitent « juste » promouvoir leurs idées. Sur la question de l'intention, l'idée serait de placer un curseur sur l'intention criminelle et de laisser aux États membres, aux États parties à cette convention, une marge d'appréciation relative. Le deuxième point porte sur le dommage. Ce dommage est-il suffisamment sérieux ? C'est un point qui a été largement souligné dans les négociations aux Nations Unies : l'atteinte, tout comme le dommage, doivent être sérieux. Ce point transparaît déjà dans certaines législations nationales. Le Royaume-Uni et les États-Unis s'intéressent aussi à cette question. Lors du déclenchement des poursuites, le test du caractère sérieux du dommage, le caractère et l'intention criminelle sont pris en compte. Certaines décisions, certains arrêts, prennent ces critères en compte : en 2001, après une attaque par déni de service (DDoS) contre le site de Lufthansa par des hacktivistes des associations

6 L'Assemblée générale de l'ONU a adopté le mercredi 26 mai 2021 par consensus une résolution proposée par la Russie visant à aboutir à un traité contre la cybercriminalité.

7 La Convention de Budapest a été modifiée par deux protocoles additionnels : Protocole relatif à l'incrimination d'actes de nature raciste et xénophobe par système informatique (28/01/2003) ; 2e protocole additionnel (17/11/2021) accélérant la coopération dans le cadre des enquêtes. La Convention réunit les États de l'Union européenne, les États-Unis, le Canada, le Japon, mais aussi des États d'Afrique, d'Amérique du Sud.

Libertad et *Kein Mensch ist illegal* qui protestaient contre l'utilisation des avions de la compagnie aérienne pour refouler des sans-papiers, un juge allemand a, par exemple, estimé que cette attaque avait été relativement brève, avec un trouble relativement mineur porté à l'activité de Lufthansa. Il n'a donc pas souhaité condamner ces hacktivistes.

Au plan juridique, la situation est aujourd'hui bloquée par la volonté de la Russie et de la Chine de criminaliser les contenus. La Chine a ainsi fait une proposition d'article visant à incriminer l'extrémisme, la déstabilisation visant la sécurité des États. L'hacktivisme est donc clairement désigné. Même si une majorité d'États s'y oppose pour le moment, le danger est là, car ce sont bien sûr les oppositions politiques qui sont visées sous couvert de sécurité nationale. Comme le rappelle **Yassir Kazar**, en Chine, seul est toléré l'hacktivisme national, mené par des personnes qui sont là pour soutenir l'État chinois. Dès que l'on est opposant, on est « cybercriminel ». D'où l'importance de veiller à ce qu'aucun instrument international ne puisse donner des arguments à certains régimes autoritaires pour mieux réprimer.

L'hacktivisme dans la **couche cognitive d'internet**

Alors que la couche « physique » d'internet était privilégiée par les hacktivistes jusqu'au début des années 2000, le développement du web, des réseaux sociaux, devenus des vecteurs d'information, a créé une nouvelle cible et un nouveau mode d'action pour les hacktivistes : la couche « cognitive » et les manipulations de l'information. Un risque encore accru avec le développement récent des intelligences artificielles dites « génératives »... Lorsque les technologies sont disponibles, elles sont utilisées. Pour le bien, mais aussi pour le pire. « Ne sous-estimons jamais la capacité de l'attaquant à les adopter de manière ultra-rapide », souligne **Thierry Berthier**.

Le *Time to Market* des nouvelles technologies est de plus en plus court, tant du côté de l'attaquant que du côté des défenseurs. Mais dans cette course à l'adoption, l'attaquant est souvent plus rapide : il est déjà en train d'utiliser et d'industrialiser son attaque grâce à ces techniques, alors que l'État ou l'organisation qui doit s'en défendre se pose encore la question de son utilité.

Une analyse partagée par le général Perrot, conseiller IA du COMCYBER-MI, qui estime que ce décalage relève de la naïveté : « naïveté des experts qui pensent être compris, naïveté des parlementaires qui pensent que ce sont des fantasmes et enfin naïveté des citoyens qui pensent que les forces de sécurité ont beaucoup de pouvoir.

On a, dit-il, inversé le système de confiance. On a une défiance envers les forces de sécurité intérieures au lieu de leur faire confiance ».

Le *Time to Market* des nouvelles technologies est de plus en plus court, tant du côté de l'attaquant que du côté des défenseurs.

