MAI 2022

CIO letter

TK

Thomas FRIEDBERGER
Deputy CEO
Tikehau Capital
and Co-CIO

Gilles DAGUET
Managing Director
Private Equity -
Tikehau Capital

François LAVASTE
Executive Director
Private Equity -
Tikehau Capital

CYBER, DE LA SÉCURITÉ À LA RÉSILIENCE

En 2021[1], deux tiers de la population mondiale possède un téléphone mobile (5,2 milliards de personnes sur 7,8 milliards d'habitants), 60 % de l'humanité (4,7 milliards de personnes) dispose d'un accès à Internet et plus de la moitié est active sur les réseaux sociaux (4,2 milliards de personnes). Il ne paraît pas présomptueux en 2022 de faire l'hypothèse que quasiment 100 % des entreprises du monde sont informatisées. Pour elles, la « digitalisation des process » de production de biens et services, de distribution, de la relation avec clients et fournisseurs ou des chaînes d'approvisionnement est une nécessité, un facteur essentiel de compétitivité. D'ici deux ans, le commerce électronique devrait représenter un marché de plus de 800 milliards de dollars, propulsé par l'émergence du « Metaverse » et des NFT[2]. Pour les États, les enjeux de la « digitalisation » participent également de la nécessité de moderniser le fonctionnement des services publics et de renforcer leur efficacité, des prestations liées à la recherche d'emploi à la santé en passant par l'éducation ou le paiement de l'impôt.

Dans ce contexte, les enjeux de la cybersécurité sont gigantesques. Car, ce qui d'un côté s'impose comme une nécessité de modernisation, un avantage compétitif ou une caractéristique du développement économique apparaît aussi comme une extraordinaire source de vulnérabilité si les systèmes et les données ne sont pas bien protégés. Nous pouvons ainsi admettre que les risques liés à la cybersécurité comptent probablement, avec les sujets de santé publique et du changement climatique, parmi ceux qui concernent le plus grand nombre d'êtres humains sur cette planète. C'est probablement la raison pour laquelle le Président de la Réserve fédérale américaine citait en avril 2021 les cyberattaques comme le principal risque pour la stabilité du système économique mondial. Selon un rapport du Forum économique mondial, le risque cyber est celui qui a le plus augmenté pendant la crise de la COVID-19[2]. Du côté européen, l'ajout anticipé de la cybersécurité dans la taxonomie sociale européenne prouve que ce secteur est central dans la construction d'écosystèmes plus résilients[3].

C'est donc à ce thème que nous dédions notre lettre. Non seulement parce que le sujet est d'une importance capitale pour les entreprises dans lesquelles nous investissons ainsi que pour nos partenaires, fournisseurs, investisseurs et actionnaires, mais aussi parce qu'**ayant identifié cette tendance de fond comme l'une des opportunités d'investissement les plus significatives des prochaines décennies**, nous disposons d'une expertise unique en Europe, apportée par une équipe d'investissement expérimentée, gérant le plus grand fonds de « private equity » dédié à la cybersécurité en Europe. C'est avec cette équipe que nous écrivons ces lignes pour partager avec nos lecteurs notre approche de ce sujet si stratégique.

1. https://wearesocial.com/fr/blog/2021/01/digital-report-2021- Digital report 2021
2. The Global Risk Report World Economic Forum 2022
3. https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/280222-sustainable-finance-platform-finance-report-social-taxonomy.pdf#page43

TK TIKEHAU CAPITAL

Le risque cyber

> SI LE RISQUE CYBER ÉTAIT UNE ÉCONOMIE, IL REPRÉSENTERAIT LA TROISIÈME ÉCONOMIE MONDIALE.

Une cyberattaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseau, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les « smartphones » ou les tablettes. Plus récemment, avec la transformation numérique de l'industrie et les véhicules connectés, ces attaques peuvent aussi porter atteinte à l'intégrité des machines-outils, des usines ou de nos voitures. Il existe quatre types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises. La cybercriminalité consiste en l'obtention d'informations personnelles afin de les exploiter ou de les revendre. L'atteinte à l'image consiste à modifier l'apparence ou le contenu d'un site, et donc à altérer l'intégrité des pages. L'espionnage consiste à acquérir de manière ciblée des informations économiques, politiques, militaires ou scientifiques. Enfin, le sabotage est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique. La cybersécurité comprend toutes les mesures mises en place pour se protéger contre ces risques. Elle regroupe en particulier la sécurité des réseaux, du cloud, des postes de travail, des téléphones portables, des infrastructures, des objets connectés, la détection des menaces, des intrusions et des fraudes, la gestion des accès, des identités, les tests d'intrusion, le filtrage des messageries et du web.

Le « think tank » français « Le club des juristes »[4] évalue le risque cyber global à 6000 milliards de dollars en 2021. Si le risque cyber était une économie, il représenterait la troisième économie mondiale derrière les États-Unis et la Chine. Ce chiffre devrait atteindre 10500 milliards de dollars en 2025, soit une croissance de près de 15% par an[5].

La crise de la COVID-19 qui a accéléré le recours massif au télétravail et au commerce en ligne n'a fait qu'amplifier

4. https://www.leclubdesjuristes.com/wp-content/uploads/2021/04/rapport_cyberattaques_DEFweb-1.pdf
5. cyberwarfare in the C-suite, Cybersecurity ventures, janvier 2021 et Rapport du ministère de l'Intérieur, État de la menace numérique

le risque cyber. Elle a également démontré la vulnérabilité de nos systèmes de santé aux attaques cyber, capables de dérober ou de falsifier massivement des données mais aussi de paralyser un système hospitalier sous tension extrême. La crise russo-ukrainienne accentue encore le risque. Dans un communiqué du 21 mars 2022[6], la Maison-Blanche réitère ses avertissements sur de très probables attaques cyber. Elle indique que l'Agence pour la Cybersécurité et la Sécurité des Infrastructures (CISA) du ministère de la Sécurité intérieure travaille activement avec les organisations des infrastructures critiques afin de partager rapidement des informations et des conseils sur les mesures d'atténuation de la menace pour les aider à protéger leurs systèmes et leurs réseaux.

Selon l'Organisation des Nations Unies, le nombre de courriers électroniquesmalveillants en circulation dans le monde a augmenté de plus de 600% au début de la pandémie de COVID-19[7]. Le « Federal Bureau of Investigation » (FBI) des États-Unis a averti qu'il existe maintenant 100 souches différentes de rançongiciels en circulation dans le monde. Il y a eu en moyenne 270 attaques par organisation en 2021, soit une augmentation de 31% par rapport à 2020[8]. Les montants récupérés par les hackers ont été multipliés par quatre entre 2019 et 2020. Aux États-Unis, près de 800000 cyberincidents ont été signalés au FBI en 2020[9] et des enquêtes suggèrent que plus de la moitié des entreprises ont été victimes d'une cyberattaque[10]. En moyenne, la résolution d'une cyberattaque requiert 280 jours à une société[11]. La cyberattaque individuelle la plus destructrice à ce jour est l'attaque NotPetya de 2017 dirigée à l'origine contre l'Ukraine mais dont les effets

> **LES MONTANTS RÉCUPÉRÉS PAR LES HACKERS ONT ÉTÉ MULTIPLIÉS PAR QUATRE ENTRE 2019 ET 2020.**

collatéraux liés à la capacité de ce vers de se propager automatiquement dans les réseaux informatiques ont été ressentis dans le monde entier. Cette agression aurait infligé plus de 10 milliards de dollars de dommages, soit un peu plus de 10% du PIB de l'Ukraine à l'époque. En novembre 2021, l'équipe de cybersécurité du cloud de la société chinoise Alibaba a divulgué une vulnérabilité de l'utilitaire Java Log 4j, un cadre open source permettant aux développeurs de logiciels d'enregistrer diverses données au sein de leur application. La semaine suivant l'annonce de la vulnérabilité Log4shell, plus de 100 tentatives d'exploitation par minute ont été relevées.

