Introduction
Répondre à la menace cyber

Par **Côme BERBAIN**
Directeur de l'innovation et du véhicule autonome,
RATP

La vision commune de la menace cyber est aujourd'hui largement déformée. Hollywood s'est emparé il y a de nombreuses années du personnage du hacker : jeune homme blanc en sweat à capuche capable, à l'aide d'outils semi-magiques de contrôler les machines et de plonger le monde dans l'apocalypse, en arrêtant la production d'énergie d'un pays, en effaçant les données des banques ou en diffusant massivement de fausses informations. Dénué de la moindre conscience de ses actes, il est le plus souvent manipulé par un autre personnage, finalement plus humain car ses intentions sont plus compréhensibles.

Rien n'est à la fois plus loin de la réalité en ce qui concerne les intentions et les méthodes, et plus réaliste dans les conséquences potentielles. La transformation numérique à l'œuvre rend nos vies et nos sociétés dépendantes de données et de systèmes informatiques de plus en plus connectés et de plus en plus ouverts : que l'on pense aux comptes bancaires, aux hôpitaux dont les ordinateurs contiennent la seule trace de la liste des traitements à fournir chaque jour aux patients ou à la ville dont l'ensemble de l'éclairage est pilotable depuis un smartphone. Cette ouverture est source d'innovations qui font évoluer conjointement les technologies et les usages, eux-mêmes générateurs de nouvelles innovations dans des cycles rapides liés à la compétition internationale des États et des entreprises. Cette vitesse laisse bien peu de place à la maturation des technologies et à la compréhension fine des enjeux, ce qui pose un défi permanent en termes de régulation et de sécurité.

La sécurité de ce nouveau monde n'est pas une problématique entièrement nouvelle : elle s'inscrit au croisement des traditions historiques de la sécurité de l'information et des transmissions, du contre-espionnage et de la contrepropagande. Elle prend cependant une importance particulière en raison de l'étendue du champ d'action, de l'immaturité de la très grande majorité des entités publiques ou privées aussi bien sur les aspects techniques qu'organisationnels, et de la grande accessibilité des techniques offensives.

La cybersécurité, dont il est question dans ce numéro, est une des composantes de cette sécurité numérique. Elle s'attache à protéger les données et les systèmes d'information, à garantir leur confidentialité, leur intégrité, leur authenticité et leur disponibilité. Bien que reposant sur un substrat technique, elle intègre également les aspects humains, aussi bien individuels que collectifs. Il est fréquent d'entendre que la principale vulnérabilité d'un système informatique se trouve « entre la chaise et le clavier ».

Elle diffère néanmoins de la question de la protection des données personnelles ou de la manipulation des algorithmes ou des informations : la collecte illicite de données n'implique pas nécessairement la violation d'un système d'information particulier ; la diffusion de fausses informations sur un réseau social tel que Twitter relève du fonctionnement normal de ce réseau et ne nécessite pas d'attaquer les serveurs de Twitter. Cependant, ces questions ne sont pas sans liens et ces dernières années ont vu apparaître des attaques combinées d'une grande sophistication.

Ce numéro vise à présenter l'état de la réflexion et des évolutions en cours en matière de cybersécurité, au plus proche du terrain et des acteurs qui la pratiquent au quotidien, et bien loin des visions romancées. Il cherche à donner des clés de compréhension concrètes et des leviers actionnables aussi bien pour le citoyen, l'employé ou le décideur autour de plusieurs dimensions :

- « Voir et comprendre ». Il est difficile de se défendre contre un ennemi invisible. Si la médiatisation des attaques progresse autour de quelques cas emblématiques (TV5monde, Saint-Gobain, Airbus…), la majorité des victimes recherche la discrétion. La détection d'attaques reste l'indispensable première étape de la cybersécurité. Il est également nécessaire de comprendre la diversité des motivations, de la cybercriminalité des groupes mafieux aux actions prêtées aux Etats, ainsi que le caractère aussi bien local que systémique, de l'attaque ciblée d'un individu aux scénarios d'« ouragans cyber ».
- Le nécessaire équilibre entre prévention et réaction : à partir de la prise de conscience de la menace réelle, la tentation principale consiste à focaliser ses moyens sur la réaction, d'autant plus qu'il s'agit d'activités valorisantes. Cependant, à l'instar des risques incendies ou des risques industriels, ce seul travail ne peut suffire. Le long travail de standardisation et de certification des solutions, de sensibilisation et de formation des acteurs, et d'organisation et de régulation de l'écosystème, est nécessaire pour éviter que les « pompiers » cyber ne s'épuisent dans une course où l'attaquant possède toujours l'initiative et un avantage naturel, détruire étant toujours plus simple que construire ou réparer.
- Le dépassement de la technique : la complexité technique du sujet ne doit pas cacher les enjeux et les problématiques non techniques. Déjà entamée ces dernières années, l'intégration des questions de formation, d'organisation et de régulation doit venir se compléter de réflexions plus globales sur le rôle des États, la responsabilité des principaux acteurs numériques, les comportements des acteurs privés, les modalités et les périmètres de la régulation, ou encore l'adaptation à la cybersécurité d'activités existantes comme la justice.

Pour cela, ce numéro expose en premier lieu l'état de la menace, les motivations des acteurs et les enjeux de la détection, avant de présenter la palette de réponses possibles apportées aussi bien par le secteur public (État, Union européenne) que par le secteur privé. Compte tenu de l'enjeu de sécurité, l'État a naturellement investi le champ de la cybersécurité, aussi bien pour apporter une réponse aux attaques les plus importantes que pour fixer aux niveaux national et européen le cadre de la régulation des activités les plus essentielles au fonctionnement de notre société, ainsi que pour ses besoins propres. Aidé par quelques exemples fameux d'attaques qui sont aujourd'hui de plus en plus médiatisées, ce cadre a permis le développement du secteur privé, aussi bien dans les startups que dans les grands groupes, sous forme de produits, de services ou d'assurances. Dans ce domaine, la France reste dans la course mondiale et participe activement à la définition des cadres européens dont les détails auront des impacts de long terme sur la compétitivité de notre industrie.

Enfin, ce numéro évoquera les nouveaux enjeux de la cybersécurité : des défis techniques apportés par l'intelligence artificielle, le *cloud* ou les objets connectés mais aussi les défis de régulation des comportements des grands acteurs numériques ou des États.

Très bonne lecture !