Thierry Berthier

Le développement des architectures de données fictives immersives (ADFI[8]) augmente encore la confusion, constate **Thierry Berthier**. Ces architectures permettent en effet de créer des espaces cognitifs visant un objectif donné et de les animer dans la durée. Ils seront d'autant plus cohérents qu'ils seront dépourvus de contradiction. Ceux qui seront confrontés à ces architectures auront donc bien du mal à distinguer la réalité ou d'une « vérité alternative ».

Tout étant affaire de subtilité, ces contenus ne seront pas faux ou vrais. Ils mélangeront les deux, selon des proportions variables. Un contenu peut ainsi être vrai à 60 % et profiter des 40 % restants pour faire passer un message. Parfois même, la proportion est de 90 / 10, ces 10 % permettant de « charger la mule » et de faire passer des messages qui relèvent de l'hacktivisme.

Les hacktivistes ont maintenant à leur portée la plupart des technologies nécessaires. Ils peuvent entraîner un modèle et réaliser à peu près toutes les manipulations par l'image de façon quasi indétectable. Alors qu'ils pouvaient déjà créer de faux émetteurs grâce à des « *bots* » un peu grossiers, ils peuvent maintenant créer et gérer des profils plus vrais que nature qui passent allègrement le test de Turing, là où plus de 50 % des gens étaient jusqu'à présent capable de distinguer un robot d'un humain, lors d'une conversation en ligne.

Un bon modèle conversationnel comme ChatGPT 4, que l'on entraîne en lui annonçant qu'il va être interrogé par une assemblée qui cherche à le découvrir, saura ainsi s'adapter aux questions, ne pas se montrer trop savant. Il va savoir se camoufler, ressembler à l'humain, au point de nous tromper.

Dans cette guerre de l'information qui va se durcir, les démocraties sont prises au piège posé par les régimes autoritaires, constate **Karine Bannelier.** En proposant à l'ONU de créer l'infraction de *« harmful information »* (information nocive), la Chine a beau jeu de souligner le lien entre démocratie et information. Pourquoi ne ferait-on donc pas à l'échelle internationale ce que l'Europe cherche à faire en son sein ? La guerre de l'information devient donc une véritable guerre cognitive qui vise à saper les fondements de la démocratie. Objectif poursuivi : ruiner la confiance des populations vis-à-vis de leurs institutions mais aussi celles des citoyens entre eux. Quand on cible des entreprises, c'est aussi la confiance des citoyens qui est mise à mal. In fine, c'est aussi l'effritement de la confiance du citoyen à l'égard de lui-même. Lorsqu'on atteint ce niveau de déstabilisation, ce sont les fondamentaux de la société qui sont détruits. Or c'est le but recherché par certains hacktivistes liés à la Russie et à la Chine.

Dans ses manifestations les plus pernicieuses, l'hacktivisme s'inscrit ainsi dans un cadre géopolitique qui révèle l'opposition entre les blocs et la fragilité des démocraties face aux idéologies totalitaires. Il connaît des développements paroxystiques en période de conflit armé. La guerre en Ukraine en offre une triste démonstration.

8 Les architectures de données fictives immersives (ADFI) sont des systèmes conceptuels permettant de gérer et de représenter des données de manière à créer des environnements virtuels augmentés où les utilisateurs peuvent interagir de manière immersive. Les technologies utilisées sont multiples : réalité virtuelle et augmentée, 3D, interfaces naturelles, retour haptique, simulation…

L'hacktivisme, **arme de guerre**

L'Ukraine est effectivement un terrain de jeu pour toutes les formes d'hacktivisme, d'origine étatique pour l'essentiel. Dès les premiers jours de l'invasion, Mikhailo Fedorov, ministre de la Transformation numérique ukrainien, a mobilisé des hacktivistes au sein de l'*IT Army of Ukraine.* Une mobilisation de même nature a été observée du côté Russe. Des ressortissants de pays tiers se sont également impliqués.

Pourtant, s'agissant de pays non-belligérants, le droit rappelle qu'en dehors de tout conflit armé, une cyberattaque est une infraction, quel que soit le bien-fondé de sa motivation. La France n'étant pas en guerre contre la Russie, les ressortissants français commettant des actions de piratage en soutien à l'Ukraine tomberaient ainsi sous le coup de la loi Godfrain. Dès les premiers jours, des mises en garde ont été diffusées, au nom du principe de *« diligence due »* qui impose à un État d'empêcher la commission d'actes hostiles depuis son territoire.

