D'une pandémie l'autre…

Christian DAVIOT

Ancien conseiller stratégie du directeur général de l'ANSSI

L'on objectera que *comparaison n'est pas raison,* qu'il est encore trop tôt pour tirer des enseignements de la période que nous traversons. Il reste que l'expérience vécue lors du traitement par la France de la pandémie Covid-19 permet d'envisager l'impact de l'inévitable pandémie virale numérique qui nous touchera avant cinq ans. Et de s'y préparer.

Oser un tel parallèle est d'autant plus opportun que cette pandémie a accéléré la transition numérique de notre pays. Plus de numérique, c'est plus d'opportunité pour tous, y compris pour les acteurs malveillants, États ou criminels. Le développement à venir des usages permis par la 5G et la perspective de « territoires intelligents » augmentent d'autant la surface d'attaque de nos sociétés.

Prenons quelques-uns des éléments qui ont caractérisé les semaines écoulées.

L'origine de la pandémie

Avant que l'origine géographique et accidentelle de la pandémie fasse consensus pour les scientifiques, certains États ont tenté d'attribuer au gouvernement du pays concerné la responsabilité de la diffusion du virus. En perspective sans doute, les traces dans la mémoire collective des cinquante millions de morts causés par un virus importé d'un autre continent en Europe, mais toujours attribués cent ans après à une grippe « espagnole » ! Censure hier, propagande aujourd'hui…

Si l'origine d'une pandémie dans le monde matériel est discutée, dans l'univers numérique, il est question d'attribution. Certains États pratiquent le « naming and shaming » : une attaque informatique réelle, souvent à des fins d'espionnage, est publiquement dénoncée et des présumés coupables désignés[1], sans qu'aucune preuve définitive ne soit apportée. Il est vrai que révéler des preuves, lorsqu'elles existent, serait dévoiler ses propres pratiques et capacités… d'espionnage ! Malgré les pressions de gouvernements étrangers et la volonté de certains ministères, la France a jusqu'ici refusé cette pratique et intelligemment choisit le dialogue bilatéral, notamment parce que l'attribution d'une attaque informatique est un choix politique plus qu'une certitude technique. Il nous faudra nous en rappeler si demain la pandémie numérique touche nos intérêts vitaux.

Les victimes de la pandémie

À ce jour, la pandémie a fait près de trente mille morts en France. Les commissions d'enquête parlementaires établiront peut-être s'il aurait pu en être autrement. Les mesures économiques prises par le gouvernement permettront d'éviter une hécatombe économique, même si la pérennité de

[1] Le lecteur identifiera aisément les quatre États généralement cités.

l'activité de plusieurs dizaines de milliers d'artisans, commerçants, indépendants, petites et moyennes entreprises est remise en question.

Si des victimes humaines seront sans doute à déplorer, la pandémie numérique qui vient n'endeuillera heureusement pas autant de familles. Ses conséquences économiques seront, en revanche, potentiellement plus graves. Un virus informatique chiffrant et/ou destructeur[2] se diffusant largement et rapidement[3], pourrait stopper net l'activité de centaines de milliers d'entreprises de toutes tailles, de la multinationale au boulanger. Éventuellement sans possibilité de reprise. La France se remettrait difficilement d'une telle mise à terre.

Le système de santé

Alors qu'ils dénonçaient il a quelques mois leurs conditions de travail, le management par la restriction budgétaire et l'état de l'hôpital public, les hommes et les femmes du « personnel soignant » ont été capables par leurs compétences et dévouement de faire face aux effets de la pandémie, parfois au péril de leur vie, en inventant des solutions leur permettant de compenser toutes sortes de pénuries.

La France n'est pas (encore) prête à faire face à une pandémie numérique, pas plus qu'une autre nation. Le choix effectué il y a dix ans d'un modèle interministériel de cybersécurité plutôt que d'en confier la mise en place à la Défense ou aux services de renseignement a cependant permis de nous doter, au travers de l'ANSSI[4], de capacités de traitement opérationnel des attaques informatiques parmi les meilleures au monde. Mais bien que les gouvernements successifs aient donné les moyens budgétaires et humains nécessaires à son développement, et malgré leurs compétences et dévouement, ralentis par un accompagnement administratif plus que perfectible, les 650 agents de l'ANSSI ne pourraient faire face seuls à une pandémie numérique touchant des milliers d'acteurs répartis sur le territoire national. La stratégie nationale pour la sécurité du numérique portée par le Premier ministre en 2015 a d'ailleurs pris en compte cet enjeu en décidant de la création d'un organisme[5] dédié à la sensibilisation des particuliers, entreprises et collectivités territoriales et au traitement des attaques informatiques dont ils sont victimes par une mise en relation avec des prestataires privés de proximité. Cette plateforme, cybermalveillance.gouv.fr, est un succès à la fois technique et pédagogique qui a montré toute sa pertinence pendant la crise du Covid-19 et mériterait d'ailleurs d'être davantage soutenue aujourd'hui par l'État, les collectivités et les entreprises.

