# Les nouvelles orientations 2019 2020 de la cybersécurité/cyberdéfense pour la Chaire Saint-Cyr, Sogeti, Thales

Par
Ambassadeur Jean-Paul Laborde
Assemblée parlementaire de la Méditerranée
Titulaire de la Chaire Cybersécurité & Cyberdéfense Saint-Cyr, Sogeti, Thales et directeur du Centre d'expertise sur la lutte contre le terrorisme (CELT)
Écoles de St-Cyr Coëtquidan[1]

Les orientations de la Chaire Cybersécurité & Cyberdéfense pour les années 2019 et 2020, en cohérence avec nos partenaires sont clairement dirigées traditionnellement vers les activités liées à la défense, mais également vers les collectivités territoriales et la cybercriminalité internationale car il est clair qu'au-delà des questions technologiques ou nationales, on ne peut faire l'économie d'aborder cette dimension clé. Toutes ces activités, même si on peut les distinguer, sont d'ailleurs hélas souvent liées. Par exemple, dans l'attaque provoquée par un virus de type rançongiciel dont a été l'objet, en fin de semaine dernière, le Centre hospitalier universitaire de Rouen, le Parquet de Paris, seul compétent en France en la matière, a ouvert une enquête pour des faits de piratage visant un système informatique public en bande organisée ainsi que pour extorsion et tentative d'extorsion en bande organisée. L'enquête dira ce qu'il en est mais il est clair que nous ne portons pas assez notre attention aux dommages causés à nos concitoyens par le crime organisé dans le secteur cyber. Je prêche pour cette paroisse depuis maintenant deux années mais il semble que le message ne passe pas suffisamment.

Évidemment, nous sommes plus tentés, du fait de notre propension naturelle à envisager la cybersécurité et la cyberdéfense sur le plan stratégique de nous orienter vers les affrontements de puissances à travers les cyberattaques pour la protection de nos sites sensibles. Certes, c'est un aspect stratégique à ne pas négliger, compte tenu de l'avance de certains pays en la matière.

Mais, en fait, les acteurs de la cybersécurité doivent aussi et de plus en plus considérer la cybercriminalité comme un sujet de justice pénale, sachant que nous faisons des progrès technologiques tangibles grâce à certaines de nos entreprises et à l'intelligence artificielle. Mais, hélas, pour cette identification, la coopération internationale en matière pénale est essentielle si ce n'est absolument nécessaire. On voit ici se reproduite le schéma classique des activités criminelles des groupes criminels organisés et pas seulement des activités de groupes mafieux. En effet, selon la Convention des Nations Unies contre la criminalité transnationale organisée, un groupe criminel organisé est un groupe composé de trois personnes ou plus, ce qui est souvent le cas pour les groupes criminels procédant à des cyberattaques et non des groupes très structurés à l'organisation hiérarchique pyramidale et complexe. Ces derniers peuvent, bien entendu, s'intéresser à ce type d'attaques mais ce n'est pas forcément de leur seul ressort. Voilà un premier tabou levé. Le second tabou est celui de l'attribution en miroir de la responsabilité pénale. En effet, au niveau international, la question de l'attribution est souvent évoquée. Ce concept recouvre, en droit international, qui peu à peu a déteint sur les définitions

[1] Ancien Sous-secrétaire général des Nations Unies et directeur exécutif du Contre-terrorisme au Conseil de sécurité de l'ONU et conseiller honoraire à la Cour de cassation

nationales, la désignation par l'autorité qualifiée du pouvoir exécutif de celui ou de celle qui a dirigé une attaque contre un État, et elle autorise ce dernier à riposter dans le cadre de la légitime défense. Les spécialistes de la cybersécurité et de la cyberdéfense ont prudemment débattu des questions relatives à « l'attribution[2] » de ces attaques entre États ou en tout cas par le pouvoir exécutif de l'État attaqué. Il est clair que l'État attaqué peut se trouver en situation de légitime défense et peut actionner l'article 51 de la Charte des Nations unies « *au vu duquel un état attaqué peut commettre un fait objectivement illicite pour repousser une violence effective et injuste. Cette notion de légitime défense a toute son l'importance à l'ONU où la riposte est normalement attribuée à des organes appropriés comme le Conseil de sécurité* **».**

A ce sujet, il est clair, que cette riposte relève, dans ce cas, des seules autorités de cet État dans le cadre de la défense de sa souveraineté. Mais, rien n'empêche également le pouvoir exécutif de saisir les autorités judiciaires compétentes pour faire juger de la responsabilité pénale des auteurs de ces attaques, comme il est possible de le constater, les deux concepts sont totalement différents et il ne faut pas les confondre. L'un relève de la souveraineté exclusive des autorités exécutives d'un. État et l'autre des décisions de l'Autorité judicaire.