Point caractéristique de cet affrontement : l'intensité des actions des deux côtés et la proximité de leurs auteurs, relève **Thierry Berthier.**

Aujourd'hui, l'affrontement est cinétique. La guerre, c'est du cinétique. Ce sont des drones, c'est de l'artillerie, c'est du sang et des larmes, des ruines. Quand il y a du cyber sur le front, c'est essentiellement pour essayer de rentrer, de pénétrer les systèmes C2, de prendre le contrôle des systèmes de commandement de l'ennemi.

Thierry Berthier

Ceux-ci partagent la même culture, ont parfois été membres des mêmes groupes cybercriminels, ont été alliés ou associés. À l'instar du groupe Conti, spécialisé dans le rançongiciel, qui s'est séparé au début des hostilités. Les pirates des deux côtés ont ainsi la même façon de travailler et de procéder, avec un bon niveau technique, et ils sont capables de monter des opérations rapidement.

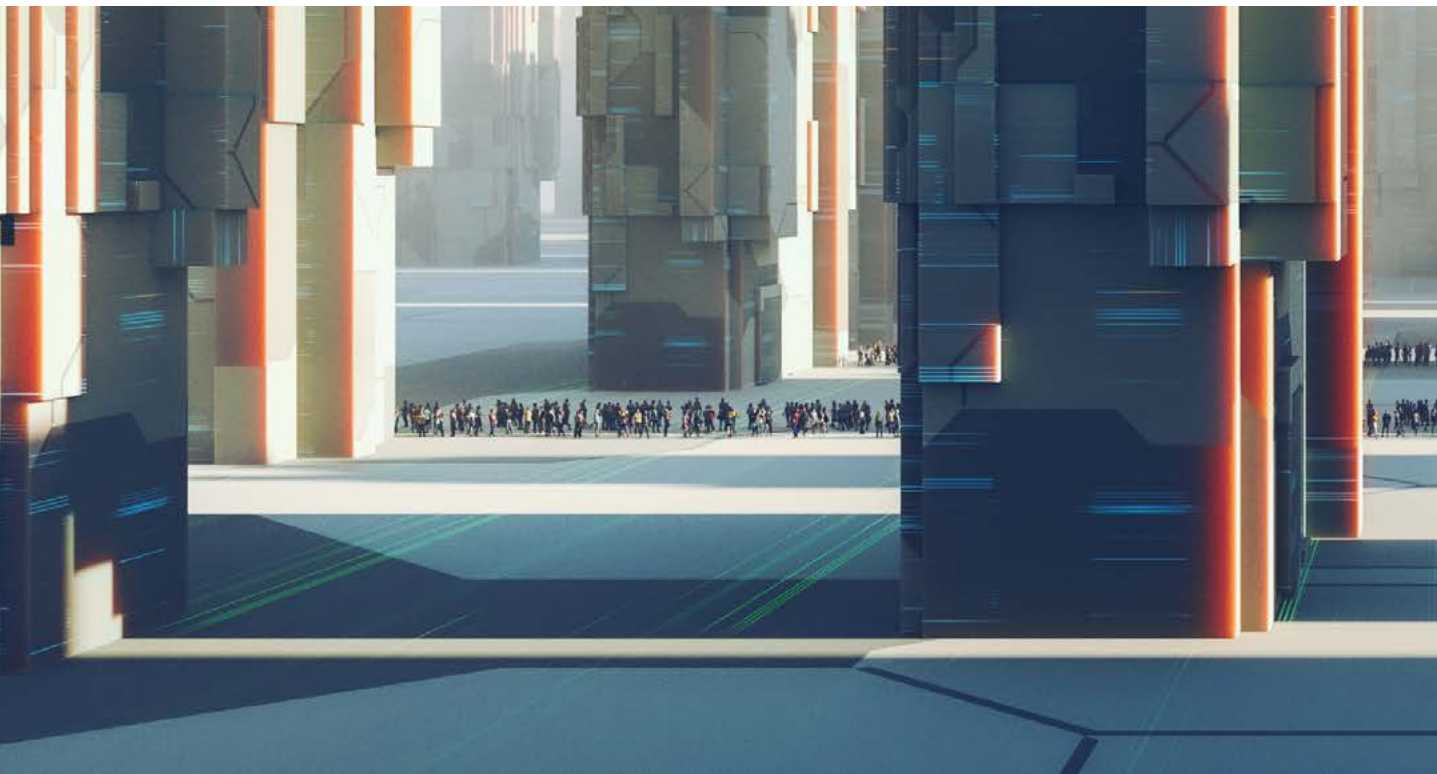
L'effet produit par les hacktivistes reste cependant limité sur le cours du conflit militaire et politique : « Aujourd'hui, l'affrontement est cinétique. La guerre, c'est du cinétique. Ce sont des drones, c'est de l'artillerie, c'est du sang et des larmes, des ruines. Quand il y a du cyber sur le front, c'est essentiellement pour essayer de rentrer, de pénétrer les systèmes C2, de prendre le contrôle des systèmes de commandement de l'ennemi ».