Les cybercriminels saisissent toutes les occasions d'exploiter les vulnérabilités des personnes et des organisations grâce à la technologie. Ils adoptent rapidement les nouvelles technologies, adaptent les stratégies de leurs attaques en utilisant

6. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity
7. https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542
8. Global Cybersecurity Outlook 2022 - World Economic Forum
9. IC3, « Internet Crime Report 2020 », 2021
10. The economic impact of cyberattacks – Goldman Sachs US economics analyst, March 7, 2022
11. IBM Security. 2020. Cost of a Data Breach Report 2020 https://www.ibm.com/security/digitalassets/ cost-data-breach report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

AUX ETATS-UNIS, LE PRIX DES ASSURANCES CYBER A PROGRESSÉ DE

204%

EN RYTHME ANNUEL EN 2021.

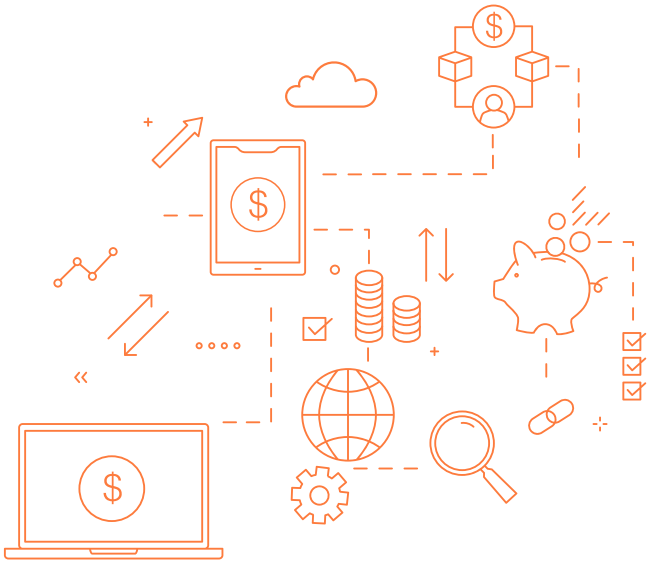
de nouvelles méthodes et coopèrent les uns avec les autres. Le crime organisé a rapidement ajouté l'angle numérique à son arsenal. Europol a récemment signalé que les groupes criminels organisés recrutaient des pirates informatiques pour le phishing ou l'envoi de logiciels malveillants pour prendre le contrôle des comptes bancaires des victimes. De plus, le crime organisé implique souvent les cybercriminels dans des opérations commerciales légales, accroissant la porosité entre business légal et criminel. Ces personnes peuvent être basées n'importe où dans le monde, ce qui empêche les forces de l'ordre de perturber ces groupes.

L'assurance est l'une des solutions privilégiées par les entreprises pour réduire l'impact des cyberincidents[12]. Une majorité d'entreprises dispose d'une cyberassurance, soit pour limiter la responsabilité financière pour des cyberincidents spécifiques, soit pour bénéficier de services de réponse aux incidents et de professionnels mis à disposition par la compagnie d'assurance. Cependant, le niveau de maturité des marchés de la cyberassurance varie considérablement d'un pays à l'autre. Dans certaines régions, il s'agit d'une pratique courante. Dans d'autres, il s'agit d'une solution qui vient seulement d'émerger. De plus, l'industrie de la cyberassurance subit un changement majeur. En raison des attaques de « ransomware » émergentes et de leur volume, l'augmentation moyenne des primes en 2021 s'élevait à 180%. Aux États-Unis, le prix des assurances cyber a progressé de 204% en rythme annuel en 2021[13]. Dans un article paru dans « Les Echos »[14], le responsable de l'assurance des risques d'Airbus Defence and Space mentionne que les cyberattaques ont coûté trois fois plus aux assureurs en un an, entre 2019 et 2020. Ces attaques ont poussé les assureurs à débourser beaucoup plus d'argent pour indemniser leurs assurés que ce qu'ils avaient reçu sous forme de primes, malgré l'augmentation de ces primes. Il prévient : « Nous ne sommes pas loin du déclenchement d'un cercle vicieux dans le marché de l'assurance cyber pour les entreprises. Il conduirait les assureurs à offrir de moins en moins de capacités alors que les entreprises en ont de plus en plus besoin ». Le ratio de sinistres sur primes, indicateur de rentabilité pour les assureurs, est en effet passé de 84% en 2019 à 167% en 2020, selon l'AMRAE[15]. Le paiement des rançons par les assureurs renforce par ailleurs les moyens des cybercriminels, créant un cercle vicieux qui montre les limites des contrats d'assurance dans ce domaine.

12. Global Cybersecurity Outlook 2022 - World Economic Forum
13. Invest Quarterly Sector Outlook: Information Security, 4Q21, Frank Marsala, Gartner- The Global Risk Report World Economic Forum 2022
14. Les Echos - les cyberattaques coûtent trois fois plus aux assureurs en un an, 26 mai 2021
15. Association pour le Management des Risques et des Assurances de l'Entreprise – amrae.fr

Une opportunité d'investissement unique

La crise de la COVID-19 puis la guerre russo-ukrainienne mettent en évidence l'extraordinaire vulnérabilité d'un modèle économique basé sur la recherche d'une croissance à court terme. La faiblesse des taux d'intérêts a permis aux États de soutenir massivement l'économie mondiale par des politiques budgétaires agressives financées par une augmentation significative des stocks de dette. En somme, le recours massif à la dette a permis de prolonger le cycle économique mais a, en contrepartie, rendu indispensable la génération de croissance à court terme pour justifier ces niveaux de levier. Or, l'inversion simultanée de trois tendances de long terme, ayant agi comme un vent favorable à la croissance des résultats des entreprises sur les trente dernières années, menace désormais ce fragile équilibre : les taux d'intérêt ont probablement atteint un point bas, de même que les taux d'imposition sur les entreprises. La mondialisation a, quant à elle atteint un point d'inflexion qui ne permettra plus aux entreprises de suroptimiser leurs coûts de production, leur fiscalité ou les niveaux de capitaux propres avec lesquels elles opèrent. La rivalité Est-Ouest affaiblit le modèle de l'entreprise mondialisée, capable de suroptimiser sa chaîne d'approvisionnement et son processus industriel en produisant là où les coûts sont les plus faibles. En outre, l'émergence de deux types de standards et de normes, deux systèmes monétaires différents ainsi que la fermeture de marchés potentiels du fait du choix d'un camp ou d'un autre forceront les entreprises à investir massivement dans la sécurité des systèmes. Pour rester compétitives et renforcer leur résilience face à ces freins à la génération de résultat financier, les entreprises vont devoir investir massivement, initiant un nouveau cycle de dépenses d'investissement. Ce cycle a déjà commencé dans certaines régions comme aux États-Unis, ou l'État a fait le choix d'aider les entreprises à relocaliser leur production



et à sécuriser leurs approvisionnements et leurs systèmes d'information. Dans ce contexte, la cybersécurité semble représenter, avec la recherche d'efficience énergétique et la « digitalisation » des processus de production, l'un des trois domaines dans lesquels les entreprises du monde entier doivent investir massivement pour réduire leur vulnérabilité et renforcer leur résilience. Les États et les services publics suivront cette tendance. La crise ukrainienne devrait provoquer une augmentation massive des budgets alloués à la cybersécurité pour toutes les organisations. La massification de l'utilisation des données, la décentralisation des paiements et la « digitalisation » des procédés rendent indispensables les investissements cyber. Il ne s'agit pas ici d'investissements tactiques mais de choix stratégiques faits au niveau des directions générales des entreprises et qui concernent tous les départements de l'organisation dans tous les secteurs d'activité.