Pendant la pandémie Covid-19, et même si elles sont légitimes, les réquisitions par des préfets de masques de protection initialement commandés par des présidents de Région pour la protection de leurs administrés ont manifesté qu'en cas de crise des intérêts concurrents pouvaient exister entre l'État et les Régions. Il en irait de même en cas de pandémie numérique. L'ANSSI serait concentrée sur les opérateurs d'importance vitale, les administrations et les orientations que lui fixera le gouvernement. Ainsi, il appartient aux Régions de se préparer à la future pandémie numérique. Certaines Régions ont déjà pris conscience des enjeux liés à la sécurité du numérique, mais leurs ressources et compétences numériques sont souvent saturées par l'obligation de répondre à des contraintes réglementaires déjà lourdes et à la bureaucratie sous-jacente.

L'appui sur des experts

En complément de l'organisation administrative existante, la création d'un conseil scientifique a permis depuis le début de la pandémie d'éclairer une décision politique qui a su prendre en compte d'autres sources d'information et expertises de terrain, au moins partiellement.

2 De type Shamoon (2012) ou NotPetya (2016) par exemple.
3 De type Conficker (2008).
4 Agence nationale de la sécurité des systèmes d'information.
5 Le groupement d'intérêt public ACYMA, cybermalveillance.gouv.fr

L'expertise française en matière de cybersécurité est d'excellent niveau. Des universitaires ont notamment mis en place une approche interdisciplinaire de ce sujet et l'envisagent sous les angles national, européen et international. Pourtant, en raison d'une conception propriétaire, datée et exiguë de la sécurité du numérique, l'administration répugne généralement à consulter ces universitaires dont certains ont pourtant acquis une renommée internationale. Cette faiblesse retarde l'organisation de notre résilience à la future pandémie numérique.

Le rôle des acteurs privés

L'engagement des entreprises dans la lutte contre la pandémie est également un fait marquant. À côté des initiatives prises par de nombreuses PME, associations ou particuliers, de grandes entreprises comme LVMH se sont mobilisées, non seulement en exploitant leurs capacités industrielles pour fournir du gel hydroalcoolique par exemple, mais également en mobilisant leur réseau international pour trouver et fournir les équipements manquants.

On assiste à la même mobilisation de grandes entreprises en faveur de la sécurité du numérique dans une sorte d'inversion des rôles. Tandis que les États s'affrontent - malgré les conventions signées - dans ce qu'ils considèrent comme un nouveau domaine de combat, au risque d'entraîner des dysfonctionnements graves de nos sociétés et de provoquer la pandémie numérique qui les affaiblirait, des acteurs privés s'engagent en faveur de la paix et de la sécurité dans le numérique. Il en va ainsi du *Tech accord* de Microsoft ou de la *Charter of trust* de Siemens. En France, l'adhésion de nombreuses entreprises de l'écosystème au projet de Campus Cyber souhaité par le Président de la République relève du même engagement.

De même qu'un éventuel vaccin ne viendra que d'un effort conjoint entre États et entreprises, la sécurité du numérique ne se fera pas sans un engagement et une écoute des acteurs privés sans qui le numérique n'existerait pas.

Confinement et déconfinement

Visant à garantir la « distanciation sociale » - cette expression a valeur d'aveu - le confinement a, au contraire, souvent rapproché les personnes et suscité innovations et solidarités de proximité. Le traitement d'une pandémie numérique se fera dans la proximité et devra bénéficier, comme le déconfinement, de l'appui des Régions.

Des chantiers majeurs à lancer

L'analogie entre pandémie Covid-19 et pandémie numérique serait à poursuivre au travers des gestes barrières, du rôle des ministères des Armées et de l'Intérieur, de la place du Conseil de défense, etc.

Des scientifiques avaient anticipé la pandémie qui nous touche. Les administrations « compétentes » ont proposé au politique des décisions qui priorisaient d'autres critères que ceux à prendre en compte en matière de santé publique.

La période qui s'ouvre va être propice à une réflexion large - pas seulement économique - sur ce que nous voulons pour la France, l'Europe et les relations internationales dans les dix ans qui viennent. Au-delà des discours généraux qui émergent sur la souveraineté, périodiquement avancée par le politique, périodiquement enterrée par les administrations, il nous appartiendra de décliner à la sécurité du numérique certaines avancées présentées comme des solutions aux pandémies comme celle (super tabou dans l'administration) de « souveraineté européenne » ou de « bien public mondial ».

Portées à propos du numérique par le Président de la République, notamment dans ses discours annuels aux ambassadeurs, ces notions mériteraient l'attention et le travail des administrations, le soutien des universitaires et l'association des entreprises et des ONG. Associées à un engagement multilatéral conforme à nos valeurs et pas seulement pavlovien, à une vraie réflexion stratégique qui enterrerait la pathétique « Revue stratégique de cyberdéfense » de 2018, ces notions sont de nature à préparer la résilience qu'il nous reste à construire avec les Régions face à la pandémie numérique à venir.

Mais ces sujets feront l'objet d'autres développements.