INSTITUT
MONTAIGNE

Résumé

Comme tous les pays, la France est aujourd'hui susceptible d'être frappée par une cyberattaque majeure. L'interconnexion des technologies et des entreprises, la digitalisation, ou encore le fait que les systèmes d'information français dépendent d'un petit nombre d'acteurs laissent planer le risque d'un « cyber ouragan ». Afin de faire face à ce défi inédit, l'Institut Montaigne a travaillé avec les grands groupes industriels, les PME et ETI ainsi que les universités, pour comprendre la nature du risque et identifier les solutions qui s'offrent à nous. De ces réflexions découle un besoin vital de coopération et de solidarité entre acteurs privés d'une part, et entre acteurs privés et publics d'autre part, afin d'anticiper et d'identifier ces attaques ainsi que de limiter leurs effets sur les systèmes d'information français.

Les cyberattaques sont aujourd'hui en pleine expansion. Quatre types d'acteurs à l'origine de ces attaques émergent : des individus isolés, des « hacktivistes », poussés par des motifs idéologiques, des groupes mafieux organisés, et des groupes menaçants liés aux États. Les cyberattaques augmentent en nombre et en intensité au fil des années. En décembre 2015, l'Ukraine était touchée par l'une d'elle, plongeant 230 000 foyers dans la pénombre durant plusieurs heures. Moins de deux ans plus tard, le 12 mai 2017, le rançongiciel WannaCry causait des pannes et dysfonctionnements majeurs dans près de 150 pays, bloquant des centaines de milliers de postes de travail.

Une menace systémique

Le risque d'une cyberattaque est amplifié par deux facteurs, qui font de cette menace une menace systémique.

Tout d'abord, notre forte dépendance technologique s'appuie sur un nombre très restreint d'acteurs. Ainsi, Windows occupe 83 % du marché des systèmes d'exploitation sur les postes de travail, et les microprocesseurs Intel représentent près de 79 % des microprocesseurs d'architecture « x86 » (un type de microprocesseur) en circulation dans le monde. Une faille détectée par un individu ou une organisation malveillante dans l'un de ces systèmes peut, si elle est exploitée, toucher et pénaliser un nombre considérable d'acteurs.

À l'échelle de la France, l'interconnexion des systèmes, facilitée par le décloisonnement des services et l'adoption grandissante du *cloud* (monopolisé par Microsoft, Google et Amazon), rend les conséquences potentielles d'une attaque dramatiques. À l'échelle des organisations, elle augmente le nombre de portes par lesquelles peuvent entrer un virus.

Le « cyber ouragan », un risque réel

Le caractère systémique de la cybermenace rend ainsi plausible le scénario d'un « cyber ouragan » touchant la France et d'autres États. Cependant, il est important de noter que les États eux-mêmes n'ont aujourd'hui que peu d'intérêt à lancer une attaque provoquant un « cyber ouragan », tant leur degré d'interdépendance économique, ainsi que les risques de représailles, sont élevés. L'Institut Montaigne a identifié le scénario le plus probable pouvant entraîner un « cyber ouragan » comme étant celui d'une attaque provenant d'un acteur non-étatique, qui aurait dérobé des outils d'attaques.

Les conséquences d'une telle attaque seraient accablantes. Le 27 juin 2017, la cyberattaque NotPetya détruisait les postes de travail de ses victimes, générant plus de dix milliards de dollars de dégâts selon la Maison Blanche. Un « cyber ouragan » aurait un impact plus grave encore.

Entreprises et administrations : des réactions hétérogènes

Chez les grandes entreprises privées, le niveau de sécurité des systèmes d'information est hétérogène et dépend du secteur d'activité. Depuis longtemps tributaires du numérique pour fonctionner, les banques sont les plus mûres en matière de cybersécurité. Les sociétés dans le secteur du service et particulièrement les sociétés en B2C *(Business to Consumer)* se développent aussi sur le volet cybersécurité. Avec une moindre utilisation des outils numériques, les industries présentent le niveau de protection le plus bas par rapport aux autres secteurs. Toutefois, il est intéressant de noter qu'une faible numérisation peut parfois représenter une forme de résilience vis-à-vis des attaques informatiques.

