Le droit pénal ne prévoit pas de circonstances aggravantes lorsque sont visées des infrastructures qui contribuent à la santé publique. il me semble aujourd'hui nécessaire d'en créer au sein de la loi Godfrain.

Général d'armée (2S) Watin-Augouard, fondateur du FIC.
Cet entretien a été publié le 6 mai 2022.

1/ Y a-t-il quelque chose qui rende, dans ses motifs ou dans ses méthodes, la cybercriminalité spécifique, différente de la criminalité en tant que telle ?

En 2007, j'avais choisi pour thème du premier FIC, « la cybercriminalité, criminalité du XXIème siècle ». Il s'agissait alors de sensibiliser les décideurs afin qu'ils prennent sans tarder les mesures nécessaires. J'avais acquis cette conviction en animant un groupe de travail sur la cybercriminalité, présidé par Thierry Breton. **La cybercriminalité est spécifique si l'on considère les infractions qui visent les systèmes numériques et s'en prennent aux systèmes de traitement automatisé de données (STAD), aux données.** Elle est plus classique, en revanche, si l'on considère les infractions « vieilles comme le monde » qui connaissent une ampleur inédite en raison de la puissance amplificatrice des réseaux (l'escroquerie, par exemple). **Ce**

qui distingue la cybercriminalité, c'est l'absence d'unité de temps, de lieu et d'action qui caractérise les infractions « dans le monde réel ». Jamais le délinquant n'a été aussi proche de sa victime, jamais il n'a été aussi loin du « gendarme ». Le prédateur est invisible, son action est souvent imperceptible, ce qui rend la traque plus complexe. Les mobiles sont multiples : par exemple, une attaque par déni de service distribué peut être crapuleuse, accompagner une action terroriste, être le fruit d'une action étatique. Le code pénal s'attache à la matérialité des faits et, en général, ne prend pas en compte le mobile.

2/ Certains hackers s'en prennent à des lieux de fragilité ou d'humanité, comme les hôpitaux. Il y a peu de communication publique autour de ce que doivent craindre ceux qui agissent ainsi, ou de ce qu'il advient de ceux qui sont appréhendés. Est-ce une vue de l'esprit, et si non, comment y remédier ?

Les hackers s'en prennent d'abord au maillon faible. **Il se trouve que les hôpitaux figurent parmi les services publics les moins bien protégés, car il était « impensable » que les prédateurs attaquent des cibles aussi sensibles. Or les prédateurs sont sans morale.** Ils exploitent précisément l'effet psychologique de leur action en espérant qu'il conduira les autorités à céder. **Le droit pénal ne prévoit pas de circonstances aggravantes lorsque sont visées des infrastructures qui contribuent à la santé publique. Il me semble aujourd'hui nécessaire d'en créer au sein de la loi « Godfrain ».** Mais les prédateurs doivent craindre d'être confondus et condamnés. Depuis 2007, des progrès ont été accomplis dans la lutte contre la cybercriminalité, à l'échelle nationale et européenne, comme en témoignent certains succès. Mais il est indispensable d'augmenter rapidement les moyens de la justice et des forces régaliennes qui sont en charge des enquêtes : la gendarmerie, la police, mais aussi les douanes et la DGCCRF. Cela nécessite notamment de pouvoir accéder à la preuve numérique et surtout de

bénéficier d'une coopération internationale qui se renforce, mais qui n'est guère pratiquée par les Etats qui tolèrent des actions malveillantes depuis leur territoire.

3/ Faut-il redouter des mouvements d'exaspération contre notre monde de plus en plus numérique, qui s'en prendraient notamment à ses infrastructures ?

C'est déjà, hélas ! une réalité. Lors de la crise Covid-19, de nombreuses actions malveillantes ont été commises sur la « couche matérielle du numérique » (incendies d'antennes, coupures à la disqueuse de câbles ou de fibres optiques). Fin avril, des actions coordonnées ont été menées sur des fibres optiques reliant plusieurs métropoles. Il est encore trop tôt pour identifier les auteurs. **Je pense que notre infrastructure numérique n'est pas suffisamment protégée, l'effort étant orienté sur la lutte contre les malwares. Il est nécessaire de concevoir une « défense numérique des territoires ».** C'est un sujet sur lequel la prochaine session « souveraineté numérique et cybersécurité » de l'IHEDN que je dirige va travailler. Mais je ne pense pas que ces actes résultent de l'exaspération d'internautes. Il s'agit d'actions de sabotage, dont les motivations restent à préciser.

On notera toutefois la résilience du réseau. Il peut connaître des périodes de perturbation, mais le retour à la normale est rapide, grâce à l'intervention efficace des opérateurs.

