

QUELLE PERSPECTIVE EUROPÉENNE EN MATIÈRE DE CYBERSÉCURITÉ? L'URGENCE D'INVESTIR DANS L'EXPERTISE HUMAINE



Par Nicolas Arpagian¹,
Directeur de la stratégie en cybersécurité, Trend
Micro, Enseignant à l'École Nationale Supérieure de la
Police (ENSP) et à Sciences Po - Saint-Germain.

La cybersécurité est un domaine à part dans le domaine des technologies de l'information. Contrairement à d'autres verticales de la planète tech, sa performance ne peut pas uniquement se mesurer, comme on en a pris l'habitude depuis la bulle Internet des années 2000, par la recension des communiqués de presse annonçant les levées de fonds des jeunes pousses du domaine. En effet, ce marché de la sécurité a la spécificité d'être également façonné par les enjeux de géopolitique et d'intérêts stratégiques des États. Ce qui fait que la nationalité des entreprises est désormais prise en compte. Or, tandis que la Chine, les États-Unis et même la Russie peuvent s'appuyer sur leur écosystème national respectif avec des acteurs de référence (BATX, GAFAM, VKontakte, Yandex...) qui sont les épines dorsales des collectivités humaines modernes, l'Europe se situe plus que jamais en consommatrice de services conçus et pilotés à partir d'autres continents que le sien. La singu-

larité et l'initiative de l'UE résident principalement dans le champ de la production normative avec des textes structurants comme le règlement général sur la protection des données (RGPD), les directives NIS sur la protection des opérateurs de services essentiels (OSE) et demain les «Digital Services Act (DSA)/Digital Markets Act (DMA)».

DE L'EXPERTISE À L'ENTREPRISE

Au regard de l'importance prise par les technologies numériques dans les activités de production, de gestion, de commercialisation et d'administration des entités privées et publiques, la question de la souveraineté technologique comme composante de la sécurité collective s'est donc désormais invitée au cœur des débats. Car les cyberattaques d'origine étatique ou criminelle des dernières années ont démontré l'intégration avérée des usages offensifs des technologies dans l'arsenal des

(1) Dernier ouvrage paru: «Frontières.com» aux Éditions de l'Observatoire, 2022.

gouvernements et des mafias. La prise de conscience des fragilisations rendues possibles par la maîtrise des techniques de cyber intrusion a conduit à imposer dans les esprits des moins technophiles des dirigeants l'importance vitale du savoir-faire en cybersécurité pour assurer la préservation de nos sociétés hautement numérisées. Or s'il est encore possible de mobiliser des ressources financières pour procéder à des investissements ou à des amorçages de capitaux, la concrétisation (en nombre et en qualité) de projets entrepreneuriaux dans le secteur de la cybersécurité est encore trop restreinte en Europe, limitant l'émergence à terme de solutions ou d'industriels de la sécurité d'essence européenne.

PERMETTRE L'AUTONOMIE DE LA PRISE DE DÉCISION

Cette pénurie d'expertise s'illustre pour commencer dans le nombre de professionnels en exercice. En 2021, ce n'est pas moins de 7 000 offres d'emploi cadre, qui ont été publiées par l'APEC dans le domaine de la cybersécurité sur le territoire national, soit presque deux fois plus qu'en 2017. Et Pôle Emploi estime que seuls 25 % des postes sont pourvus pour cause de manque de candidats ou de professionnels qualifiés. Il devient donc urgent de miser sur la formation, initiale et continue, pour élargir le nombre et l'origine des talents qui peuvent s'exercer dans le domaine de la cybersécurité. Cette diversité est nécessaire au regard de l'indispensable pluralité d'approches qu'il convient d'adopter pour concevoir des stratégies et des solutions de sécurité, tant offensives que défensives.

Cette situation, qu'il s'agisse de disposer d'un vivier de spécialistes à même d'intervenir utilement dans les entreprises ou les administrations, ou de porteurs de projets innovants susceptibles de donner naissance à des éditeurs de services performants, s'appuie donc sur un même besoin. Celui d'avoir des femmes et des hommes formés à cette matière de la cybersécurité. Qui connaît des déploiements dans l'ensemble des environnements techniques : applications, messageries, serveurs, « cloud computing », terminaux mobiles, communications sécurisées... Sans oublier les sujets qui s'annoncent tels ceux relevant de la mécanique

quantique ou des environnements complexes comme les metavers.

Cette expertise est indispensable pour assurer la souveraineté à laquelle les démocraties aspirent. Cela débute en ayant dans ses rangs civils ou militaires, des expert(e)s capables d'auditer des équipements et des suites logicielles, afin de s'assurer qu'ils ne font que ce qu'il leur est autorisé de faire. Et cela, malgré les mises à jour en continu qui modifient à distance les plus connectés des systèmes. L'élaboration de technologies, dites de confiance, passe par la compréhension exhaustive des tenants et aboutissants techniques qui composent les programmes auxquels on confie le bon fonctionnement de nos services de santé, de nos armées et de l'ensemble des infrastructures critiques, ou non.

UNE DIVERSITÉ DE TALENTS POUR APPRÉHENDER UN MONDE COMPLEXE

C'est en suscitant un apprentissage approfondi des technologies et de leurs fonctionnalités, et en croisant les disciplines afin de bénéficier de la pluralité des approches scientifiques et techniques, que naissent les circonstances créatrices à même de faire éclore des innovations de rupture. Cela prend du temps et peut sembler hors d'atteinte au regard de l'avancée des autres compétiteurs. Mais le principe du philosophe Jean Bodin, bien que né au XVI^e siècle, n'a jamais été autant d'actualité : « Il n'est de richesses que d'hommes ». La famille européenne n'a plus les moyens de retarder ce choix stratégique en faveur de la formation et de l'apprentissage. L'obligeant à innover également dans ses méthodes d'enseignement, dans le recrutement de ses formateurs et dans l'évaluation de ses cursus. Cet investissement dans l'esprit humain exigera d'y consacrer un temps qui pourra paraître long à certains court-termistes de profession. Mais c'est bien sur ce terrain de l'intelligence qu'il nous faut concentrer nos moyens. ■