# Les menaces terroristes et l'impact des nouvelles technologies

Par
Ambassadeur Jean-Paul Laborde
Assemblée parlementaire de la Méditerranée
Directeur du CELT et titulaire de la Chaire Cyber sécurité des Écoles de St-Cyr Coëtquidan

Avant d'entrer dans le vif de notre sujet, laissez-moi m'incliner à mon tour devant les victimes de l'attaque terroriste qui a endeuillé hier la ville allemande de Halle, ce qui est aussi l'occasion de rappeler à notre mémoire les victimes (tuées et blessés) de l'attaque terroriste de Strasbourg le 11 décembre dernier et de nous incliner également devant elles.

Le sujet de notre première session a trait aux menaces terroristes et aux nouvelles technologies.

Qu'ont donc à faire les nouvelles technologies dans les questions liées au terrorisme ?

Il faut tout d'abord 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, par exemple 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[1]. Or, il est indéniable qu'avec le développement des technologies, les différents outils cyber des réseaux criminels sont de plus en plus importants et peuvent être utilisés à des fins terroristes. On va examiner ce qu'il en est en réalité.

Dans ce contexte, je suis particulièrement honoré de me trouver ici au Conseil de l'Europe, pionnier de la lutte internationale à la fois contre le terrorisme contre lequel il dispose d'outils efficients et en même temps d'instruments internationaux contre la cybercriminalité. C'est pourquoi conférence est si symbolique aujourd'hui entre Conseil de l'Europe, Assemblée parlementaire du Conseil de l'Europe et Assemblée parlementaire de la Méditerranée. 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. 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.

L'ONU démarre maintenant ces travaux sur une possible coopération internationale de lutte contre la cybercriminalité sans parler de ses liens avec le terrorisme et essaie également de trouver des solutions sur la question du terrorisme au Moyen-Orient, en Afrique. Ensemble, nous avons un peu d'avance et nous devons montrer la voie. Merci donc à Jan Kleijssen, Directeur à la direction de la société de l'information et de l'action contre la criminalité du Conseil de l'Europe, à Alexandre Seghers, Secrétaire exécutif du Comité de la Convention sur la cybercriminalité ainsi Marie Agha-Wevelsiep, Directeur de programme au Bureau du

[1] 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

Conseil de l'Europe sur la Cybercriminalité mais aussi à Fatima Khachi, Adjointe au Secrétaire général de l'APM et Vladimir Kirushev, Administrateur de programme à l'APM pour l'organisation de cette réunion qui vient absolument à point nommé et merci surtout à nos chers parlementaires de l'APM présents aujourd'hui pour avoir accepté de réfléchir ensemble aux moyens à mettre en œuvre pour lutter contre ces phénomènes criminels et leurs liens entre eux.

L'ampleur de attaques cyber doivent évidemment nous donner de plus en plus à réfléchir à leur possibles incidences sur les méthodes terroristes. En effet, depuis les cyberattaques de 2017 sur Renault et les services de santé anglais, les enjeux de cybersécurité sont beaucoup plus connus du grand public. De nouveau, les récentes attaques de ces dernières semaines sur les différents services publics, et plus particulièrement les services de santé et les hôpitaux français nous y ont également plus sensibilisés. Les inconvénients que nous éprouvons toutes et tous dans notre vie quotidienne avec les problèmes rencontrés avec les cyber-attaques sur nos cartes de crédit par exemple viennent aussi nous dire combien les cybers attaques sont proches de nous. Certes, les études, commentaires, programmes, projets et travaux des institutions sur le cyber se sont davantage concentrés jusqu'à ce jour sur les cyber-attaques contre ou entre les organes de défense ou de sécurité des États. Elles se sont aussi focalisées sur les questions relatives à la propagande pré-électorales. Les spécialistes de la cybersécurité et de la cyberdéfense ont également prudemment débattus les questions relatives à « l'attribution[2] » de ces attaques entre États ou en tout cas par le pouvoir exécutif de l'État attaqué. Ainsi, à la suite de l'attribution d'un fait illicite commis par un État ou une organisation non-étatique, il devient clair que l'État attaqué peut se trouver en situation de légitime défense et actionner l'article 51de la Charte des Nations unies « *au vu duquel état attaqué commet un fait objectivement illicite pour repousser une violence effective et injuste. Cette notion de légitime défense a de l'importance à l'ONU où la protection est attribué à des organes appropriés comme le Conseil de sécurité et les opérations de maintien ou de rétablissement de la paix.* ***La légitime défense représente alors une exception à cette interdiction[3] ».***

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.

Or c'est encore une fois oublier que sur les attaques liées aux activités des groupes criminels organisés.