« Ce conflit est un terrain d'expérience, estime **Damien Bancal**. En témoigne le nombre de fermes de bots que les autorités ferment, quasiment une ferme de bots par mois, tenue par des pirates russes qui ont pour mission clairement de profiter des téléphones portables pour lancer et diffuser des *fake news* ». En témoigne aussi le nombre de pirates informatiques qui sont toujours sur place et qui agissent aussi bien comme hackivistes ou comme cybercriminels.

Les groupes de *hackers* sont-ils en capacité de respecter le droit des conflits armés, et notamment le principe de distinction entre civils et militaires qui interdit toute action visant des non-combattants ?

Karinne Bannelier

Au plan juridique, l'emploi de « l'arme cyber » dans la guerre en Ukraine met en lumière les difficultés d'application du droit des conflits armés qui s'appuie sur la Convention de Genève et les protocoles additionnels de La Haye, observe **Karine Bannelier**. Première question : les hacktivistes peuvent-ils appliquer les principes que le droit édicte ? Le droit des conflits armés n'interdit pas à des *hackers* de participer à des opérations. Mais ces groupes de *hackers* sont-ils en capacité de respecter le droit des conflits armés, et notamment le principe de distinction entre civils et militaires qui interdit toute action visant des non-combattants ? Cette hypothèse est d'autant moins probable que ces groupes opèrent dans la clandestinité, souvent sous le contrôle d'États qui bénéficient, par l'intervention de « tiers attaquants », de l'avantage de la « négation possible ». Les attaques conduites par des États et visant des infrastructures sensibles se sont ainsi largement répandues. Deuxième question soulevée : quel statut doit-on accorder aux *hackers* ? Participent-ils directement aux hostilités ? Les groupes de *hackers*, en fonction des actions qu'ils vont conduire dans le conflit ukrainien, vont-ils perdre leur protection de civils parce qu'ils participent directement aux hostilités, ce qui signifie qu'ils pourraient devenir des cibles légitimes ? Dans ce cas, la Russie ou l'Ukraine auraient un droit de riposter contre ces *hackers*, pas uniquement via le cyberespace, mais également par des moyens cinétiques. On mesure alors le risque d'escalade, voire de mondialisation du conflit, liés à ces groupes hacktivistes.



Si les mesures prises dans la cadre de la cybersécurité, à l'échelle nationale ou européenne, ont pour objectif de limiter les effets de l'hacktivisme malveillant, en protégeant davantage les systèmes de traitement automatisé de données, pour eux-mêmes ou pour les données qu'il stockent ou échangent, il apparaît clairement que le champ des contenus est désormais un domaine hors contrôle ou presque, malgré les efforts récents pour le réguler. Habitués à prendre pour vérité vraie tout ce qui est véhiculé sur internet, notamment sur les réseaux sociaux, les esprits n'ont pas encore acquis une capacité de discernement leur permettant de passer les informations au crible de l'esprit critique. C'est sans doute la bataille des esprits qu'il faudra gagner au XXIe siècle si l'on ne veut pas que les citoyens deviennent esclaves sous les coups de boutoir d'un hacktivisme idéologique. Parmi les solutions, il y a sans doute l'hacktivisme citoyen, celui qui veille, qui éveille, dans un cadre éthique qu'il faut encore sans doute préciser.

agora
INCYBER FORUM

RETROUVEZ NOS DERNIÈRES ACTUALITÉS
ET NOS PROCHAINS ÉVÉNEMENTS SUR :

agora-incyber.com