Pour ma part, j'irai bien plus loi au regard des attaques perpétrées il y a deux ans sur les hôpitaux londoniens et l'entreprise française Renault ou encore au regard de l'attaque récente contre l'hôpital de Rouen. Certes, il faut se prémunir au niveau local et augmenter sensiblement la capacité de résilience des systèmes informatiques locaux ou régionaux. A ce sujet, la Chaire Saint-Cyr, dans le cadre de sa vision stratégique cybersécurité/cyberdéfense se penche sur la thématique de la cybersécurité des collectivités locales et un colloque aura lieu précisément sur ce sujet en février prochain. Mais, en même temps, il faut aussi se projeter plus loin afin de déceler mais aussi de punir les attaques contre ces collectivités locales. Ces dernières sont détentrices de données personnelles immenses que les groupes criminels plus que tout autre organisation étatique ou paraétatiques seraient intéressés à connaître. Ces données, tout d'abord, constituent souvent un capital de vie pour les patients des hôpitaux, par exemple, et donc peuvent faire l'objet de rançons mais aussi, sans même parler de rançons, peuvent être revendues à des groupes peu scrupuleux pour projeter dans l'avenir l'état de santé de tel ou tel morphotype de citoyen ou même de citoyens eux-mêmes afin de dessiner la carte de santé de pays, de régions ou encore au niveau planétaire. Voilà donc les activités criminelles auxquelles il faut s'attaquer maintenant et qui nécessitent une coopération internationale approfondie non seulement entre les services de renseignements, comme l'a d'ailleurs évoqué le représentant de la Direction générale de la sécurité intérieure mais aussi au niveau de la police judiciaire et des autorités judiciaires. Certes, Europol et Eurojust travaillent déjà sur ce thème mais il faut, à la vérité de dire, que cette question dépasse largement le territoire de l'Union européenne. C'est pourquoi, nous nous sommes lancés dans un projet de coopération avec le Conseil de l'Europe dont les États dépassent le cadre de ceux de l'Union Européenne, nous sommes donc entrés, au niveau de la recherche appliquée, dans une réflexion approfondie autour du projet de protocole sur la coopération internationale du Conseil de l'Europe afin d'améliorer cette coopération internationale pour laquelle à ce moment précis seule la Convention de Budapest tient lieu de socle. Le protocole s'élabore autour de questions complexes telles que la possibilité de réponse des entreprises du numérique aux demandes des autorités judiciaires d'autres pays. Certes, déjà

[2] Tout fait internationalement illicite d'un État engage sa responsabilité internationale. A ce sujet, l'article 1er de la Commission de Droit International a édicté qu'il faut, pour engager la responsabilité internationale d'un état, la violation d'une règle de droit et que celle-ci soit applicable a un sujet de droit international. L'imputation de ce fait se définit alors comme l'attribution de ce fait illicite à cet état ou à cette organisation internationale. (https://www.doc-du-juriste.com/droit-public-et-international/droit-international/dissertation/imputation-agression-droit-international-face-montee-terrorisme-447279.html)

les GAFA s'autorisent à répondre pour l'identification des auteurs de messages à contenu terroriste mais on est loin d'une réponse régulière et habituelle. Et encore, il n'y a pas de coopération sur le contenu des messages. On est donc bien loin d'une coopération approfondie sur des attaques cyber. C'est pourquoi, nous avons les 10 et 11 Octobre dernier activement participé à une réunion commune de l'Assemblée parlementaire de la Méditerranée et du Conseil de l'Europe qui permet de faire réfléchir ensemble des institutions internationales et des parlementaires de la zone Méditerranée sur l'importance de cette coopération. La solidité des lois nationales et leur modernisation est un impératif premier et je voudrai ici, publiquement exprimer toute ma gratitude à Maître Cécile Doutriaux, membre de la Chaire, qui, au cours de ce séminaire, a fait un exposé qui a été unanimement apprécié par l'assistance. C'est tout à l'honneur de notre Chaire d'avoir ainsi des membres très actifs de notre réseau qui procurent ainsi un vrai renom à cette dernière. Nous avons également participé les 16 et 17 octobre dernier à la réunion annuelle des services de sécurité à Moscou sur ce sujet et tous les acteurs présents ont souligné à la fois l'importance de la coopération internationale et de la protection des droits des personnes victimes de ces attaques.

