# Pour le développement d'une coopération internationale entre les services de sécurité et les agences d'application de la loi

*par*
Jean-Paul Laborde
*Ambassadeur de l'Assemblée parlementaire de la Méditerranée,*
*Conseiller de l'Initiative mondiale de lutte contre la criminalité organisé et titulaire de la Chaire cyberdéfense/cybersécurité*
*Directeur du Centre d'expertise sur la lutte contre le terrorisme au Centre de recherches des Écoles de St-Cyr-Coëtquidan e*[1]

Monsieur le Directeur,
Excellences, chers collègues, mesdames messieurs,

Le titre de notre session nous entraîne vers la coopération des services de sécurité et des agences chargées de l'application de la loi pour la protection de l'information dans l'espace national. Pourtant, mon intervention veut aller plus loin. Je crois qu'il faut avoir une vision à moyen terme et non à court terme pour pouvoir lutter contre la cybercriminalité pour autant qu'elle soit liée au terrorisme, voire même pour trouver des équilibres entre les différentes nations en matière de cyberdéfense.

En effet, si l'on veut lutter contre les flux d'information liés au terrorisme ou tout simplement contrer la cybercriminalité seulement au niveau national, il sera difficile de le faire ; il faut, en réalité une véritable coopération internationale. L'espace information, du fait de l'utilisation des réseaux sociaux, du dark-web et autres systèmes informels de communication, est libre ; en sus, je pose même la question, peut-on vraiment dire qu'il est national ? Même dans les pays où un contrôle plus fort existe, on ne peut pas dire que l'espace d'information est protégé, d'ailleurs le faut-il ? La liberté d'expression fait partie de nos valeurs, au regard même du Pacte des droits civils et politiques de l'Organisation des Nations Unies, qui, je le rappelle, a été ratifié ou incorporé dans l'ordre juridique interne de 186 États dans le monde. Autant dire qu'il fait partie de l'ordre juridique international. Donc, la quadrature du cercle que nous devons résoudre tous ensemble est à la fois d'assurer cette liberté d'expression et, en même temps, d'empêcher la cybercriminalité et les messages de propagande du terrorisme de se répandre librement et ainsi de permettre le recrutement de nouveaux terroristes à travers l'internet, comme l'évoquait hier la directrice exécutive de la Direction exécutive contre le terrorisme du Conseil de Sécurité. Les messages faisant l'apologie du terrorisme qui sont postés sur le web, sont souvent à l'origine des actions terroristes individuelles. Ces attaques individuelles que l'on qualifie d'actes de terrorisme « en provenance de loups solitaires » nous montrent bien que « ces loups » ne sont pas si solitaires que l'on veut bien le dire puisqu'ils ont eu des contacts avec des représentants des organisations terroristes justement à travers l'internet.

Sur le plan de la cybersécurité, et en particulier de l'intégrité des messages figurant sur l'internet, il faut distinguer entre plusieurs types d'attaques. S'il s'agit d'affaires interétatiques, la seule réflexion que je peux vous proposer et qui relève éventuellement de la cyber défense, est de dire qu'aucun état, aucune entité n'est à l'abri de telle attaques, comme l'a relevé le Vice-Ministre de la Sécurité d'État de la République populaire de Chine dans son intervention d'hier et que donc, la seule issue est de coopérer et de vivre en paix en s'assurant que, grâce à un dialogue et à une coopération intelligente, ces attaques puissent être rapidement résolues très

[1] JP Laborde est l'ancien directeur exécutif de la Direction exécutive contre le terrorisme du Conseil de sécurité des Nations Unies et conseiller honoraire à la Cour de cassation, France.

vite après leur détection, comme le mentionnait durant cette conférence, le représentant de la République de Moldavie. Mais, ce n'est pas ici le cœur de mon propos.

Ce qui me paraît le plus dangereux est ce que nous laissons trop souvent de côté, à savoir la lutte contre la cybercriminalité qui vient directement prendre des informations au cœur de nos vies sur ce qui est le plus important pour nous tous en tant que citoyens. Que dire des attaques cyber qui deviennent systématiques contre les hôpitaux pour récupérer les données de milliers de patients ou de malades ? Sait-on que ces informations, volées dans les bases de données des cliniques ou des hôpitaux, peuvent être revendues par les cybercriminels à des entités économiques ou autres intéressées par ces dernières. Inutile de souligner combien ces atteintes aux données individuelles peuvent être préjudiciables aux personnes et finalement aux collectivités nationales. Sans coopération entre les agences de sécurité et celles chargées de l'application de la loi au niveau international, dont le but doit être, à l'évidence, la protection des citoyens, il ne peut y avoir de lutte efficace contre ce type de criminalité pour le meilleur de nos sociétés, de leurs communautés humaines et de leurs droits personnels. Or, sans coopération avec les grandes entreprises du net pas de lutte efficace contre ce fléau. Il faut dire qu'à ce sujet, les choses avancent car on peut désormais interroger directement ces grandes entreprises qui soutiennent les réseaux sociaux pour obtenir à tout le moins l'identification de ces criminels. Mais, hélas, les systèmes juridiques de nombreux pays ne permettent pas de procéder à ces recherches rapides. Certes, les entreprises qui soutiennent les systèmes de dialogue ou d'échange d'information sur les réseaux sociaux sont de plus en plus nombreuses, de plus en plus petites et donc restent souvent à un niveau faible de coopération avec les services de sécurité. Sur le plan international, il en est de même. Oui, les GAFA peuvent coopérer..mais les autres ? La semaine dernière, l'Assemblée parlementaire de la Méditerranée a organisée, pour un échange entre ses parlementaires, une réunion commune avec le Conseil de l'Europe, qui a insisté , d'une part sur l'importance de s'équiper d'un arsenal législatif adapté au niveau de chaque pays pour lutter contre ces menaces et, d'autre part, sur l'importance de la coopération internationale pour laquelle un protocole sur cette question cruciale est actuellement en négociation entre les pays de ce Conseil qui permettra de résoudre beaucoup plus fréquemment, entre les États qui auront ratifié cet instrument, la question de la preuve judiciaire et de la responsabilité des attaques cyber devant les tribunaux et de former juges et procureurs qui se tiennent souvent trop loin de ces questions cruciales.

