Cybersécurité, l'urgence absolue

La cybercriminalité est la « criminalité du XXIème siècle », thème du 1er Forum International de la cybersécurité (FIC), en 2007. A l'époque, peu de décideurs prenaient la question au sérieux. Aujourd'hui, elle est le fléau qui menace non seulement les personnes physiques et morale - avec le risque pour les entreprises de ne pas se relever après une cyberattaque - mais aussi les Etats.

Marc WATIN-AUGOUARD,

Chef de la Majeure « Souveraineté numérique et Cybersecurité à l'IHEDN

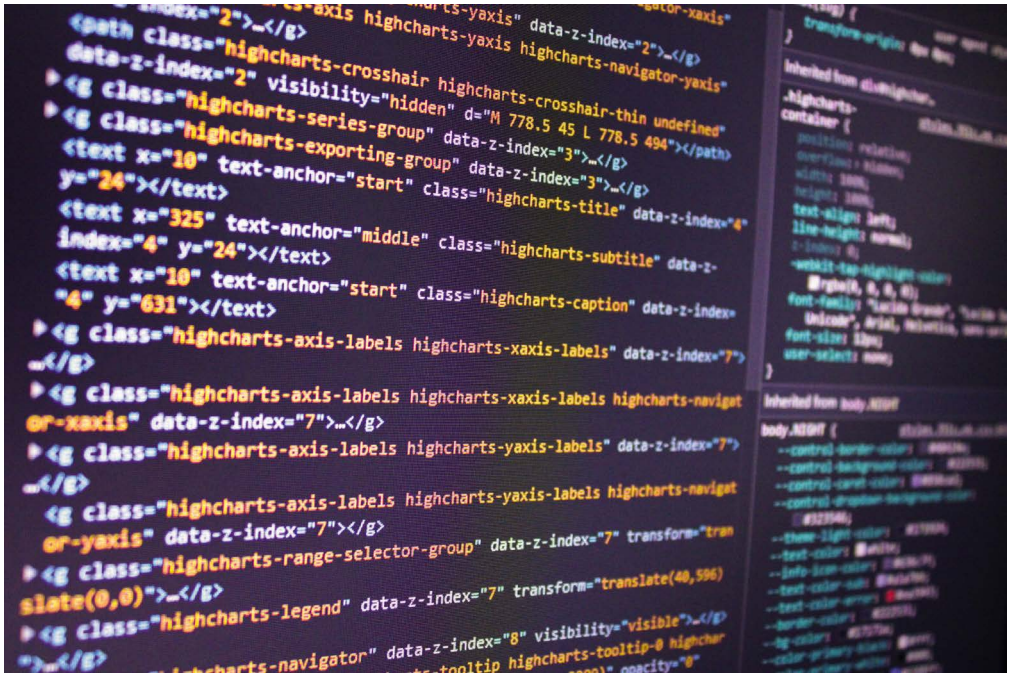
Pour comprendre cette évolution, il faut observer la « tectonique des plaques ». La cybercriminalité est le fruit d'un double mouvement : la migration des délinquants vers le cyberespace s'accompagne d'une migration des Etats et d'organismes paraétatiques qui le pénètrent pour mener des actions « infra-guerre » ou pour accompagner leurs actions de guerre cinétique par des opérations cybernétiques.

Le délinquant est généralement plus intelligent qu'on ne le pense. Agir dans le cyberespace offre pour lui le meilleur rapport avantage/risque pénal. Jamais il n'a été aussi près de sa victime ; jamais il n'a été aussi loin de son juge ou de son gendarme, car il peut agir à distance, depuis un Etat « cybervoyou » qui ne coopère pas ou, pire, encourage les prédateurs.

La deuxième migration vient de certains Etats peu respectueux du droit international ; elle rejoint la première. Jadis, les Etats avaient recours à la force pour s'en prendre à un autre Etat. C'était la politique de la canonnière. Aujourd'hui, sans renoncer à la force, ils trouvent dans l'espace numérique un terrain propice à des actions masquées, en dessous du seuil de l'agression armée, qu'ils confient le plus souvent à des cybercriminels en groupe organisé agissant pour leur compte, afin de mieux brouiller les pistes. S'ils ne sont pas pris, ils reçoivent le salaire de leur turpitude. Dans le cas contraire, l'Etat déclare les ignorer et promet une action vigoureuse venant de lui qui, comme il l'a toujours affirmé, met tout en œuvre pour lutter contre la cybercriminalité. Si les images de certaines arrestations s'arrêtent devant la porte de la prison, il est établi qu'il existe une sortie donnant accès aux services secrets. La règle de la « diligence due » qui impose à un Etat de ne pas tolérer une action hostile depuis son territoire est ici bafouée.

Cette tendance lourde devrait s'accélérer, la cybercriminalité s'inscrivant dans une zone grise, hybride. Si l'Etat n'accentue pas sa stratégie d'action, notamment avec l'augmentation sensible de ses capacités d'investigation et de poursuite des prédateurs, le risque est grand de voir sa légitimité remise en cause, car sa première justification est de protéger les personnes physiques et morales et les biens matériels et immatériels.

