Le modèle français de cybersécurité : priorité à la défense

Par **Guillaume POUPARD**
Agence nationale de la Sécurité des Systèmes d'information (ANSSI)

L'année 2019 marque la dixième année d'existence de l'Agence nationale de la Sécurité des Systèmes d'Information, l'ANSSI. Dix ans qui ont contribué à implanter durablement l'Agence dans l'écosystème français, européen et international de la cybersécurité. Dix ans aussi durant lesquels la menace numérique n'a cessé de croître, de s'adapter pour se faire toujours plus présente. Dix ans, enfin, qui ont permis de confirmer la pertinence du modèle français et le choix, audacieux, de ne pas cantonner la cybersécurité à un secteur tout en séparant strictement les activités défensives, confiées à l'ANSSI, des activités cyberoffensives.

Plus de dix ans après l'impulsion initiale, la cybersécurité est devenue une priorité stratégique majeure pour de nombreux États. C'est ainsi qu'on assiste, au niveau mondial, à la consolidation d'un « premier cercle » de puissances cyber, composé sans surprise des États-Unis, du Royaume-Uni, de la Chine, de la Russie et d'Israël. La dimension numérique est désormais pleinement intégrée dans les stratégies d'influence, d'ingérence ou de découragement des puissances étrangères. Le cyberespace est marqué par une montée des tensions, donnant lieu à une instabilité croissante, servies par des stratégies résolument offensives et, parfois, à visées hégémoniques.

Dans ce contexte, la France demeure une puissance cyber. Sa stratégie audacieuse lui a permis de rapidement développer des capacités autonomes. Elle reste l'une des rares nations capables de faire entendre une voix indépendante, équilibrée et forte, dans les instances européennes et internationales.

Cette place singulière tient pour beaucoup à son modèle d'organisation, qui nous a permis d'accompagner l'évolution de la menace tout en rendant possible le déploiement d'une véritable politique publique de la cybersécurité, condition d'une transformation numérique en confiance.

Une menace en constante évolution

C'est le quotidien du défenseur – plus généralement de quiconque évolue dans la gestion des risques – que d'être perçu comme un empêcheur de tourner en rond. On lui demande parfois d'arrêter de jouer les Cassandre (oubliant par ailleurs que celle-ci ne se trompait jamais). On lui reproche parfois de noircir le tableau ou de verser dans le catastrophisme pour précipiter une prise de conscience, voire justifier sa raison d'existence. Mais si le défenseur est condamné à parler au conditionnel, c'est bien pour ne pas avoir à parler au passé.

Nul besoin de grossir le trait en effet : l'activité de l'ANSSI ne cesse de démontrer que la menace numérique est tout sauf virtuelle, que les défis pour la sécurité du cyberespace restent immenses. Pour cause : la menace numérique est entrée dans une dimension nouvelle. Les attaques informatiques sont plus sophistiquées, mieux élaborées, plus destructrices. Elles touchent désormais toute la société, du citoyen à la grande entreprise jusqu'à nos institutions démocratiques. À la faveur d'une explosion des usages et d'une externalisation toujours plus importante, la surface d'attaque ne cesse d'augmenter, sans que cela ne se traduise mécaniquement par un accroissement de la sécurité – loin s'en faut.

Une recrudescence des attaques « par rebond »

Dans un environnement globalisé, synchronisé, externalisé, dans lequel les flux sont devenus tout aussi physiques que numériques, l'interdépendance croissante des acteurs expose chacun d'entre eux à la défaillance d'un des membres de leur écosystème. En cela, la *supply chain* – comprendre les liens de sous-traitance et d'externalisation entre les acteurs – constitue tout à la fois un puissant moteur de performance pour les entreprises et les administrations, mais également un véritable défi pour la sécurité du numérique.

Les attaquants l'ont bien compris. Ils exploitent désormais cette fragilité à leur profit, visant d'abord les prestataires d'entreprises pour atteindre leurs cibles principales. Cette tendance, particulièrement prégnante ces derniers mois, concerne notamment les entreprises de services du numérique (ESN) mais également un grand nombre de prestataires. Ces modes opératoires compliquent la mission du défenseur, qui doit surmonter les difficultés techniques et réglementaires induites par la nature de ces victimes et leur envergure souvent internationale.