Les TPE/PME/ETI sont les moins bien protégées. Or, selon les chiffres de l'Insee, les TPE/PME/ETI représentent à elles seules près de 73 % des emplois français (soit plus de 19 millions d'emplois, en 2015). Le faible niveau de sécurité de leurs systèmes d'information s'explique par l'absence de cybersécurité intégrée par défaut dans leurs équipements, ainsi que par le manque de compétences et de ressources allouées à la cybersécurité au sein de l'entreprise. Un « cyber ouragan » touchant simultanément les TPE/PME/ETI françaises engendrerait une crise économique et sociale majeure.

Face au défi posé par la cybermenace, l'Institut Montaigne formule treize recommandations réparties selon trois grands axes. Notre objectif est d'inciter les acteurs français à la solidarité et à la coopération, en amont et durant les crises cyber, afin d'augmenter la cyberrésilience de l'ensemble du tissu économique et des administrations.

Nos propositions

Axe n° 1 : Mobiliser l'ensemble du tissu économique

Afin de se préparer à l'éventualité d'un « cyber ouragan », les entreprises devront institutionnaliser leurs pratiques face aux cybermenaces. Afin de mobiliser les dirigeants au plus haut niveau, l'Institut Montaigne recommande que les grandes entreprises rédigent un rapport annuel sur les risques cyber auxquelles elles auraient fait face, à disposition des administrateurs, et qu'elles se mobilisent pour accroître le niveau de cybersécurité de leur chaîne d'approvisionnement et de leurs fournisseurs. Concernant les grandes entreprises évoluant dans des secteurs critiques, l'inclusion d'exigences précises de cyberrésilience dans la Loi de programmation militaire, comme la réalisation annuelle d'un exercice de crise, serait également nécessaire. Pour les TPE/PME/ETI, un diagnostic cybersécurité annuel devrait être réalisé par leurs experts comptables ou commissaires aux comptes, à destination des dirigeants de ces entreprises.

Axe n° 2 : Démultiplier les compétences et être solidaire en cas de crise

La coopération et la solidarité entre acteurs privés d'une part, et entre acteurs privés et publics d'autre part, sont indispensables pour faire face à un « cyber ouragan ». C'est pourquoi nous proposons que les acteurs privés se préparent dès à présent à développer la possibilité de mettre à disposition leur personnel et leurs compétences pour leurs pairs dans le cas d'une attaque majeure les ayant épargnés, *via* un cadre légal préétabli par leurs soins. Cette solidarité peut également se traduire par la mise en place d'une plateforme sécurisée d'échange entre les entreprises stratégiques pour la nation, opérée soit par l'État, soit par un acteur de confiance majeur de la cybersécurité en France, afin de partager les signatures d'attaques et les informations clés sur ces attaques. Enfin, l'État peut également être mobilisé, en étendant le rôle de la réserve opérationnelle de cyberdéfense à la résolution des crises touchant le secteur privé. Cette réserve pourra notamment monter en puissance en y incluant le secteur académique dès les phases de préparation à un « cyber ouragan », ainsi qu'en y intégrant les jeunes diplômés ayant suivi un parcours de formation en cybersécurité financé par l'État.

Axe n°3 : Pouvoir répondre à des attaques larges et rapides

L'ensemble de ces acteurs doit être capable de réagir à grande échelle et rapidement face à un « cyber ouragan ». Pour cela, il est nécessaire de tirer le meilleur parti de l'intelligence artificielle, tout en anticipant et prévenant ses dérives éventuelles. D'autre part, nous proposons la création d'un label de cyberrésilience pour les équipements pouvant impacter des vies humaines (comme la pédale de frein d'une voiture), afin qu'ils puissent fonctionner *a minima* de manière dégradée en cas d'attaque. Enfin, nous encourageons l'État à définir une doctrine opérationnelle pour faire face à une attaque large, et les entreprises à mettre en place une stratégie de défense active qui respecte le cadre législatif en vigueur.