Le modèle économique capitaliste, basé sur l'espérance de profit généré par le secteur privé, recherche en permanence l'effet d'échelle qui permet de démultiplier la capacité bénéficiaire d'un « process ». Au XXe siècle, cet effet d'échelle fut permis par le recours au pétrole comme principale source d'énergie ainsi que par la dérégulation et la mondialisation de l'économie après la faillite du modèle communiste, à la fin des années 1980. **Au XXIe siècle, cet effet d'échelle est permis par les technologies numériques et la capacité d'un produit, d'un service ou d'une marque à toucher l'ensemble de la population mondiale disposant d'un dispositif de communication. Le risque cyber menace ce modèle économique tout entier.**

Partout dans le monde, l'explosion inquiétante du nombre de « ransomwares » et leur niveau de sophistication croissant démontrent l'urgence pour les acteurs de l'économie d'engager des plans consistants d'investissement pour se défendre et assurer leur résilience et leur pérennité. Il s'agit non seulement de protéger la propriété intellectuelle et les données mais également de préserver les emplois qui seraient menacés en cas d'incapacité de l'organisation à exercer son activité ou de perte financière. Dans une étude publiée par PricewaterhouseCoopers[16], une majorité de chefs d'entreprises interrogés s'attendent à une hausse significative des risques cyber dans des domaines aussi variés que les tentatives d'intrusion par des virus (malware), de demande de rançon (ransomware), de perturbation des chaînes d'approvisionnement, de désinformation, les attaques émanant d'États sur des infrastructures critiques ou l'exercice d'influence sur la recherche et le développement pratiqués par l'entreprise. Plus de 25 % des chefs d'entreprises anticipent une croissance à deux chiffres des budgets cyber en 2022. C'est d'autant plus stratégique que les entreprises bénéficiant des meilleures organisations dans ce domaine, c'est-à-dire d'un engagement cyber du dirigeant, d'un bon niveau de fiabilité

16. 2022 Global Digital Trust Insight, PwC

L'ÉCOSYSTÈME CYBER GLOBAL EMPLOIE

3,5 M

DE PERSONNES MAIS MANQUE D'ENVIRON 3 MILLIONS D'EMPLOYÉS SUPPLÉMENTAIRES.

des données et d'une organisation performante, ont beaucoup plus de marge de progression dans le domaine cyber que les autres.

Or, le secteur de la cybersécurité est composé d'un grand nombre de startups et de sociétés non cotées de taille moyenne financées par des fonds de « Private Equity », principalement américains, même si l'Europe et la France en particulier se hissent parmi les leaders de l'investissement non coté dans le secteur. Outre ces petites entreprises, un nombre limité de grands groupes cotés complète l'écosystème de la cybersécurité. Cet écosystème en très forte croissance n'est donc pas mature. Tout comme la transition énergétique, le secteur représente une mégatendance qui en fait une opportunité d'investissement unique. L'écosystème cyber global emploie 3,5 millions de personnes mais manque d'environ 3 millions d'employés supplémentaires[17]. Les universités auront du mal à former rapidement un nombre aussi important de spécialistes, accentuant le besoin crucial d'automatiser les « process » cyber et de miser sur l'intelligence artificielle pour suppléer le manque de spécialistes humains. Les besoins d'investissement dans ce domaine sont donc massifs.

Car l'industrie a besoin de l'apport de la technologie pour améliorer ses processus de production. Pas uniquement pour les rendre plus efficients, mais aussi plus en phase avec la recherche d'une croissance durable. L'inverse est également vrai. La technologie a besoin de l'industrie pour prendre du sens et se rapprocher de l'humain. Nous avons évoqué dans une lettre précédente[18] les risques de creusement des inégalités du fait du progrès technologique. Nous avons également évoqué le risque de compartimentation de la société par les bulles filtrantes permises par la tech : l'internaute se voit proposer des contenus en harmonie avec ses convictions ce qui favorise le repli communautaire et la rupture du débat et du dialogue. **La tech a donc besoin de trouver sa voie pour se réhumaniser. Sa contribution à rendre l'industrie plus durable et plus locale et à en faire un véritable avantage compétitif pour les écosystèmes régionaux participe à sa rédemption et fait probablement partie des concepts de « tech for good ». Cela n'est pas réalisable sans la contribution de la cybersécurité.**

17. https://www.weforum.org/agenda/2021/01 top-cybersecurity-challenges-of-2021/
18. Tikehau CIO letter - Robot Rock, Mars 2021

Conséquences pour les entreprises

Pour les chefs d'entreprise, le problème réside dans le constat que la cybermenace change et s'adapte chaque jour, ce qui invalide toute hypothèse que la protection mise en place à une date donnée soit une garantie pour l'avenir. 95 % des problèmes cyber sont liés à une erreur humaine[19]. La question qui se pose est en fait de savoir « quand » et « dans quelle mesure » l'entreprise sera touchée plutôt que « si ». De plus la cyber n'est pas seulement un sujet pour le service informatique d'une organisation dans la mesure où une attaque peut sérieusement affecter la continuité de l'ensemble de l'entreprise. Il s'agit donc d'un sujet stratégique à traiter au niveau du comité exécutif et du conseil d'administration et auquel l'ensemble des collaborateurs doivent être sensibilisés et formés. Pour imposer les meilleures pratiques, il apparaît donc nécessaire de cartographier les risques cyber, l'impact potentiel des attaques, des dommages contre la structure et de hiérarchiser les efforts à déployer en conséquence. Il convient également de mettre en place un plan de continuité des activités et de reprise après sinistre ainsi que d'organiser un exercice de cybersécurité au moins une fois par an au même titre que les exercices d'évacuation incendie.

Une entreprise est aussi sûre que le maillon le plus faible de son écosystème.

Les cyberattaques contre d'autres organisations de la chaîne d'approvisionnement numérique peuvent avoir un impact négatif sur les entreprises en aval et leurs opérations. En 2021, le groupe de « ransomware » Revil a exploité une vulnérabilité dans une plate-forme logicielle de surveillance et de gestion à

19. Invest Quarterly Sector Outlook: Information Security, 4Q21, Frank Marsala, Gartner. The Global Risk Report World Economic Forum 2022 : CHAPTER 3 Digital Dependencies and Cyber Vulnerabilities

distance et lancé l'une des plus grandes attaques de « ransomware » de l'histoire, affectant l'ensemble de la chaîne d'approvisionnement de la plate-forme[20]. L'attaque a perturbé près de 1500 entreprises dans le monde, y compris une chaîne suédoise d'épiceries, ce qui a forcé la fermeture temporaire de plus de plus de 800 magasins[21]. Au cours des dernières années, les attaques indirectes ayant abouti sont passées de 44% à 61%[22]. En plus de se focaliser sur son propre système d'information, l'entreprise doit donc également se préoccuper de la résilience de l'ensemble de la chaîne de ses partenaires, clients et fournisseurs.

