La cyber criminalité

Menaces économiques et sociétales

Excelia Group – 17 et 18 octobre 2018 (La Rochelle)

Synthèse

Pierre Berthelet

docteur en droit, spécialiste en sécurité et auteur de securiteinterieure.fr

Cette première édition du colloque organisé dans le cadre du mois européen sur la cybersécurité s'est avérée être très enrichissante. Elle témoigne de l'intérêt des participants pour une question devenue un enjeu sociétal majeur. De prime abord, la cybersécurité correspond à un thème mal défini. Au vu de la diversité des sujets abordés, elle apparait en effet comme un concept malaisé à cerner. Elle s'apparente à un vaste fourre-tout, allant de la fraude à la résilience en passant par l'analyse de la valeur et la certification. D'ailleurs, la lecture du programme est, toujours à première vue, déconcertante eu égard à la multitude des thématiques évoquées. Pourtant, ce désordre n'est qu'apparent, et il existe une véritable cohérence du sujet. Il est même possible d'aller plus loin en considérant qu'il existe un vrai cheminement logique permettant de progresser dans l'analyse au fil des différents ateliers.

À ce propos, il est possible d'identifier trois thèmes majeurs :

- La cyberattaque,
- La cyberprotection,
- La cybervulnérabililté.

À cet égard, ces trois thèmes peuvent être couplés, donnant lieu à deux axes d'analyse :

- La sécurité nationale d'un côté (cyberattaque et cyberprotection)
- La sécurité sociétale (cyberprotection et cybervulnérabililté)

La sécurité nationale d'abord. C'est le thème des tables rondes du 17 octobre après-midi. Le constat dressé par divers intervenants a trait à la variété des menaces. Il n'y a pas un type de cyberattaques mais divers types. Il n'y a pas une catégorie de cyberattaquants, mais de multiples catégories. Ce peut être le petit escroc qui, au moyen de faibles outils et aux connaissances modestes, s'approprie indument des données à caractère personnel. Ce peut être le hacker chevronné qui, pour le compte d'un État ou d'une organisation criminelle, s'introduit dans des systèmes hautement sécurisés.

Un élément largement partagé par les divers intervenants porte sur la difficulté d'établir une catégorie précise des menaces : militaire, terroriste, criminelle etc. Relevant du champ des « nouvelles menaces » les cybermenaces se caractérisent par leur caractère furtif et

évanescent. La difficulté concerne d'ailleurs l'imputation des cyberattaques. S'ensuit un jeu d'attribution entre la cybervictime (un État occidental qui va rapidement accuser la Russie par exemple), le cyberattaquant (la Corée du Nord qui va brouiller les pistes en laissant des indices faisant penser à une menace iranienne) et des tiers (par exemple Daesh qui, de manière opportuniste, va revendiquer une attaque qui n'est pas de son fait).

Côté cyberprotection, le commentateur ne manquera pas de souligner que la gamme des mesures déployées est particulièrement large, celles-ci allant de la prévention à la résilience en passant par la protection proprement dite (par exemple le renforcement des systèmes par la mise en place de patches correctifs). Au-delà du caractère technique des mesures instaurées, il est possible de considérer une évolution de la cybersécurité. C'est la métaphore du château-fort *versus* celle de l'aéroport. Jadis, la sécurité consistait à « fermer la porte », c'est-à-dire sécuriser physiquement son système informatique, dans le but d'empêcher que des indésirables ne pénètrent la salle. C'est la sécurité informatique. Cette vision de la sécurité « château-fort » se retrouve actuellement dans certains discours relatifs à la menace migratoire ou terroriste : renforcer les contrôles frontières, verrouiller les entrées, se barricader pour empêcher tout mouvement. Cette solution fait référence à la citadelle encerclée.

À présent, les systèmes sont connectés et la cybersécurité doit se réaliser de manière différente, à l'image de l'aéroport : mettre en place différents points de contrôle, ayant des fonctionnalités différentes. Il s'agit non pas d'empêcher les flux, mais au contraire de les laisser passer (par exemple les données), tout en surveillant et en filtrant. Tout l'enjeu consiste à détecter les éléments dangereux, facteurs de risques, ainsi que des sources de désordre de nature à altérer ces flux. C'est la sécurité au sens où l'avait entendu par le philosophe Michel Foucault.