Plus inquiétante serait une atteinte aux câbles sous-marins. C'est une infrastructure sensible dont la fragilité est évoquée alors que le conflit en Ukraine laisse imaginer des actions ciblées. La décision prise par la ministre des armées d'engager la marine nationale dans la profondeur (jusqu'à 6000m) témoigne, à mon avis, d'une prise de conscience. **Mais n'oublions pas que les câbles arrivent sur terre via les atterrissements.**

4/ Quelle est la probabilité d'un scénario aux termes duquel la formidable concentration de pouvoir que confère le levier numérique échoirait dans les mains d'une organisation ou d'un Etat voyou ?

Certains Etats « voyous » concentrent des moyens importants. Sauf à imaginer une fragmentation du net qui s'observe déjà partiellement, on ne voit guère l'intérêt qu'auraient ces acteurs à remettre en cause le fonctionnement global d'internet dont ils ont besoin, ne serait-ce que pour le business et l'envoi de leurs « banderilles numériques ». Plus inquiétante serait une domination sur des éléments essentiels (technologies, terres rares) sans lesquels le numérique ne peut fonctionner. **Celui qui maîtrisera l'ordinateur quantique pourra disposer d'un pouvoir absolu.** La recherche et développement, la formation de scientifiques est donc une urgence absolue.

Il faut être vigilants sur la bataille des normes qui se joue au sein d'instances internationales. La même vigilance s'applique aux négociations relatives à la gouvernance d'internet qui se déroulent notamment au sein de l'ONU (UIT en particulier).

S'agissant des grandes plateformes, la question de leur domination se pose. Leurs ressources, qui dépassent le PIB de certains Etats, leur offre de nombreuses possibilités qui pourraient, à terme, remettre en cause la souveraineté des Etats. **Ces plateformes possèderont bientôt la majorité des câbles. Je n'exclue pas des tensions entre les Etats et ces plateformes.** Elles sont aujourd'hui sous-jacentes dans les régulations que les Etats, en particulier l'Europe, entendent imposer. Une Europe numérique forte est une nécessité, car **les plateformes pourraient profiter de l'opposition USA/Chine pour marquer encore davantage leur territoire.**

5/ Après avoir été bercé d'illusions par le récit du

village global, nous nous réveillons devant le spectacle d'un monde hostile, divisé, et soumis aux règles tacites de la prédation. En tant que nation, comment, à chaque échelon, agir "en bon père de famille" ?

Il faut que la culture de cybersécurité soit partagée par tous, quel que soit le niveau de responsabilité. La formation est un enjeu majeur pour la prochaine décennie. Aucun diplôme d'Etat, ou reconnu par lui, ne devrait être décerné sans un socle minimal de connaissances. Je crois en un internet sûr et libre s'appuyant d'abord sur les individus. Il faut leur garantir une souveraineté numérique, c'est-à-dire une maîtrise de leurs données qui conditionnent leur sphère d'intimité, de liberté. Les citoyens ne peuvent être protégés si les personnes morales (entreprises, collectivités territoriales, services publics, associations, etc.) ne le sont pas elles-mêmes. Comment le seraient-elles si l'Etat n'est pas souverain, lui qui est le garant de la défense et de la sécurité nationales ? **L'Etat, lui-même, ne peut être fort que dans une Europe qui doit faciliter la construction d'une « tortue romaine » qui harmonise des standards de cybersécurité élevés, partagés par tous les Etats membres.** Cette présentation, par emboitements successifs, me semble de nature à fixer les responsabilités de chacun, à mettre en évidence les interdépendances. Elle le mérite de replacer l'humain au cœur de sa cybersécurité ; elle met en exergue la nécessité de développer une cybersécurité collective et collaborative. Nous gagnerons ensemble ou serons défaits dans la solitude.

6/ La numérisation croissante du monde ouvre la porte à la multiplication des menaces imaginables. Considérez-vous que le monde physique peut – ou doit rester – notre point d'ancrage ?

Une chose est acquise : la transformation numérique n'est pas réversible. Elle va au contraire s'accentuer, sauf à être freinée par des exigences environnementales ou par

l'inacceptabilité sociale de nouvelles technologies. Pour autant, **il faut demeurer « les pieds sur terre » en renforçant notre cyberrésilience.** Celle-ci doit veiller à ne pas nous placer dans une dépendance extrême, à poursuivre des activités essentielles sans numérique, pendant toute la durée d'une perturbation. **Le monde physique n'est pas remis en cause par le numérique qui est un « substrat » qui l'irrigue, l'innerve.** Il n'y a pas d'antagonisme ; les deux doivent se conjuguer. Le numérique doit nous permettre de mieux aménager le monde physique, de mieux le protéger. D'où l'importance de la convergence de la transformation numérique et de la transition écologique.

7 / Vous avez fondé le FIC. Que lui devons-nous depuis sa création ?