En termes de coût pour les entreprises, une étude du Council of Economic Advisors (CEA) a estimé que les grandes entreprises cotées en bourse perdaient en moyenne près de 500 millions de dollars en valeur par cyberévénement indésirable[23]. Pendant la crise sanitaire, les agresseurs se sont concentrés sur les opportunités à faible risque et à fort rendement, ce qui a forcé les équipes de cybersécurité des entreprises à travailler sans relâche pour protéger leurs organisations contre la persistance des menaces. Les équipes de cybersécurité doivent s'outiller pour faire face à l'évolution des menaces, avoir une visibilité à la fois sur leurs propres réseaux et sur les réseaux étendus de leurs chaînes d'approvisionnement et de leur écosystème tiers, et surtout, pour retenir les talents. Or, non seulement le monde manque de talents dans le domaine de la cybersécurité, mais la capacité d'adaptation de ces talents à l'environnement de l'entreprise n'est pas non plus évidente. Dans une interview sur la chaîne Youtube Thinkerview[24], deux « hackers éthiques » français décrivent non sans humour les difficultés pour une entreprise d'embaucher des talents ayant leur profil : hors de question de rédiger un CV, nécessité de disposer d'une salle de sieste sur le lieu de travail pour faciliter le travail de nuit, pas d'horaires fixes, etc.

LES ATTAQUES INDIRECTES AYANT ABOUTI SONT PASSÉES DE 44% À

61%

20. Global Cybersecurity Outlook 2022 - World Economic Forum
21. Klugerman, Yaffa. 2021. The 5 Most Notable Third-Party Data Breaches of 2021 (So Far). Panorays
22. Bissell, Kelly, et al. 2021. State of Cybersecurity Resilience 2021. Accenture
23. Economic report of the président - White house – 2018
24. Le Hacking au XXIe siècle – Thinkerview, Septembre 2021

Toutes les entreprises, petites comme grandes, et plus largement tous les acteurs de l'économie mondiale, États inclus, sont concernés par le sujet cyber. Les canaux de financement de ce secteur sont donc stratégiques. Pour l'Europe, il est absolument crucial de permettre à ces sociétés de rester sur le continent en leur fournissant les moyens financiers performants pour se développer et éviter ainsi un exode vers les marchés de capitaux américains si profonds. La cybersécurité illustre à la fois le cruel besoin d'une politique industrielle performante basée sur des partenariats entre les États et leur écosystème industriel et les enjeux stratégiques qui entourent la révolution technologique que nous vivons.

Dans ce contexte, il n'est pas étonnant de constater que les investisseurs dans les fonds de « private equity » dans la cybersécurité sont aussi les entreprises elles-mêmes, pour ces mêmes raisons stratégiques. Ces investissements leur permettent en effet de comprendre et d'accéder aux expertises développées par les entreprises levant du capital par l'intermédiaire de ces fonds.

L'année 2021 est une année record pour la levée de fonds dans le « private equity » dédié à la cybersécurité. Au total, plus de 21 milliards de dollars ont été levés par 727 sociétés, soit plus de trois fois le montant levé sur les trois années précédentes cumulées. Les États-Unis concentrent plus de 80% du montant des levées, laissant à Israël et à l'Europe environ 15% du total. En Europe, le Royaume-Uni reste de loin leader devant la France, l'Allemagne, l'Espagne et la Suisse.

> LA CYBERSÉCURITÉ ILLUSTRE À LA FOIS LE CRUEL BESOIN DE POLITIQUE INDUSTRIELLE PERFORMANTE BASÉE SUR DES PARTENARIATS ENTRE LES ETATS ET LEUR ÉCOSYSTÈME INDUSTRIEL ET LES ENJEUX STRATÉGIQUES QUI ENTOURENT LA RÉVOLUTION TECHNOLOGIQUE QUE NOUS VIVONS.

LES ÉTATS UNIS CONCENTRENT PLUS DE

80%

DU MONTANT DES LEVÉES.

Joep GOMMERS
CEO and founder of EclecticIQ, a Tikehau Capital portfolio company

Avant de lancer EclecticIQ en 2014, Joep travaillait dans la menace cyber chez iSIGHT Partners.

Chez EclecticIQ, nous avons le privilège de pouvoir apporter notre soutien à certaines des organisations du monde entier les plus souvent ciblées en matière de menaces cyber, le tout par le biais de notre gestion, partage et traitement de l'information. Notre activité permet aux entreprises et organismes nationaux de sécurité en question de prévenir, repousser et contrecarrer les menaces cyber qu'elles rencontrent.
Cet article a donc pour but de fournir aux dirigeants le lisant une série de conseils visant à aider le reste de leurs équipes de cybersécurité à concevoir des programmes favorisant non seulement un important retour sur investissement (ROI) mais aussi un degré de sécurité qui correspond à la réalité que ces menaces posent.

COMPRENDRE SON ENVIRONNEMENT POUR MIEUX COMPRENDRE LES RISQUES

La gestion des risques sous-entend la gestion de l'incertitude entourant les objectifs de votre société, qui par définition fait de la cybersécurité un souci d'envergure. Cette même incertitude est influencée en grande partie par l'environnement dans lequel vous évoluez. Sans une compréhension limpide de l'environnement, des acteurs en matière de menaces cyber qui en font partie ou encore de leurs aptitudes et intentions (malveillantes), il devient presque impossible de saisir le niveau de risque auquel vous faites face, et encore moins de prendre les mesures nécessaires à sa gestion.

LE PAYSAGE DES MENACES A ÉVOLUÉ. VOTRE APPROCHE SE DOIT D'EN FAIRE AUTANT

Il y a bien des années de cela, posséder une connaissance complète de votre entreprise, de ses opérations, de ses systèmes et faiblesses informatiques était tout ce dont vous aviez besoin pour concevoir des contrôles de sécurité assurant la gestion des risques. À l'époque où le nombre et la nature de potentielles menaces cyber étaient connus, le simple fait d'être conscient de leur impact sur votre organisation était suffisant. Mais de nos jours, alors que les menaces cyber sont constantes, répandues et capables d'évoluer rapidement, il est impossible de se protéger seul contre toutes ces menaces et les vecteurs de cyberattaque existants. Pour un retour sur investissement élevé en matière de gestion des risques cyber, il est primordial de s'assurer au préalable que ledit investissement réduise au maximum le degré d'incertitude qui pèse sur les objectifs de l'entreprise. Cela signifie que tous vos efforts et investissements visant à garantir la cybersécurité de vos opérations ne doivent pas uniquement reposer sur une connaissance de votre société, mais aussi que les décisions prises dans ce sens doivent être informées par le paysage d'ensemble des menaces auxquelles vous êtes confronté. Aligner vos efforts et investissements en cybersécurité avec la réalité des menaces environnantes permet d'observer un retour sur investissement qui, en conséquence, réduit l'incertitude autour de vos objectifs et diminue ainsi les risques.

Néanmoins, comprendre le paysage d'ensemble des menaces vous faisant face n'est pas toujours chose aisée. Transformer cette compréhension des risques en de véritables activités opérationnelles et finalement en valeur commerciale n'est encore une fois pas des plus simples. Les renseignements sur les menaces cyber peuvent se présenter sous une multitude de formes. Prendre la bonne décision et s'assurer que ces renseignements sont correctement mis en œuvre peut faire la différence entre un investissement perdu et un investissement en cybersécurité sur lequel un retour est perçu.

UNE MÉTHODE EN QUATRE ÉTAPES POUR MODELER SA GESTION DES RISQUES ET RÉDUIRE LA DANGEROSITÉ DES MENACES

En tant que cadre ou dirigeant responsable de prendre d'importantes décisions, vous serez amené à travailler auprès de vos équipes de cybersécurité afin de surveiller les risques et réduire le nombre de menaces grâce à la CTI (Cyber Threat Intelligence, en anglais). Les quatre points indiqués ci-dessous se doivent ainsi d'être discutés au sein de vos équipes. Adopter une approche holistique. Nouer un lien avec sa communauté. Obtenir les renseignements nécessaires. Réagir en conséquence.