Le risque (presque) nouveau du sabotage

En plus de l'espionnage numérique, qui continue de mobiliser une partie significative des ressources de l'ANSSI, les derniers mois ont été marqués par une menace nouvelle – pas tant par sa nature que par son impact potentiel : la menace du sabotage. Les conséquences humaines et économiques d'attaques de grande ampleur ou judicieusement ciblées pourraient en effet s'avérer catastrophiques. Imaginez : si vous coupez les transports en commun d'une capitale, toute l'activité économique du pays concerné pourrait être paralysée en quelques heures. Si, du jour au lendemain, les distributeurs de billets ne distribuent plus de billets, il y a fort à parier que cela donnerait lieu à d'importants troubles à l'ordre public.

Plus préoccupant encore : les infrastructures sensibles ou critiques semblent être de plus en plus ciblées par des actions de cartographie et de prépositionnement. Qu'il s'agisse d'États ou d'organisations criminelles, les attaquants s'attachent aujourd'hui à préparer les conflits ou les actions criminelles de demain. Ces attaques, dont les objectifs demeurent encore flous, pourraient constituer des opérations de reconnaissance en vue de préparer des actions de sabotage futures. Cette menace se fait plus prégnante à mesure que le contexte géopolitique se fait de plus en plus incertain.

Une prolifération des armes numériques et des vulnérabilités

La prolifération d'armes numériques et la divulgation de vulnérabilités informatiques, logicielles ou matérielles, favorisent la montée en compétence des attaquants. C'est ce qui a permis le franchissement d'un nouveau cap en 2017, avec des attaques inédites en termes d'échelle et de nocivité.

En paralysant de nombreuses entreprises, grandes et petites, mais également des acteurs comme des services hospitaliers, les attaques *WannaCry* et *NotPetya* ont démontré qu'il était possible de porter des atteintes considérables à des intérêts nationaux, sans pour autant que des infrastructures critiques soient forcément touchées. Elles obligent le défenseur à toujours élargir son périmètre de supervision, pour tenir compte d'une plus grande variété de victimes et d'attaquants. En outre, le réemploi d'outils malveillants favorise l'anonymat et complique le travail déjà délicat d'attribution par les services compétents. Les découvertes de failles critiques, matérielles ou logicielles, parfois médiatisées avant l'application de correctifs, offrent enfin aux attaquants de nouvelles possibilités d'agression plus massives et plus discrètes.

Des attaques de plus en plus lucratives

De plus en plus d'attaques ont pour finalité l'enrichissement des attaquants. Ceux-ci profitent en particulier des failles de sécurité pour compromettre un grand nombre d'équipements par le dépôt discret de « mineurs ». Il devient alors possible de se servir clandestinement de la puissance de calcul cumulée de ces systèmes pour générer des actifs de cryptomonnaies.

La préoccupation croissante des organisations à l'égard des enjeux de sécurité numérique et le renforcement parallèle de leurs capacités de défense amènent par ailleurs nombre d'attaquants à se tourner vers des cibles moins exposées, mais plus vulnérables. Ainsi, de nombreuses campagnes d'hameçonnage ciblant des collectivités territoriales ou des acteurs du secteur de la santé sont observées depuis 2018. Les objectifs de ces campagnes sont multiples mais comprennent généralement le vol de données personnelles, la demande de paiement d'une rançon après chiffrement des données, le minage de cryptomonnaies et la constitution de réseaux de machines zombies (*botnets*).

Face à cet accroissement de la menace, l'intuition stratégique française était la bonne

Cette évolution du risque numérique teste en permanence la résilience et la solidité de notre modèle de protection. Ce modèle s'organise autour d'une stricte séparation entre les activités cyberoffensives et les activités dédiées à la sécurité numérique –ces dernières étant en large partie confiées à l'ANSSI, autorité nationale à portée interministérielle.

Aux origines du modèle français

Le modèle français de cybersécurité est le résultat d'une succession de choix politiques ambitieux issus d'une prise de conscience : la transformation numérique de la société, de l'économie et de l'action publique devra se faire en confiance, ou elle ne se fera pas.