Dans le « monde réel », la sécurité relève essentiellement de la puissance publique. Dans l'espace numérique, en revanche, l'Etat doit composer



avec de nombreux acteurs privés qui possèdent une part importante de la réponse, ne serait-ce qu'en raison de leur connaissance de la menace et de leurs offres de cybersécurité. Par les capteurs qu'ils déploient ou les systèmes basés sur l'IA qu'ils mettent en œuvre, ils ont une vision en temps réel des cyberattaques et des comportements dont ne disposent pas les ministères régaliens. Le partenariat public-privé est parfaitement illustré par l'écosystème israélien, à Be'er Sheva, ville ayant poussé dans le désert du Néguev. Y sont rassemblées des universités, des centres de recherche, des startups, des entreprises du numérique, des acteurs étatiques (armée, police). C'est sur ce modèle que se créent, en France, les Campus Cyber, dont le premier vient d'ouvrir ses portes sur l'esplanade de la Défense. 1800 acteurs publics et privés, civils et militaires se croisent, se rencontrent, partagent leur expérience de la cybersécurité. Le partenariat public-privé est aussi l'une de motivations de la création du FIC en 2007. Mais cette manifestation, la plus importante en Europe et qui s'implante au Canada (FIC Nord Amérique), est aussi un lieu où s'exprime la volonté de développer la coopération internationale. Sans elle, point de salut ! Comment, en effet, lutter contre un phénomène transfrontalier en limitant son champ d'action à l'intérieur des frontières ? Europol, agence européenne de coopération, marque des points, chaque fois que plusieurs états mettent en commun leur renseignement et leurs capacités d'investigation.

A supposer que tout l'arsenal public et privé soit en ordre de bataille, cela ne suffirait pas pour permettre de sécuriser une « métamorphose numérique » qui n'en est qu'à ses balbutiements. Avec l'hyperconnexion qu'annoncent la 5G puis la 6G, il faut désormais résonner de manière systémique, en construisant une cybersécurité collective et collaborative. Les territoires (départements, régions) retrouvent une raison d'être, dans un monde numérique apparemment sans frontière. Parce qu'ils rassemblent des acteurs qui se connaissent, ils peuvent être ces espaces d'échange et de solidarité sans lesquels il ne peut y avoir de résilience.

La cybersécurité, c'est d'abord un état d'esprit, une conscience partagée, avant d'être le résultat de technologies. Au sein des institutions, des entreprises, des collectivités territoriales et des services publics qui leur sont rattachés, la cybersécurité ne doit pas être le monopole des spécialistes (DSI, RSSI, directeurs de la sûreté, etc.). Chacun est concerné, en commençant par le COMEX qui doit désormais hisser la question au niveau stratégique. La question n'est pas de savoir si on va être attaqué, mais quand ? Cela signifie qu'il faut anticiper,

planifier l'organisation de la gestion de crise cyber à venir.

Le coût de la cybersécurité est parfois présenté comme un obstacle, eu égard au coût exorbitant d'un RSSI, d'un centre de supervision (SOC), d'un EDR, même si la mutualisation peut souvent apporter une réponse. Est aussi invoqué le coût de l'assurance cyber. Ces arguments ne doivent pas être balayés, car ils constituent un obstacle pour beaucoup d'entités.

En vérité, si l'on considère que 85% des incidents sont d'origine humaine, c'est l'acculturation de tous au risque cyber qui est sans doute la mesure la moins coûteuse et donc la plus accessible. La gendarmerie nationale multiplie les actions de sensibilisation. La DGSI en fait de même au profit d'entreprises sensibles. Il faut aller encore plus loin pour développer une conscience partagée sur le risque cyber qui ne concerne pas seulement les autres. Toute personne, toute entreprise, toute administration connectée est une cible potentille, surtout si elle offre une faible défense. Les collectivités territoriales, les hôpitaux ont cru à une protection absolue du fait de leur mission de service public. On mesure aujourd'hui le résultat !

Dans le monde réel, nous avons la chance de compter sur les pompiers en cas d'incendie, sur des policiers et gendarmes pour arrêter les délinquants. Mais cela n'interdit pas- au contraire – de développer une politique de prévention mise en œuvre à titre individuel et collectif. Il ne viendrait à personne l'idée de jeter un mégot allumé dans sa corbeille, de laisser sa porte ouverte à tous vents. Pourtant, c'est ce qui arrive trop souvent encore dans notre utilisation de l'outil numérique. Comme le souligne l'Agence nationale pour la sécurité ses systèmes d'information (ANSSI), la première démarche est d'adopter une « hygiène informatique » qui évite bien des déconvenues.

Finalement, sans négliger l'apport des technologies, la cybersécurité est d'abord l'agrégation de nos comportements. Il est donc urgent de replacer l'humain au cœur de la cybersécurité. ■