Adopter une approche holistique. Il est courant de voir des entreprises travailler exclusivement avec des équipes de cybersécurité opérationnelles ayant pour but de détecter ou de déjouer avec immédiateté toute activité malveillante. Cependant, tenter de réduire le niveau de risque posé par des menaces cyber nécessite d'adopter une approche bien plus holistique. Éviter l'émergence d'une situation défavorable peut en effet passer par des actions prises en amont, directement au sein de l'entreprise. La prévention est souvent un outil stratégique, signifiant qu'il est préférable de s'assurer que les risques, la conformité et les acteurs commerciaux et légaux sont pris en compte dans la mise en place des systèmes de renseignements contre les menaces que vous souhaitez instaurer au sein de votre entreprise. Lorsque l'heure de la prévention est passée, il devient nécessaire de stopper les menaces malveillantes sur leur route et ainsi les « repousser ». Cela suppose de reposer sur les efforts de techniciens informatiques, d'Architectes Sécurité et de vos équipes opérationnelles, par le biais par exemple de spécialistes en manœuvres de sécurité et en réponse aux incidents. Lorsque vos efforts sont en vain et un incident se produit - puisqu'il n'est pas question de savoir SI mais plutôt QUAND un incident aura lieu -, il devient alors nécessaire d'œuvrer pour un résultat concluant en mettant fin à ce « conflit » selon des termes qui vous sont favorables. Assurez-vous donc que votre programme réponde aux besoins de chacun des acteurs liés aux efforts visant à « prévenir, repousser et contrecarrer » les menaces (soit une gestion stratégique, tactique et opérationnelle des risques), mais aussi que ces derniers comprennent sous quelle forme obtenir et utiliser les renseignements protégeant contre lesdites menaces.

Nouer un lien avec sa communauté. La plupart des organisations ciblées font face aux mêmes menaces, mais dans leur coin. Cette isolation engendre une perte de temps et de ressources, lesquels sont investis par une entreprise pour répondre aux incidents malveillants qui sont pourtant monnaie courante au sein de leur secteur d'activité. Une coopération étroite avec des centres de cybersécurité locaux, un CERT de secteur ou toute autre initiative communautaire est le meilleur moyen d'améliorer votre accès à l'information. Il convient de garantir une telle coopération grâce au partage des connaissances, à la consommation des ressources opérationnelles à votre disposition, mais aussi en échangeant des informations relatives aux menaces et incidents.

Obtenir les renseignements nécessaires. Contrairement aux idées reçues, être proactif représente une approche bien plus rentable que la recherche de renseignements concernant une menace

imminente. Une pertinence à caractère immédiat signifie généralement que vous êtes d'ores et déjà vulnérable. Empêcher cette vulnérabilité en amont doit donc être votre priorité n°1. Cela ne veut pourtant pas dire que vous devez renoncer à récolter des renseignements sur les menaces qui vous touchent directement et immédiatement. La surveillance des empreintes numériques externes, la découverte d'actifs corrompus ou vulnérables, la protection contre des fuites de propriété intellectuelle et d'accréditation ou encore des abus de marque sont autant de choses qui se doivent de figurer dans votre programme.

Votre attention doit toutefois se fixer sur l'obtention de renseignements capables de vous informer quant aux méthodes et capacités des acteurs en termes de menaces qui, à première vue, sont ceux qui s'opposent à vos objectifs et ont pour habitude de cibler des organisations comme la vôtre, de s'attaquer aux technologies en votre possession, votre secteur d'activité ou encore les communautés (géographiques) auxquelles vous appartenez. Il est alors préférable de rechercher des informations quant à des menaces ayant déjà sévi ailleurs, là où les efforts de réaction d'autres vous permettent d'être proactif, ou bien d'acquérir des informations sur les capacités sous-jacentes de ces acteurs afin de pouvoir repérer des menaces ne s'étant pas encore matérialisées. C'est en particulier un accès à des indicateurs de compromission (ou IOC) et à des règles de détection que vous vous intéresserez, lesquels vous permettront de repérer des infrastructures et outils de menaces cyber connus. Cela étant dit, alors que les menaces sont en constante évolution, la pertinence de ces IOC diminue rapidement. Ils ont besoin d'être renforcés à l'aide de connaissances plus robustes qui demeurent pertinentes tandis que les acteurs en matière de menace continuent d'agrandir l'arsenal des outils et infrastructures à leur disposition. Vous devez également vous assurer que des renseignements concernant les capacités cachées et les TTP (« Tactics, Techniques and Procedures ») utilisées par les acteurs en termes de menaces vous sont disponibles. Ces techniques et leur modus operandi, tout comme les engrenages d'une entreprise, sont bien souvent plus difficiles à modifier pour les attaquants. Une entreprise, une équipe informatique ou encore des Architectes Sécurité peuvent ainsi utiliser ces connaissances pour mettre en place toute une série de contrôles. Ces derniers pourront contrer les techniques des attaquants ou modifier les procédés et systèmes en place pour minimiser l'impact du réseau d'attaque (combinant diverses techniques) à la disposition des malfaiteurs.

Réagir en conséquence. Avoir accès à l'information et aux renseignements ne veut pas nécessairement dire que ces connaissances sont exploitées comme il se doit par les parties concernées. Une information mise en application n'est pas toujours synonyme d'une information comprise. Et la compréhension ne donne pas toujours lieu à une action, tout comme une action n'équivaut pas nécessairement une solution efficace. Agir grâce aux renseignements acquis, à l'instar d'une réaction face à une problématique client, revient à s'assurer que l'attention portée au problème est constante et globale. Ainsi, ce dernier et ses éventuelles solutions doivent être communiqués aux départements appropriés au sein de l'organisation, et une action qui convient doit être mise en œuvre. En fonction du département concerné, une action peut prendre diverses formes et nécessiter différentes étapes avant d'être adoptée. Certaines formes de risque posé, certains types de gestion ou encore différentes parties de l'entreprise auront potentiellement besoin de briefings ou de comptes-rendus par écrit détaillant les informations obtenues. Les équipes opérationnelles auront quant à elles besoin de données agrégées, analysées et d'un outillage automatisé. Comprendre comment les différents services (et les personnes qui les composent), processus et technologies requises sont structurées, c'est s'assurer que les départements correspondants peuvent agir en conséquence. Veillez donc à toujours garder une approche réaliste lorsque vous travaillez à la réalisation de votre but final.

L'écosystème cyber

Dans le développement d'un écosystème fertile pour la cybersécurité, le partenariat entre État et entreprises est clé. Dans certains pays leaders, le partenariat entre l'armée et les entreprises privées représente même un avantage compétitif important. Il n'est donc pas étonnant de constater que les pays leaders en matière de cybersécurité sont tous des puissances militaires importantes : États-Unis, Chine, Russie, Israël, Royaume-Uni, France. **D'un côté, les économies capitalistes bénéficient de marchés de capitaux liquides et profonds permettant des levées de fonds importantes. De l'autre, les économies plus étatiques comme la Russie ou la Chine peuvent bénéficier des effets d'une planification sur le long terme pour développer leur écosystème cyber.**

En Israël, le directeur général de l'initiative Team8[25] parle « d'avantage injuste » tant l'armée est mise à contribution dans le développement des entreprises privées de ce secteur. Au sein de l'armée israélienne, l'unité 8200 recrute ainsi les meilleurs étudiants pour effectuer leur service militaire dans la cyber. L'unité 8200 est une unité de renseignement de l'Armée de défense d'Israël, responsable du renseignement d'origine électromagnétique et du décryptage de codes. Selon le Directeur des sciences militaires du Royal United Services Institute, un groupe de réflexion britannique spécialisé dans la défense et la sécurité, « l'unité 8200 est probablement la meilleure agence de renseignement technique au monde et se situe au même niveau que la NSA à tout point de vue, sauf l'échelle. »[26]. Après leur service militaire, les jeunes entrepreneurs sont accueillis par l'équivalent de l'unité Team 8200 dans le business, Team8 pour les aider à fonder et à développer leur société. La cybersécurité a été déclarée priorité nationale en 2010. **Depuis, Israël est ainsi devenu en une décennie l'un des leaders mondiaux dans ce domaine avec plus de 300 start-ups actives dans le pays et deux des dix plus importantes entreprises mondiales du secteur.** 20% des investissements privés mondiaux dans la cybersécurité sont à destination d'entreprises israéliennes et plus de 30 entreprises multinationales ont déjà installé leur centre de recherche et développement cyber en Israël[27]. La ville de Beer-Sheva, située au milieu d'une

20%

DES INVESTISSEMENTS PRIVÉS MONDIAUX DANS LA CYBERSÉCURITÉ SONT À DESTINATION D'ENTREPRISES ISRAÉLIENNES.