Quelques mois après l'attaque informatique majeure – la première du genre – ayant paralysé l'Estonie pendant plusieurs semaines [(1)], le *Livre blanc sur la défense et la sécurité nationale* de 2008 aboutissait à la création, en 2009, de l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), dans une visée strictement défensive et interministérielle. Cette création préfigurait un modèle original d'organisation nationale de cybersécurité, capable d'en accompagner les différents aspects.

En 2013, le nouveau *Livre blanc sur la défense et la sécurité nationale* élargissait le champ d'action de l'Agence aux acteurs privés les plus sensibles et stratégiques, dits « opérateurs d'importance vitale » (OIV). La *Stratégie nationale pour la sécurité du numérique* présentée publiquement par le Premier ministre en 2015 confirmait quant à elle l'ambition de porter une politique publique globale de la cybersécurité et de s'adresser au reste de la société, notamment les citoyens.

Enfin, les travaux stratégiques conduits en 2018 ont permis de réaliser un saut qualitatif important dans la gouvernance et le pilotage des activités de réponse aux attaques informatiques, notamment les plus sensibles. Ils ont en particulier permis d'expliciter les rôles des – désormais nombreux – acteurs institutionnels qui interviennent dans le champ de la sécurité numérique.

(1) L'attaque contre l'Estonie a en effet paralysé des activités essentielles au fonctionnement de ce pays pendant plusieurs semaines : s'appuyant sur la technique du DDoS, l'offensive a bloqué des sites Internet gouvernementaux ainsi que des médias, des partis politiques et des activités bancaires. Le gouvernement estonien avait alors accusé la Russie d'être à l'origine de l'attaque. Cette attaque a largement précipité une prise de conscience mondiale sur le risque numérique.

Contre-modèles

L'effort français en matière de cybersécurité s'inscrit dans une dynamique de développement capacitaire et de réflexion stratégique que l'on retrouve chez les autres principales puissances cyber. Ces dynamiques ont donné lieu à des organisations parfois très distinctes – le reflet d'autant de stratégies et de doctrines propres à chaque État. Certains pays, essentiellement guidés par des considérations pratiques et d'efficacité technique, tendent ainsi à regrouper les capacités défensives et offensives au sein de leurs appareils de défense ou de renseignement. C'est le cas, par exemple, des États-Unis. Le modèle américain présente l'avantage de mutualiser les compétences techniques nationales au sein d'un même pôle d'expertise, en l'espèce la *NSA*. Il pose cependant la question de l'acceptabilité, par le secteur privé, des interventions de l'État en matière de cybersécurité.

Par ailleurs, la concentration des capacités au sein des appareils militaires ou de renseignement peut rapidement déboucher sur une inclinaison naturelle à privilégier les aspects offensifs. Prenons l'exemple de la gestion des failles informatiques, qui sont recherchées par « le défenseur » à des fins de correction et par « l'attaquant » à des fins d'exploitation. La valeur de ces vulnérabilités ne cesse d'augmenter et le marché mondial connaît actuellement une forte inflation. Lorsque l'attaquant et le défenseur sont la même personne, on conçoit bien naturellement qu'il puisse être difficile de renoncer à un tel actif stratégique.

Enfin, faute de dispositif global de cybersécurité, certains pays en sont presque contraints à attaquer pour se défendre, de manière à neutraliser la menace à sa source, dans une forme de « fuite en avant » qui se traduit par des stratégies offensives préjudiciables à la stabilité du cyberespace.

Avantages du modèle français

Un peu plus de dix années après l'intuition initiale, le modèle français confirme toute sa pertinence. Mieux, il continue d'essaimer : des pays aussi divers que le Japon, Singapour, la Belgique ou Israël s'en inspirent parfois explicitement pour construire ou reconstruire leurs propres gouvernances.

Du point de vue de l'ANSSI, il présente en effet quelques indéniables avantages. À la différence d'un service de renseignement, le périmètre strictement défensif de l'Agence lui permet d'afficher une posture non ambiguë devant ses interlocuteurs, qu'il s'agisse d'entreprises ou d'administrations victimes, d'assemblées parlementaires, de chercheurs, de médias ou encore d'industriels. Ce modèle a rendu possible l'élaboration de législations très ambitieuses – souvent pionnières. Il en va ainsi du dispositif réglementaire de sécurisation des activités d'importance vitale, qui nous est envié (officieusement) par nombre de pays étrangers. Les récentes évolutions législatives ont également permis d'accroître significativement les capacités de détection de l'ANSSI ; elles sont également rendues possibles par ce modèle protecteur et rassurant.