Enfin, il faut noter, au niveau mondial, une évolution certaine dans cette matière par la création d'un groupe de travail intergouvernemental ouvert au niveau de l'ONU, outre le groupe d'experts déjà crée qui lui ne regroupe que des experts comme son nom l'indique et ne représente pas les États. Il est intéressant de noter, à ce sujet, que le groupe intergouvernemental ouvert, a, à l'étonnement de tous, avancé dans la volonté de coopération et de création possibles d'outils de coopération internationale. J'ai, en ma qualité de titulaire de la Chaire été invité à la tenue d'un séminaire, en marge de l'Assemblée générale traitant de ce sujet, organisé par Microsoft, le Comité International de la Croix Rouge internationale et la Haute Représentante des Nations Unies pour le désarmement qui est en charge de ces questions sur les points positifs et négatifs d'une telle coopération. Il en est ressorti que, certes, il faut aller de l'avant mais que la diffusion d'informations à travers cette coopération ne devrait pas non plus nuire au travail important réalisé pour la protection des droits des personnes dans le cadre de conflits armés par le droit international humanitaire.

Il convient aussi de poser un autre problème qui nous demande des efforts supplémentaires par rapport au travail qu'il faut accomplir en cybersécurité/cyberdéfense il y a quelques années que deviendrait maintenant notre cybersécurité/cyberdéfense sans l'apport et le soutien de l'intelligence artificielle ? Ceci étant, l'intelligence artificielle est un outil multi facettes. Ainsi, elle peut être utilisée par les acteurs de la cybersécurité/cyberdéfense mais elle peut l'être également à des fins malveillantes.

C'est pourquoi, nous avons organisé en avril dernier une réunion de haut niveau avec le CNAM et d'autres partenaires sous la direction éminente de Thierry Berthier et en coopération avec lui pour réfléchir à ces problématiques. Ce fût, il faut le dire un grand succès avec plus de trois cents participants venant du monde entier et un regard croisé public-privé sur chaque thème. Nous prévoyons un séminaire de même type pour faire un point sur l'avancée de cette question courant 2000.

Nous devons, c'est aussi l'évidence, nous développer dans ces axes de travail sur des publications qui nous permettrons de faire un point sur ces questions cruciales.

Pour suivre, je voudrai évoquer un sujet qui me tient à cœur par-dessus tout et qui pourrait constituer un axe de recherche également clé que constituent les liens entre cybercriminalité et

terrorisme d'une part et de l'usage préventif de la cybersécurité/cyberdéfense dans cette perspective d'autre part.

Tout d'abord, qu'ont donc à faire les nouvelles technologies, la cybersécurité/cyberdéfense dans les questions liées au terrorisme ?

En premier lieu, il faut souligner la flexibilité des terroristes pour utiliser tous les moyens possibles que la modernité peut mettre à leur disposition. A cet effet, entre utilisation des nouveaux outils et confusion des genres criminels, les organisations terroristes trouvent leur compte.

On ne peut nier les liens objectifs entre crime organisé et organisations terroristes, selon leurs besoins et les résultats escomptés. C'est pourquoi, récemment le Conseil de Sécurité de l'ONU a adopté une résolution sur ces liens[3]. Or, avec le développement des nouvelles technologies, les réseaux criminels utilisent de plus en plus l'outil cyber car il est facile d'approche et finalement, pour l'instant préserve de peines importantes en comparaison avec d'autres types de criminalité (par exemple extorsion au préjudice de banques par cyber attaques par rapport à des braquages au préjudice de ce même type d'institutions). C'est pourquoi, dans cette période de changements et surtout après la défaite territoriale de Daesch qui donc est à la recherche de nouvelles opportunités de frapper, on peut légitimement se poser la question de savoir si les techniques du cybercrime ne risquent pas d'être utilisées par les organisations terroristes.
Déjà, il est clair qu'en Syrie, d'autres méthodes que celles traditionnellement employées par les terroristes, ont été utilisées, par exemple, les attaques au gaz innervant.