25. https://team8.vc/
26. https://fr.wikipedia.org/wiki/Unit%C3%A9_8200
27. https://www.businessfrance-tech.fr/2018/11/22/israel-2eme-leader-mondial-en-cybersecurite/

zone quasi-désertique du pays, est aujourd'hui capitale de la cybersécurité du pays, même si de nombreux entrepreneurs continuent de s'installer à Tel Aviv. Depuis 2015, Beer-Sheva regroupe à la fois le bureau national de l'autorité de la cybersécurité, l'Université Ben Gourion dédiée à la question cyber, le centre de cybersécurité de l'armée, le centre d'affaires CyberSpark où un grand nombre de multinationales comme IBM ou Dell ont développé leurs centres stratégiques de cybersécurité.

Aux États-Unis, les agences gouvernementales sont au cœur de l'écosystème cyber. La « National Security Agency » (NSA) a noué des partenariats avec les universités américaines. La CIA dispose de son propre fonds d'investissement In-Q-Tel, qui peut investir dans des entreprises américaines mais aussi étrangères. La « Defense Advanced Research Projects Agency » (DARPA) est l'agence du département de la Défense chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire. Elle a été à l'origine du développement de nombreuses technologies dont les réseaux informatiques, notamment l'ARPANET devenu Internet. La DARPA finance aujourd'hui les thèses des meilleurs étudiants dans la cyber. Les entreprises ensuite créées sont protégées des investisseurs étrangers grâce au « Committee on Foreign investment in the US » (CFIUS)[28]. Le CFIUS est un comité interagences autorisé à examiner certaines transactions impliquant des investissements étrangers aux États-Unis et certaines transactions immobilières effectuées par des personnes étrangères, afin de déterminer l'effet de ces transactions sur la sécurité nationale des États-Unis.

En France, Le Campus Cyber, une tour de 26000 mètres carrés à la Défense inaugurée en février 2022 est le résultat de deux années d'échanges et de discussions entre les acteurs de la cybersécurité et l'État. Il rassemble des représentants d'entreprises de cybersécurité de toutes tailles, des services de l'État, d'instituts de recherche comme l'INRIA et d'écoles spécialisées. Le but est de créer un environnement favorable pour l'innovation technologique et le rayonnement de la filière cyber française. Entre 1600 et 1700 personnes travailleront sur le campus, dont 30% représentant des grandes entreprises et 25% des services de l'État (Agence nationale de la sécurité des systèmes d'information, gendarmerie, police ou services de renseignements, militaires du ComCyber).

28. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

La cyber comme élément de politique industrielle

Pour la plupart des leaders de l'économie mondiale, la cyber fait l'objet, comme la tech au sens large, d'une stratégie claire au niveau de l'État. La Chine et les États-Unis ont ainsi en commun d'afficher une politique de développement technologique dans le cadre d'une vision stratégique au niveau national. C'est essentiel car les investissements nécessaires pour dominer dans des domaines comme l'intelligence artificielle sont gigantesques et nécessitent à la fois une puissance de feu privée venue de géants capables d'investir des sommes considérables, et une volonté publique de développer et soutenir ces technologies. Cela nécessite des programmes de subventions des start-ups, des contrats publics et un plan très clair de développement en infrastructures technologiques civiles comme militaires. Les États-Unis voient la domination technologique comme une arme géopolitique. Leur situation sur le globe, loin du principal foyer de population mondial qu'est l'Eurasie, les contraint à maintenir une domination technologique qui prend le relai d'une domination des routes terrestres et maritimes. Si l'on considère les tendances démographiques à horizon 2100[29], l'Asie comptera cinq milliards d'habitants (contre quatre milliards en 2020) et l'Afrique quatre milliards (contre un milliard en 2020). Ces deux continents représenteront alors 80 % de la population mondiale. Il est donc probable que

CES DEUX CONTINENTS REPRÉSENTERONT ALORS

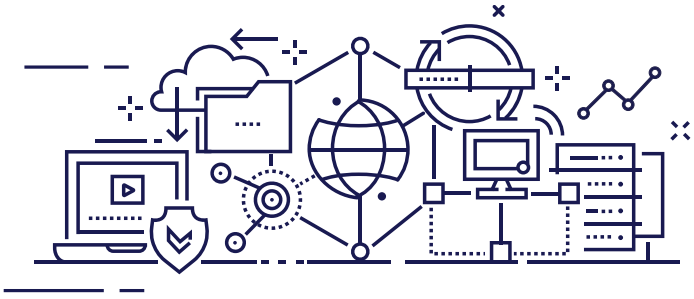
80 %

DE LA POPULATION MONDIALE.

29. Tikehau CIO letter – Just about people, Juin 2021

l'océan Indien devienne le cœur de l'économie mondiale, après l'océan Atlantique au XXe siècle et le Pacifique au XXIe. Or, les États-Unis, qui bordent ces deux derniers océans, ne bordent pas l'océan Indien, qui est aux antipodes par rapport à l'Amérique du Nord. Pour maintenir leur domination économique mondiale, les États-Unis devront être capables de projeter leur puissance loin de leurs frontières. La technologie est en cela essentielle au maintien de leur leadership mondial.

Pour la Chine, l'enjeu est autant géostratégique que domestique : contrôler sa vaste population pour lui assurer un développement économique maîtrisé dans une période d'urbanisation rapide. Dans le contexte de la cybersécurité, l'évolution du modèle de croissance chinois mérite un instant d'attention. L'entrée de la Chine dans l'Organisation mondiale du commerce en 2001 eut pour effet de doubler l'offre de travail globale, provoquant le plus grand choc d'offre de l'histoire économique. La population chinoise en âge de travailler, pléthorique, éduquée et peu chère, contribua à faire du pays, en une décennie, l'atelier du monde et le premier exportateur mondial. La combinaison d'un poids démographique considérable à l'échelle de la planète, d'une intégration dans l'économie mondiale acquise dans des conditions très favorables, et d'un régime politique en contrôle total de l'économie permit à la Chine de réaliser ce qu'aucun autre pays n'a pu accomplir et ce qu'aucun autre ne pourra probablement plus réaliser : passer du statut de pays pauvre en 1980, souffrant de sous-développement et de famines, à celui de première économie mondiale à horizon 2030. Le contrôle de l'économie chinoise par l'État garantit le succès d'un modèle de croissance basé sur des exportations rendues compétitives non seulement par le coût de sa main d'œuvre, mais aussi par une devise artificiellement dévaluée. Mais alors que la population chinoise entame un gigantesque retournement démographique par son vieillissement, cette inversion de tendance coïncide avec la montée des ambitions géopolitiques de la Chine. Ces ambitions s'accompagnent d'un besoin de changement de modèle de développement en imposant sa devise à ses partenaires commerciaux pour construire une sphère d'influence économique. Pour cela, développer une société de consommation importatrice est nécessaire et cela tombe bien puisque le vieillissement ne permettrait plus au pays de rester compétitif avec un modèle exportateur. Ses réserves de change s'amenuisent et sa population en âge de travailler se contracte sous l'effet du vieillissement accéléré par des décennies de politique de l'enfant unique. Les foyers ont souvent deux salaires (le taux de travail des femmes est élevé) et l'enfant unique ayant quitté le foyer, le pouvoir d'achat augmente au point que les dépenses de consommation, en valeur absolue, devraient dépasser celles des États-Unis vers 2024, faisant du consommateur chinois un moteur majeur de la croissance