D'autres pays ont cherché à élaborer un cadre contraignant pour leurs acteurs privés. À l'instar des États-Unis ou de la Russie, ces initiatives se sont souvent soldées par des échecs, les entreprises rechignant à collaborer activement avec les services de renseignement. Autre caractéristique propre au modèle français : l'ANSSI est un organisme interministériel, placé sous l'autorité du Premier ministre. Ce positionnement lui permet d'assurer la coordination interministérielle et la cohérence des positions. Il lui assure également un droit de regard et de contrôle sur les systèmes d'information des autres administrations, ce qui participe incontestablement du rehaussement de la sécurité de l'État.

C'est là un point essentiel de notre stratégie, ce qui fait sa force : le modèle français permet de déployer une politique globale de cybersécurité, c'est-à-dire une politique qui s'attacherait non seulement à défendre les infrastructures – publiques et privées – les plus critiques, mais aussi à parler au plus grand nombre, c'est-à-dire à l'ensemble des acteurs de la transformation numérique du pays.

Enfin, la séparation claire des missions, loin de les opposer, permet au contraire une répartition équilibrée des moyens mais également une coopération efficace au profit de la défense et de la sécurité nationale.

Tirer parti de toutes les opportunités offertes par notre modèle

Le risque numérique, accru par l'accélération technologique et le développement des usages, rend nécessaire une bien meilleure prise en compte des enjeux de sécurité par l'ensemble des acteurs de la transformation numérique. La sécurité doit sortir de son domaine réservé pour associer l'ensemble des architectes de la société numérique. Car au-delà des menaces sur la société, l'économie, la souveraineté et la stabilité du cyberespace, il en va du développement même des technologies.

L'État peut contribuer à créer les conditions de cette montée en puissance. Il s'agit en particulier de structurer un écosystème français de la cybersécurité, par la création de synergies entre les acteurs publics, économiques, de la recherche et de l'éducation. La vitalité de certains acteurs nationaux du secteur le montre : un marché français de la cybersécurité est en construction. Il est désormais nécessaire de l'accompagner.

D'autres pays ont mené cet effort structurant pour assurer la croissance de leurs industries de cybersécurité et ainsi garantir les moyens de leur souveraineté numérique. Israël constitue de ce point de vue un exemple particulièrement inspirant. L'État hébreu a en effet très tôt affirmé son ambition d'organiser son modèle autour de ces synergies. Cette ambition est caractérisée, pour Israël, par la création en 2016 du *CyberSpark*, qui réunit sur un même site des entreprises israéliennes et étrangères, des centres de recherche privés et publics et des unités spécialisées de l'armée israélienne.

La mission pour la création d'un « cyber campus », récemment confiée à Michel Van Den Berghe par le Premier ministre, participe de cet objectif de rapprocher des mondes qui ne se parlent pas suffisamment. De la même manière, l'ANSSI a récemment entrepris une démarche inédite d'ouverture auprès de son écosystème. Notre modèle nous le permet.

Cela passe par un changement de regard sur la cybersécurité. Celle-ci ne peut plus être appréhendée uniquement comme un poste de coût ou un patch appliqué en bout de course de l'innovation. Interrogez les experts de l'ANSSI : c'est un champ d'innovation passionnant, d'une grande richesse scientifique, profondément transdisciplinaire et associant une grande variété d'acteurs, privés et publics, en France comme à l'international. Elle pose des défis intellectuels majeurs pour les innovateurs de tous bords.

Si ces défis concernent naturellement les ingénieurs, les artisans des politiques publiques, du droit et des relations internationales ne sont pas en reste. Comment œuvrer à la stabilité du cyberespace ? Doit-on permettre aux acteurs privés de se faire justice eux-mêmes, de riposter aux attaques dans un contexte où les entreprises deviennent elles-mêmes des « champs de bataille » ? La stabilité du cyberespace est un sujet qui bouscule les habitudes politiques, diplomatiques et militaires. Les questions sont nombreuses et les perspectives excitantes, passionnantes, structurantes.