C'est pourquoi, en avance sur son temps, la conférence conjointe des 10 et 11 octobre dernier de l'Assemblée parlementaire de la Méditerranée et du Conseil de l'Europe à laquelle la Chaire s'est jointe, a déjà envisagé la question de la cybercriminalité et de ses liens avec le terrorisme. Les parlements ont, en effet, un rôle crucial à jouer dans cette lutte pour maintenir l'équilibre nécessaire entre la lutte contre ces fléaux et le maintien de l'état de droit mais aussi la mise en place de législations adéquates. Or, le Conseil de l'Europe, toujours à la pointe du droit international, nous montre encore la voie et nous sommes ici pour réfléchir aux moyens législatifs mais aussi à ceux relevant de la diplomatie parlementaire pour faire face à la conjonction de ces fléaux.

Dans ce contexte, les États, ne laissaient que très peu de place aux faits criminels eux-mêmes et à la détermination de la responsabilité pénale étatique ou individuelle.

[3] Le Conseil de sécurité a adopté à l'unanimité la résolution 2482 (2019) sur les liens entre terrorisme international et criminalité organisée : https://www.espacemanager.com/le-conseil-de-securite-adopte-des-mesures-pour-briser-les-liens-entre-le-terrorisme-international-et

Mais alors, qu'en est-il des liens possibles entre cyber attaques et terrorisme et pour parler clair du cyberterrorisme ?

Ici il faut ici être précis sur les termes et c'est pourquoi les parlementaires ont pleinement leur rôle à jouer sur ces questions. En effet, par exemple, l'usage d'internet par les terroristes ne constitue pas en soi le cyber-terrorisme. A la fois à la Chaire Cybersécurité & Cyberdéfense des Écoles de Saintt-Cyr, dont je suis le titulaire et dans le cadre de l'Initiative mondiale contre la criminalité transnationale organisée à laquelle je participe, nous rencontrons fréquemment les GAFA et nous voyons bien les progrès faits ensemble pour empêcher les terroristes et leurs organisations d'utiliser les moyens de la cyber dans le cadre de leurs actions criminelles.

On a pu distinguer ici plusieurs utilisations mais qui ne sont pas à proprement parler des utilisations cyber mais plutôt celles des moyens que mettent à disposition les nouvelles technologies.

Tout d'abord, il s'agit bien entendu de l'utilisation d'internet à l'usage de prosélytisme, de recrutement des terroristes, ou d'appels pressants aux fins d'attaques terroristes, bref il s'agit de l'utilisation du web et des messageries internet. Dans ce cas, l'utilisation de l'internet a été si vaste par Daesch que les États et la communauté internationale ont été dans l'obligation de prendre des mesures très concrètes, telles que l'effacement des messages et le blocage des conversations sur le net qui permettent de recruter de nouveaux émules terroristes. C'est l'objet du projet de règlement européen actuellement en discussion. Il faut noter, également, que de nombreux états de l'Union européenne, se sont déjà doter de dispositions de surveillance et d'interception sur le plan préventif ainsi que de moyens de répression de ces techniques de recrutement de terroristes et d'appel à la commission d'attaques terroristes. Mais, il faut aussi être conscients que les appels à la radicalisation ainsi qu'à commettre des attaques terroristes sont souvent venues de pays hors frontières de l'Union européenne et, en particulier, des pays dans lesquels Daesch était très bien implanté. Il faut donc faire appel à la coopération internationale en matière pénale détecter ces actes, identifier les délinquants et les traduire en justice dans le cadre évident de l'état de droit et du respect des droits de la personne humaine. D'où l'utilité évidente d'un protocole international sur cette coopération internationale en matière pénale que prépare le Conseil de l'Europe.

En second lieu, outre le recrutement des terroristes, l'internet peut-il également servir, à travers les messages électroniques, à permettre aux terroristes de communiquer entre eux et à préparer, ou perpétrer des attaques terroristes. À en croire les autorités, il faut répondre par l'affirmative[4]. Par exemple, *« Sid-Ahmed Ghlam, le suspect des attentats avortés dans les églises de Villejuif (Val-de-Marne), n'utilisait son smartphone qu'en mode Viber. Yassin Salhi, l'auteur de la décapitation de son patron dans l'Isère, avait choisi l'application WhatsApp pour transmettre la photo de son "trophée" à son contact en Syrie. Quant aux trois jeunes du dossier Sémaphore, les enquêteurs ont découvert après leurs arrestations qu'ils communiquaient entre eux via une autre application de messagerie cryptée, Telegram. »* Voilà donc des utilisations précises d'internet par les terroristes. Il n'empêche, nous n'en sommes toujours par au cyber terrorisme.