mondiale. Mais en cherchant à rattraper son retard économique pour augmenter le produit intérieur brut par habitant, la Chine a sacrifié trois éléments : les considérations environnementales qui sont maintenant un frein à son développement, son indépendance monétaire vis-à-vis du dollar américain et son approche égalitaire du communisme. Désormais, l'enjeu pour la Chine est simple : rétablir l'équilibre dans ces trois domaines. **Derrière l'intervention de plus en plus militante du gouvernement chinois dans le secteur de la tech se cache une décision délibérée de mettre moins l'accent sur la croissance économique à court terme en faveur d'autres objectifs : réduire les inégalités, assurer la stabilité sociale et s'attaquer au problème démographique.** L'annulation de l'introduction en bourse de Ant Group, les différentes procédures antitrust engagées contre des géants de la tech en situation de créer des monopoles, ou encore les restrictions sévères imposées à l'éducation en ligne sont autant de messages adressés à la fois aux entrepreneurs chinois et aux marchés : la priorité de la Chine n'est pas la tech ludique ou la tech de consommation mais bien la tech répondant aux priorités de la politique industrielle. C'est-à-dire la tech qui permettra d'assurer l'indépendance vis-à-vis des États-Unis et de réduire les inégalités sociales. Les investisseurs devraient donc privilégier les secteurs que le gouvernement favorise. Parmi ceux-là, la cybersécurité occupe probablement une place de choix.

Les États-Unis et la Chine ont donc intégré la technologie et la cybersécurité au cœur de leur politique industrielle. Israël a fait de même avec une efficacité remarquable. L'Europe n'a pas été aussi systématique dans ce domaine. Les deux leaders dans le domaine de la cybersécurité que sont le Royaume-Uni et la France ont fait le choix d'adopter des politiques de partenariats public-privé dans ce domaine mais ce n'est pas le cas dans tous les pays européens, et le Brexit laisse la France seule en position d'intégrer la cybersécurité dans une politique industrielle à l'échelle de l'Union Européenne.

Cette domination industrielle sino-américaine se double d'une faiblesse politique de l'Europe en matière économique. Il n'existe pas de consensus entre les États membres quant à la nécessité de mettre en place une véritable politique industrielle favorisant

l'émergence d'une industrie numérique européenne. Ainsi, lorsque la France et l'Allemagne parlent de « souveraineté numérique », les pays du Nord défendent une notion d'autonomie stratégique beaucoup plus floue et ne voient l'Europe que comme un marché. Mais en dépit de ses divergences internes, l'Europe a établi les bases d'une vision unifiée de l'espace numérique, fondée sur le refus de la marchandisation des données personnelles et de la surveillance de masse. Au-delà de ces grands principes, plusieurs dispositifs et législations ont été adoptés par l'Union européenne dans le domaine du numérique tels que le RGPD[30] ou le « cyber diplomacy toolbox »[31]. D'autres dispositifs sont en cours d'élaboration comme le « Digital Services Act » ou le « Data Markets Act ». En matière de standards industriels, le « Cybersecurity Act », entré en vigueur en 2019, institue un schéma de certification de cybersécurité s'appliquant à l'ensemble des produits, services et processus IT. Gaia-X a quant à lui pour ambition de créer un standard d'interopérabilité facilitant l'échange de données entre plateformes cloud pour développer « l'économie de la donnée ». La crise ukrainienne aboutira probablement au renforcement de la cohésion européenne en matière de cyber.

L'avenir de l'Europe passe probablement par une réindustrialisation, un rapatriement de l'appareil de production dans le but de renforcer la résilience des entreprises et de créer des emplois. Réindustrialiser, c'est choisir ses priorités et assumer de ne pouvoir être bon partout. Une industrie nationale suppose une demande forte, soit stimulée par la commande publique, soit par l'évolution des politiques d'achat des entreprises en faveur de la structuration d'écosystèmes locaux. L'évolution des comportements individuels privilégiant l'industrie nationale fait également partie de l'équation. L'enjeu de cette renaissance industrielle est aussi de transformer notre système dont la crise a montré l'essoufflement. La crise a fait renaître une envie de produire, d'inventer et d'innover en Europe. Produire en Europe, c'est redonner des perspectives à cette région du monde. Cela signifie investir dans la modernisation, la « numérisation des process » de production et des chaînes d'approvisionnement, mais cela signifie aussi s'exposer au risque cyber. C'est la raison pour laquelle la cybersécurité doit faire partie d'une politique industrielle au XXIe siècle.

30. Règlement Général pour la Protection des Données ou GDRP pour General Data Protection Regulation
31. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf

Éléna POINCET
Co-fondatrice et Directrice Générale de TEHTRIS

Précédemment experte opérationnelle dans la gestion et la conduite d'équipes spécialisées pour le ministère des Armées. Élue « Personnalité IT 2020 du Monde Informatique », lauréate en 2021 du « Bold Woman Award » de la Veuve Clicquot et du Prix « les Margaret » 2022 de la Journée de la Femme Digitale (JFD).

L'hyperautomatisation

au service d'une cybersécurité augmentée

LA MENACE CYBER S'INTENSIFIE ET SE COMPLEXIFIE. LA VITESSE DES ATTAQUES AUGMENTE AU-DELÀ DE LA CAPACITÉ HUMAINE À TRAITER L'INFORMATION ET À RÉAGIR.

Il a été démontré qu'une attaque pouvait ne durer que 37 minutes entre l'intrusion, l'exfiltration des données et le déploiement du ransomware sur un parc numérique. Face à ces menaces inconnues, les équipes responsables des systèmes d'information sont impuissantes si elles recourent seulement à de la détection pour certaines et à de la neutralisation gérée par l'humain pour d'autres. Aujourd'hui, les outils traditionnels ne suffisent plus.

À CETTE PROBLÉMATIQUE D'IMMÉDIATETÉ RENCONTRÉE PAR LES RSSI (RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION) FACE AUX MENACES, TEHTRIS RÉPOND PAR L'HYPER AUTOMATISATION GRÂCE À LA TEHTRIS XDR PLATFORM.

Dès sa conception en 2012, la TEHTRIS XDR Platform a été imaginée et conçue à l'image de l'industrie 4.0 : robotisation intensive, machine learning et deep learning, le tout grâce à notre Intelligence Artificielle Cybéria. Cette approche est orchestrée par notre SOAR (Security Orchestration, Automation & Response) intégré. Ainsi, toute l'infrastructure est surveillée, et les menaces inconnues sont détectées et neutralisées en temps réel et sans aucune intervention humaine. Les informations provenant des différents modules de cybersécurité sont corrélées intelligemment pour offrir une visibilité à 360°.

COMMENT CELA FONCTIONNE-T-IL CONCRÈTEMENT ?