Dans cette perspective, tous les acteurs de la sécurité sont mis à contribution : le secteur privé en premier lieu, mais aussi les institutions internationales et l'Europe. L'image de Blanche neige avait été évoquée de manière judicieuse. Les sept nains (les États membres) ont déployé des dispositifs de cybersécurité, tandis que l'Union européenne jouait le rôle de la belle endormie. Un élément d'explication pourrait être que les compétences de l'UE se limitaient à un volet économique au début des années 2000 (l'approfondissement du marché intérieur). Or, suite aux attaques terroristes et aux menaces dites « dyssimétriques et transnationalisées », le retour à l'Etat a été préconisé par de nombreux experts et décideurs. À l'époque, il faut se rappeler que l'Internet opposait deux camps ayant deux visions diamétralement opposées : les libertaires qui concevaient le net comme une utopie au sens de Thomas More : un nouveau continent sans règles, hors de tout contrôle étatique, destiné à permettre à tout un chacun de s'accomplir à l'abri d'un pouvoir politique régalien jugé omnipotent et liberticide, et de l'autre les partisans d'une sécurité accrue, qui voyaient le net comme un espace sans foi ni loi, un *far west* où proliféraient terroristes, pédophiles et trafiquants. Finalement, cette deuxième approche semble l'avoir emporté au fil du temps, l'idée d'une régulation s'imposant progressivement. Or, il était délicat pour l'Union, de venir défier les États, politiquement et juridiquement, dans un domaine revendiqué par eux au nom de leur souveraineté qu'ils revendiquent sur le net. Il est vrai que, au nom d'une régulation

transnationale, l'intervention de l'Union a été souhaitée désormais par ces mêmes États, amenant ainsi à se questionner sur les contours de la sécurité nationale, mais ces interrogations ne doivent pas occulter l'importance du deuxième volet, à savoir la sécurité sociétale. Ce type de sécurité met en évidence l'importance des citoyens comme membres de la collectivité.

À ce sujet, il faut distinguer :

- La cybervulnérabililté qui renvoie à la difficulté de l'intégration des plus fragiles. Il s'agit traditionnellement des publics socialement modestes. De nombreuses interventions soulignent le défi actuel d'inclure ces publics et de faire en sorte qu'Internet soit un outil (parfois au-delà de la dimension ludique). Un point important mis en évidence est que 13 millions de Français ne possèdent toujours pas d'identité numérique. Un autre point a trait quant à lui aux aînés. Jadis sources de sagesse et dépositaires d'autorité, ceux-ci sont relégués au rang de public en difficulté, voire d'analphabètes qu'il convient d'éduquer. Étrange inversion dans l'échelle des valeurs occidentales… Quoiqu'il en soit, ces publics en marge, au-delà de la variété de leurs profils, présentent certains traits communs, notamment, leur méconnaissance des fonctionnalités des outils informatiques et celle des dangers du net. Ceux-ci se révèlent particulièrement vulnérables et requièrent, à ce titre, une cyberprotection accrue, ce qui permet de mentionner le point suivant ;
- La cyberprotection fait écho à toutes les personnes utilisatrices du net mais qui, à un moment donné ou un autre de leur vie, ont été victimes de cybercriminels. Cet aspect mérite d'être développé car il est un point central de ce colloque.

La plaquette indique : « tous complices, tous victimes ». Cette formule a bien été expliquée par les différents intervenants : tous complices, car il appartient aux personnes ayant connaissance d'une cyberattaque, qui, il faut le rappeler, est un acte délictueux, de la dénoncer aux autorités, notamment via un site dédié (*Cybermalveillance*.*gouv*.*fr*). « Tous victimes » : la difficulté soulignée par certains intervenants a trait au fait, pour une personne victime de ce type d'actes, d'en parler et de se confier : soit elles sont dans le déni (ou la minimisation), soit elles se trouvent dans la honte.