Si l'on se réfère à un panorama qui date un peu mais qui est sûr et qui n'a fait depuis lors que croître, quels chiffres donnent le vertige et ils datent de 2015 :

***« 400 MILLIONS DE DOLLARS***

*C'est la perte financière estimée liée aux fuites de données, provenant de 700 millions de données compromises.*

---

[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)

[3] https://www.doc-du-juriste.com/search?q=acte+illicite&start=0&topConsult=0&fullSearch=1

*79 790 INCIDENTS ont été détectés dans 61 pays en 2014, avec 2122 cas avérés de perte de données.*

***38%***
*Dans **38%** des cas, quelques secondes suffisent aux attaquants pour compromettre un système. Et dans 28% des cas, il ne faut que quelques minutes pour voler les données.*

*82 SECONDES*
*C'est le temps qui s'écoule entre l'envoi d'une campagne de phishing et le premier clic. Au total, 23% des destinaires ouvrent les emails, 11% cliquent.*

***99,9% DES VULNÉRABILITÉS EXPLOITÉES***
***99,9% des vulnérabilités des systèmes sont exploitées plus d'un an après avoir été identifiées. 7 millions de vulnérabilités ont été exploitées en 2014, mais 10 vulnérabilités couvrent à elles seules 97% des attaques. Elles sont souvent très anciennes.***

*170 MILLIONS DE MALWARES*
*Il existe plus de **170 millions de malwares**. Sur 20 000 organisations, 5 évènements liés à des malware ont lieu chaque seconde.*

*30% D'ERREURS HUMAINE*
*30% des incidents sont attribuables à l'erreur humaine. Pour les fuites de données, le chiffre tombe à seulement 10%.*

*9 MODÈLES DE RISQUES*
*Il y a 9 modèles de risques identifiés, mais trois d'entre eux représentent 75% des attaques : les erreurs humaines, les menaces internes, et les malwares[4] ».*

En outre, l'année 2017 a donné lieu *à nombreuses cyberattaques à portée mondiale, les entreprises française, par exemple enregistrent des pertes financières estimées à 2,25 millions d'euros en moyenne, en hausse de 50% (à taux de change constant en un an)[5]*. Tels sont les résultats de la dernière étude du cabinet de conseil et d'audit PwC.

Il convient à la vérité de dire qu'aujourd'hui les réactions s'organisent ; c'est pourquoi, j'ai demandé à Maître Cécile Doutriaux de venir nous exposer la réaction des juristes français dans ce nouveau contexte et que la Gendarmerie en France a récemment démantelé un réseau complet de cybercriminels, à la suite de l'impulsion qui lui a été donnée sur ces sujets par le Général d'armée Watin-Augouard, ancien inspecteur général de la Gendarmerie et grand spécialiste de la cyber et qui n'a pu, hélas, se joindre à nous aujourd'hui. En Europe, aux Etats unis, les réactions s'organisent.

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

---

[4] https://www.usine-digitale.fr/article/la-complexification-des-cyberattaques-en-8-chiffres.N339067

[5] https://www.pwc.fr/fr/espace-presse/communiques-de-presse/2017/novembre/les-entreprises-francaises-accusent-des-pertes-financieres.html

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/cyber défense des Écoles de St-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 pour faire du prosélytisme, recruter des terroristes, faire des appels pressants aux fins d'attaques terroristes, bref utiliser le web et les 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 implantés, à savoir l'Irak et la Syrie. Il faut donc faire appel à la coopération internationale en matière pénale détecter ces actes, identifier les délinquants et les traduite en justice dans le cadre évident d'e 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 telle que le prépare actuellement l'équipe d'Alexandre Seghers avec les représentants qualifiés du Conseil dans le cadre d'Octopus dont il vous parlera mieux que moi. Il s'agit là d'un outil indispensable, auquel nous pouvons réfléchir également dans le cadre de l'APM.

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[6]. 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

[6] 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)***

terrorisme, à savoir l'utilisation des moyens cyber pour commettre, en direct, des attaques terroristes.

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 ici faire la distinction entre la menée d'attaques terroristes peu coûteuses, comme l'a très bien souligné Francois 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[7] du soutien financier dont ont besoin les organisations terroristes pour survivre et qui, d'ailleurs fait l'objet de sanctions de la part du Conseil de sécurité de l'ONU à travers les résolutions 1267 et suivantes ainsi que de la part d'autres instances internationales ou régionales et qui, elles, utilisent les outils de l'internet. Mais..ceci n'est toujours pas du cyber terrorisme.

Alors qu'est-ce que 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 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 du Conseil de l'Europe et de l'APM, le lieu est tout à fait approprié. Soyons les pionniers de cette lutte afin que, pour une fois, la répression et la réaction laissent la première place à la prévention et à une stratégie institutionnelle et parlementaire conjointe au niveau de nos institutions régionales.

---

[7] 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.