Je ne peux pas être juge et partie…J'espère qu'il a contribué à éveiller les consciences. Le FIC n'est pas seulement un espace propice à l'échange sur les solutions de cybersécurité. **C'est aussi un lieu de réflexion où la réponse à la question « pourquoi ? » est aussi importante que celle à la question « comment ? ».** Le FIC est d'abord un état d'esprit, une manière de partager une vision du numérique s'appuyant sur des valeurs communes. Il est très important qu'il soit fréquenté aussi par des juristes, des sociologues. La présence croissante d'étudiants, d'enseignants, de chercheurs atteste aussi de sa portée « pédagogique », tant les contenus sont d'une grande richesse.

Le modèle du FIC est désormais « exporté ». En novembre, avec les Canadiens nous inaugurerons le FIC « Amérique du Nord ». Nous avons d'autres ambitions « planétaires ». Le soutien de l'Europe, que j'avais obtenu grâce au regretté Jacques Barrot, ancien commissaire européen, est stratégique. Si l'Europe veut que sa voix porte, elle doit se tourner aussi vers le reste du monde. Le FIC est un formidable outil de rayonnement pour elle.

A l'échelon national, je note que les autorités politiques sont de plus en plus assidues, car c'est un lieu idéal pour exposer une vision. **Nous espérons un jour avoir la visite d'un Premier ministre, voire du Président de la République.**

8/ Que vous inspirent les perspectives d'une future hybridation de l'humain et de l'électronique, par voie d'implants, de prothèses etc ? Le lien entre ces deux mondes facilitera-t-il la tâche des garants de la cybersécurité ou cela la rendra-t-elle beaucoup plus ardue ?

La question est existentielle ! Elle dépasse le champ de la cybersécurité parce qu'elle concerne nos corps, nos cerveaux, nos « âmes ». Tout reposera, me semble-t-il sur une éthique forte. Quelles limites ne doivent pas être dépassées ? « Science sans conscience n'est que ruine de l'âme », écrivait Rabelais. Il n'y a pas de conscience sans connaissance, ce qui ne ramène à l'acculturation partagée que j'évoquais précédemment. On peut espérer des progrès de la médecine grâce à des objets connectés, mais il faudra à chaque fois s'interroger sur la finalité, sur la protection des données médicales qui figurent parmi les plus sensibles. **Esclaves mais en bonne santé, telle est la question faustienne qui mérite d'être posée.** Les transhumanistes nous annoncent un monde idéal, celui de la quasi-éternité pour les humains « augmentés ». Mais qui sera augmenté ? **Je crains une société qui ne s'intéresse qu'aux « utiles » et abandonne les plus faibles dans leur condition de mortels.** Yuval Noah Harari, dans son livre Homo Deus, une brève histoire de l'avenir, nous annonce une population divisée en deux catégories : les humains augmentés formant une élite, les humains ordinaires, inutiles et dépassés, n'ayant aucune fonction économique et sociale.

Sans aller vers cet extrême (Google y travaille avec Ray Kurwell…), nous devons commencer par la réflexion éthique qui est conditionnée par la cybersécurité du système envisagé.

9/ La ménagère de moins de 50 ans ne serait-elle victime que d'un sentiment de cyber-insécurité, comme on l'entend dire parfois avec un brin de moquerie de l'insécurité ?

Je ne me moque jamais des personnes qui évoquent un sentiment d'insécurité. Elles attendent d'être rassurées, faute de quoi tous les imaginaires sont possibles. Le sentiment devient un ressentiment. Dans le domaine de la cybersécurité, la difficulté tient au caractère invisible, impalpable des manifestations de la cybercriminalité ou de l'emprise exercée via le contrôle de nos données. Il faut d'abord tenir le bon discours et éviter la paranoïa que certains alimentent pour mieux vendre leurs solutions. Mais il faut aussi éviter d'être naïf. Le cyberespace est porteur de dangers, mais nous pouvons ensemble les conjurer. **Churchill disait qu'on « ne devait jamais tourner le dos à un danger pour tenter de le fuir. Si vous le faites – ajoutait-il-, vous le multipliez par deux. Mais si vous l'affrontez rapidement et sans vous dérober, vous le réduirez de moitié ».**

10/ Doit-on s'étonner que notre pays, qui a laissé tomber l'éducation civique et le service militaire, soit le terreau de petits génies du malware et de Mozart du ransomware ?

Notre pays n'a pas le monopole des « petits génies du mal ». J'ai cru comprendre que les virtuoses opéraient davantage depuis quelques Etats qui ferment les yeux ou les encouragent.

Mais votre question souligne peut-être le fait que nous ne savons pas capter et orienter les talents, y compris lorsqu'ils n'ont pas d'intention malveillante. Il est indispensable de faire naître chez tous une « conscience citoyenne ». Cela veut dire que les prescripteurs doivent être capables de faire passer les messages, de donner l'exemple. Cette citoyenneté passe notamment par un comportement irréprochable sur les réseaux sociaux où le pire côtoie le meilleur. Le service militaire a une autre vocation que celle

de former des cybercitoyens. C’est à l’école, dans la famille que tout commence. Vaste programme !