Or, le fait que les cyberattaques touchent des personnes « lambda » (ou des PME/TPE) apparaît comme une tendance de fond. Alors que bon nombre de structures (par exemple les structures d'importance vitale) sont largement sécurisées, les cyberattaquants tendent de plus en plus à se focaliser sur les maillons les plus vulnérables : les entreprises mal protégées et les citoyens insouciants des risques du net. Un intervenant de Pôle emploi a révélé que bon nombre de connexions sur le site venant du Bénin : des cyberescrocs tentent en effet de soutirer des données à caractère personnel des demandeurs d'emploi en abusant de leur naïveté (par exemple en leur faisant miroiter une promesse d'embauche à la condition de renvoyer certaines données à caractère personnel).

En tout état de cause, la cyberprotection renvoie à l'importance de la prise de conscience du public du fait qu'il est acteur de la cybersécurité. Les ateliers du 18 octobre au matin ont mis en évidence trois volets largement imbriqués :

1. La vigilance. Le danger mis en évidence est celui concernant l'utilisateur lui-même. C'est l'image de la maison sécurisée (hautes haies, caméras de vidéosurveillance, porte d'entrée renforcée) mais dont la fenêtre donnant directement sur la rue reste toujours grande ouverte). Les chiffres mentionnés par le service informatique d'Excelia sont glaçants : 60% des étudiants ont leur ordinateur infecté. En outre, une expérience a été menée par ce même service : un mail de phishing a été envoyé au personnel et il s'avère que, en cinq minutes, plusieurs membres ont « mordu à l'hameçon » contaminant ainsi (de manière simulée rappelons-le) tout le système informatique de l'école. Un autre intervenant a déclaré que « si vous pensez que votre ordinateur n'est pas infecté, c'est qu'il l'est déjà, mais les pirates se sont arrangés pour que vous n'en n'ayez pas conscience ». Enfin, une illustration a été reportée par un autre intervenant encore : un service informatique a infecté malencontreusement la sauvegarde du serveur de l'entreprise (c'est-à-dire le double du serveur principal), car il avait bêtement oublié de le déconnecter du serveur principal ayant été entretemps attaqué et rendu inopérant, mettant de ce fait en péril la pérennité de l'entreprise tout entière. L'enjeu porte donc sur l'éducation et l'éveil des consciences : à l'utilisateur de ne pas avoir des comportements à risque (brancher un clé USB inconnue sur son ordinateur) et à l'entreprise de mettre en œuvre de manière diligente une série de mesures de précaution (par exemple en acquérant uniquement des produits certifiés) ;
2. L'identité numérique. Chaque citoyen qui possède son identité, doit en prendre soin. Comme il n'est pas pensable qu'un individu donne spontanément ses papiers d'identité ou des photos intimes à un inconnu, il doit avoir un comportement identique sur le net. Un aspect important mis en évidence est la sensibilisation et la prise de conscience. Différents dispositifs sont mis en place (par exemple des gendarmes référents sur ce thème) ;
3. La responsabilisation. Un assureur n'ira pas assurer la maison d'un individu qui a oublié de fermer sa porte à clé. Le juge tend, lui aussi, à ne plus accepter certains comportements négligents sur le net. Il est désormais attendu que tout un chacun se montre vertueux, et même exemplaire : l'envoi de photos de vacances à ses « amis » sur Intagram montre aux cambrioleurs que l'habitant n'est pas présent. L'étalement sur Facebook d'un intérieur somptueux révèle aux voleurs que l'auteur du compte possède un mobilier de valeur. Un bon délinquant n'est pas forcément celui qui aura un doctorat en informatique, mais celui qui aura su collecter habilement le plus d'informations sur une personne, informations que celle-ci a contribué à diffuser au plus grand nombre !

Au final, il est possible de se rappeler la formule d'un texte de loi : la sécurité est affaire de coproduction. Il est permis, pour clore ce colloque, de considérer que cette co-production passe par l'individu lui-même, qui est un acteur incontournable de la cybersécurité : celle-ci est son affaire, notre affaire à tous. Je vous remercie pour votre attention.