[4] Cette généralisation du chiffrement, notamment sur les smartphones – au point de devenir un argument marketing – ne cesse d'inquiéter, et pas seulement en France. Au Royaume-Uni, David Cameron a déjà évoqué l'idée d'interdire ces messageries mobiles cryptées. Pour Barack Obama, elles pourraient représenter une "menace pour la sécurité nationale" ; le patron du FBI est parti en guerre contre les nouvelles fonctionnalités de cryptage introduites par Apple et Google dans leur système d'exploitation mobile. (Journal du Dimanche-JDD (***19 juillet 2015, modifié à 16h34 , le 20 juin 2017)***

Une autre utilisation de l'internet dans le cadre des activités d'une organisation terroriste en est le financement des organisations terroristes, voire le soutien financier à une attaque terroriste. Ici, la palette est large. En effet, de l'utilisation de l'internet-banking au transfert de fonds par téléphone mobile, de nombreuses zones d'ombres existent ainsi que de nombreux trous dans les raquettes des organismes de contrôles. Il faut, à cet égard, distinguer les pays dans lesquels les contrôles sont efficaces, de ceux qui utilisent des cellules de renseignements financiers mal équipées avec des personnels mal formés des pays et de systèmes off-shore dont les détenteurs ne seraient peut-être même pas au fait des placements financiers qui serviraient à soutenir des organisations terroristes, par l'effet même de l'opacité des opérations de comptes mises en place dans ces centres ou places off-shore. Mais, il faut aussi faire la distinction entre la menée d'attaques terroristes peu coûteuses, comme l'a très bien souligné François Molins, alors procureur de la République de Paris, dans son intervention à la Conférence « No Money for Terror » qui s'est tenue les 25 et 26 avril 2018 à Paris[5] du soutien financier dont ont besoin les organisations terroristes pour survivre et qui, elles, utilisent les outils de l'internet. Mais..ceci n'est toujours pas du cyber terrorisme.

Mais finalement qu'en est-il le cyber terrorisme ? Il serait clair que des infractions utilisant les moyens cyber pour attenter à la vie d'autrui dans le but d'intimider la population générale ou d'obliger un gouvernement à faire ou ne pas faire quelque chose constituerait un acte de terrorisme au sens des Conventions contre le terrorisme de l'ONU. Pour l'instant de telles situations ne se sont pas produites. Mais, sur les cibles molles, les infrastructures sensibles par exemple, on ne peut pas dire que le risque n'existe pas. Il faut s'y préparer car la meilleure défense contre les attaques de ce type est constituée par la prévention. La note optimiste, dans cette optique, nous a été révélée durant le dernier Forum international pour la Cybersécurité qui s'est tenu à Lille en janvier dernier. Il y a été confirmé que, nous savons de mieux en mieux identifier les attaques cyber et y répondre. Alors, persévérons dans cette direction pour un monde dans lequel nous arriverons à contrer très fermement les éventuelles attaques cyber d'organisations terroristes.

Ici, dans le cadre de l'European Cyber Week, je vous invite à être pionniers dans ces domaines. En tout cas la Chaire Cybersécurité & Cyberdéfense Saint-Cyr, Sogeti, Thales le sera. Elle le sera d'autant plus que dans le cadre de ses relations avec la Chaire Cyb'Air et la Chaire Navale sous la coordination de l'Amiral Pascal Verel que je me dois de remercier pour son action de coordination qui s'est concrétisée en juin dernier par une première journée inter chaires à renouveler bien sûr, nous pouvons faire face à une série de défis : les défis technologiques, les défis relatifs aux sciences humaines et les défis juridiques. Il est clair qu'ensemble nous sommes plus forts et il le faut absolument Je souligne, à cet effet, que c'est dans le cadre d'un partenariat public-privé plus que d'un mécénat, en respectant les lois, les normes et les compétences de chacun que nous y arriverons sans négliger les apports de la société civile qui doit toujours être un partenaire pour nous.

Je vous remercie de votre attention

[5] https://www.voaafrique.com/a/no-money-for-terror-fin-de-la-conférence-sur-le-financement-du-terrorisme-en-france/4365797.html
"les terroristes ont eu besoin de 25.000 euros pour organiser les attentats de janvier 2015 (contre Charlie Hebdo et le supermarché Hyper Cacher) et 80.000 pour ceux du 13 novembre" à Paris et Saint-Denis.