Il faut immédiatement noter que, sur le plan de la lutte contre le terrorisme, comme le relève les résolutions pertinentes du Conseil de sécurité et de l'Assemblée générale des Nations Unies, protéger les citoyens contre la radicalisation est une composante essentielle de la lutte contre le terrorisme. Or, peut-on prévenir cette radicalisation sans contrôler les messages terroristes et ne pas mettre à mal la liberté d'expression ? Oui, si d'une part nous travaillons de plus en plus avec le secteur privé et si l'on s'appuie également sur la société civile. Étrange peut-être de tenir ces propos devant les services de sécurité ! En fait, je ne le crois pas. En effet, les entités de renseignements connaissent très bien le rôle de chacun et l'important de l'implication de toutes et tous dans cette perspective de lutte contre la cybercriminalité. En tout cas, il faut échanger au moins nos pratiques sur cette question cruciale ; certes, il faut distinguer les informations elles-mêmes des méthodes et les pratiques mais partager les méthodes de travail et les pratiques est un point essentiel. Pour cela, il faut avant tout, un dialogue constant au niveau des services de sécurité. Il faut aussi, pour ces services, un dialogue fructueux et confiant entre ces agences et la société civile qui doit pouvoir fournir des informations de base, concernant les personnes susceptibles d'être entraînées sur les voies de cette radicalisation mais surtout donner l'exemple de convictions de paix, religieuses ou autres.

Or, pour ce dialogue, nous disposons des grands organes des Nations Unies, l'évaluation de la radicalisation, et le combat contre celle-ci étant une priorité à la fois de l'Office pour la lutte contre le terrorisme et l'organe d'évaluation des menaces et des capacités anti-terroristes, à savoir la Direction exécutive contre le terrorisme du Conseil de sécurité. Évidemment, me direz-vous, rien ne vaut l'approche bilatérale qui est la tendance naturelle de vos services. Je ferai remarquer que, si nous agissons ainsi, nous nous privons, d'avoir dans une même réunion, d'une part des échanges multilatéraux et donc plus riches sur des pratiques multiples concernant la prévention de la radicalisation, ce qui n'est pas simple et nécessite le soutien de la société civile, en particulier des leaders religieux et, d'autre part, des échanges d'information concernant les réseaux terroristes qui seraient susceptibles d'être activés. En matière de lutte contre la radicalisation, la transmission de l'information concernant la personne en voie de radicalisation est cruciale et il faut qu'elle soit communiquée à temps.

Mais la sécurité de l'espace d'information n'est pas malgré tout une chose simple…quelques exemples nous donnent une idée de l'immensité de la tâche :

***2015***

***« 400 MILLIONS DE DOLLARS***

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

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

Et cette tendance est en constante augmentation.

Aussi, je voudrai, monsieur le directeur, aller encore un peu plus loin dans la vision à moyen terme que je propose. On le sait, Daesch a subi un revers militaire sévère. Oui, nous nous accordons tous pour dire que cette organisation terroriste va continuer son œuvre de mort soit d'une manière souterraine soit en utilisant les media. Certes, nous n'avons pas encore à subir de cybercriminalité menant à des attaques terroristes mais il faut nous en prémunir.

Quelles sont donc les étapes à mettre en œuvre ? Commençons par les étapes de base : tout d'abord, il nous faut des mesures de sécurité bien étudiées qui soient à la fois solides et qui respectent l'État de droit mais aussi des législations efficaces et compatibles entre les états qui, ainsi permettent la coopération internationale et , comme l'a fait très bien remarquer Monsieur le Vice-Ministre des Affaires Étrangères de la Fédération de Russie, Mr Oleg Siromolotov. Or, en matière de cybersécurité, rien ne sert d'avoir des législations extrêmement dures si elles ne sont pas en harmonie avec celles d'autres États car alors il n'y aurait pas de coopération possible. Au regard des résolutions du Conseil de sécurité et de celles de l'Assemblée générale de l'ONU ainsi que des conventions existantes, nous devons certainement amender les législations pour faire face à ce nouveau type de menace. L'Assemblée parlementaire de la Méditerranée y compris ses parlements associés a déjà entrepris ce travail critique. On s'est en effet aperçu que, souvent, les États ratifient, prennent les mesures nécessaires sur le plan exécutif mais souvent ne changent pas leur législations internes et se retrouvent ainsi dans l'impossibilité de mettre en œuvre les mesures nécessaires d'extradition et de coopération internationale en matière pénale.

Le reste vous appartient.

Monsieur le directeur,

Merci encore pour m'avoir permis de partager avec vous encore durant cette session, mes réflexions sur ce sujet si sensible et nous avoir inviter dans cette magnifique cité de Sochi pour participer à cet évènement de si haut niveau durant lequel nous avons pu partager autant d'information et préparer notre travail du futur en pensant qu'en protégeant l'espace national d'information à travers notre coopération, nous protégeons, à coup sûr, l'avenir de nos enfants,