Les modules de la TEHTRIS XDR Platform sont des capteurs intelligents placés sur les parcs numériques qui agrègent et analysent toutes les informations en centrale et permettent d'offrir une vue holistique de la cybersécurité. Ces modules prennent la forme de sondes systèmes - TEHTRIS EDR/EPP/MTD – ayant pour but de protéger les ordinateurs, serveurs, téléphones, tablettes, etc..., et de sondes réseaux - TEHTRIS NTA - visant à surveiller les flux. Le module TEHTRIS SIEM permet de centraliser, de corréler et d'archiver tous les journaux d'évènements de l'environnement du client. TEHTRIS Deceptive Response va d'abord leurrer et détecter les attaquants. Les modules communiquent ensuite, interagissent entre eux grâce au SOAR et remontent toutes les informations aux analystes. Les équipes de cybersurveillance peuvent rapidement proposer des actions d'atténuation et de mitigation du risque. Ce système est doublement performant puisqu'il va s'autoalimenter et apprendre de ses découvertes. La XDR est par ailleurs ouverte dès lors qu'elle peut accueillir tous les modules de cybersécurité du marché.

PENSÉE ET CONÇUE POUR SIMPLIFIER, CENTRALISER ET ORCHESTRER, LA TEHTRIS XDR PLATFORM PERMET AINSI AUX ANALYSTES DE SE CONCENTRER SUR DES TÂCHES À HAUTE VALEUR AJOUTÉE.

Pour s'adapter à l'évolution constante de la menace et du risque, les organisations ont besoin de solutions souples et faciles à opérer, préservant le temps des hommes et femmes de la sécurité, centralisant les informations et optimisant la cybersécurité sans pour autant alourdir les systèmes. L'avenir repose donc sur l'hyper automatisation qui doit offrir une cybersécurité augmentée au service de la protection des entreprises.

IL EST CLÉ DE RAPPELER QU'INITIALEMENT, NOUS ÉTIONS LES PREMIERS À PROPOSER CETTE TECHNOLOGIE.

Aujourd'hui, la TEHTRIS XDR Platform « fête » ses 10 ans et reste la seule plateforme XDR européenne 100 % native capable de détecter et répondre aux cyberattaques en offrant une vue unifiée sur tous les parcs numériques des entreprises et des administrations publiques.

TEHTRIS EST UNE ENTREPRISE EXPERTE EN CYBERSÉCURITÉ ET ÉDITRICE D'UNE SOLUTION DE CYBERDÉFENSE QUI LUTTE CONTRE LE CYBERESPIONNAGE ET LE CYBERSABOTAGE.

La société a été fondée à Pessac en 2010 par Éléna Poincet et Laurent Oudot. La TEHTRIS XDR Platform est au service de tous les secteurs d'activité du monde. L'hyper automatisation des solutions de TEHTRIS est basée sur l'intelligence artificielle et conçue pour détecter et neutraliser automatiquement les menaces inconnues en temps réel et sans recours à l'action humaine. TEHTRIS a finalisé une Série A record de 20 millions d'euros en décembre 2020, menée par Tikehau Capital.

La cyber comme élément de souveraineté

La deuxième révolution industrielle est issue du remplacement du charbon par le pétrole. Par son incroyable efficacité énergétique, le recours au pétrole permit la multiplication des machines et de leur puissance. Dans son livre sur l'histoire du pétrole, Matthieu Auzanneau remarque que dès lors que le pétrole prouve sa remarquable capacité à créer de l'effet d'échelle dans la production, l'asservissement de peuples entiers devient superflu quand il suffit de s'assurer le soutien de quelques chefs tribaux pour l'accès aux concessions pétrolières. Les modalités du contrôle colonial passent alors de l'ordre militaire à l'ordre capitaliste[32]. Au XXIe siècle, la donnée est devenue la matière première de la création de valeur. Comme la plupart des guerres du XXe siècle peuvent être lues à travers le prisme de l'enjeu pétrolier, les conflits du XXIe siècle seront probablement liés à la technologie et à la donnée. Les tensions autour de Taïwan et sa position de leader dans la production de semi-conducteurs en est l'illustration. La collecte des données et son exploitation créent la valeur économique de manière d'autant plus profitable que les quantités considérées sont gigantesques.

> AU XXIe SIÈCLE, LA DONNÉE EST DEVENUE LA MATIÈRE PREMIÈRE DE LA CRÉATION DE VALEUR.

Des tentatives de benchmarking émergent pour mesurer le niveau de souveraineté des États en matière de cybersécurité. L'indice mondial de cybersécurité (GCI) publié par l'Union internationale des télécommunications[33], agence des Nations Unies, mesure la maturité en matière de cybersécurité de 193 pays à travers le monde. L'indice NCSI[34] de Thales fournit quant à lui une évaluation plus spécifique de la souveraineté numérique nationale, aidant chaque nation à déterminer où elle en est et ce qu'elle doit améliorer pour atteindre ses objectifs en matière de stratégie nationale d'éducation, de

32. Or noir, la grande histoire du pétrole – Matthieu Auzanneau, 2015
33. International Telecommunication Union - ITU
34. National Cyber Sovereignty Index™

formation, de recherche, d'amélioration de la cybermaturité des entreprises, de technologie souveraine et de capacités gouvernementales[35].

Mais dans la technologie, les États-Unis et la Chine accentuent leur avance sur les autres nations, au point de menacer la souveraineté des pays tiers. Ces deux pays bénéficient de la taille de leurs « marchés domestiques » de la donnée. Qui plus est, ils sont homogènes en termes de langue, de régulation et de législation. Dans ce secteur, les trois grands blocs économiques mondiaux devraient donc, en théorie, nettement dominer. Mais l'Europe souffre de plusieurs faiblesses structurelles. La première : l'absence de marché domestique européen homogène qui explique probablement l'absence de géant européen de la technologie en face des géants américains et chinois. SAP et Dassault Systèmes sont encore très loin des GAFAM aux États-Unis et des BATX (Baidu, Alibaba, Tencent et Xiaomi) en Chine. L'Europe a également fait le choix de protéger le consommateur en imposant une réglementation stricte sur l'exploitation des données personnelles avec le Règlement Général sur la Protection des Données[36]. Cet aspect est intéressant car il détermine probablement quel bloc pourra prendre le leadership dans le domaine de l'intelligence artificielle. De ce point de vue, la Chine a probablement un avantage considérable, celui de la « démocratie managée ». Le contrat implicite entre le parti communiste chinois et le peuple depuis l'entrée de la Chine dans l'Organisation mondiale du commerce est relativement clair : en échange de l'acceptation par les citoyens chinois de la stabilité du régime, le parti leur offre une augmentation du niveau de vie et la restauration de la place de leader de la Chine dans le monde, qui compte tant aux yeux du peuple chinois. La plus grande tolérance quant à l'exploitation des données personnelles est un avantage compétitif considérable dont dispose la Chine dans la course à la domination technologique.

Si l'on ajoute à cela la qualité du système éducatif, le nombre d'ingénieurs diplômés chaque année, et la puissance de la politique industrielle et des partenariats public-privé, on comprend pourquoi la Chine et les États-Unis font la course en tête dans la tech. En matière de « cloud computing » par exemple, une dizaine d'acteurs, principalement américains, se partagent ainsi 77% du marché mondial. Le premier européen, OVHcloud, ne détient qu'environ 1% de part de marché. Même constat dans le domaine des composants : l'Europe ne produit que 9% des semi-conducteurs mondiaux, un marché très largement dominé par Taïwan. Il en résulte la domination des business de la donnée (stockage, analyse, commerce) par des entreprises américaines et chinoises, posant au reste du monde un problème certain de souveraineté. Les tensions entre la Chine et Taïwan font peser sur

35. https://www.thalesgroup.com/fr/marches/defense-et-securite/solutions-cyberdefense/cyber-souverainete
36. en Anglais GDPR - General Data Protection Regulation - est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Ce règlement a été définitivement adopté par le Parlement européen le 27 avril 2016

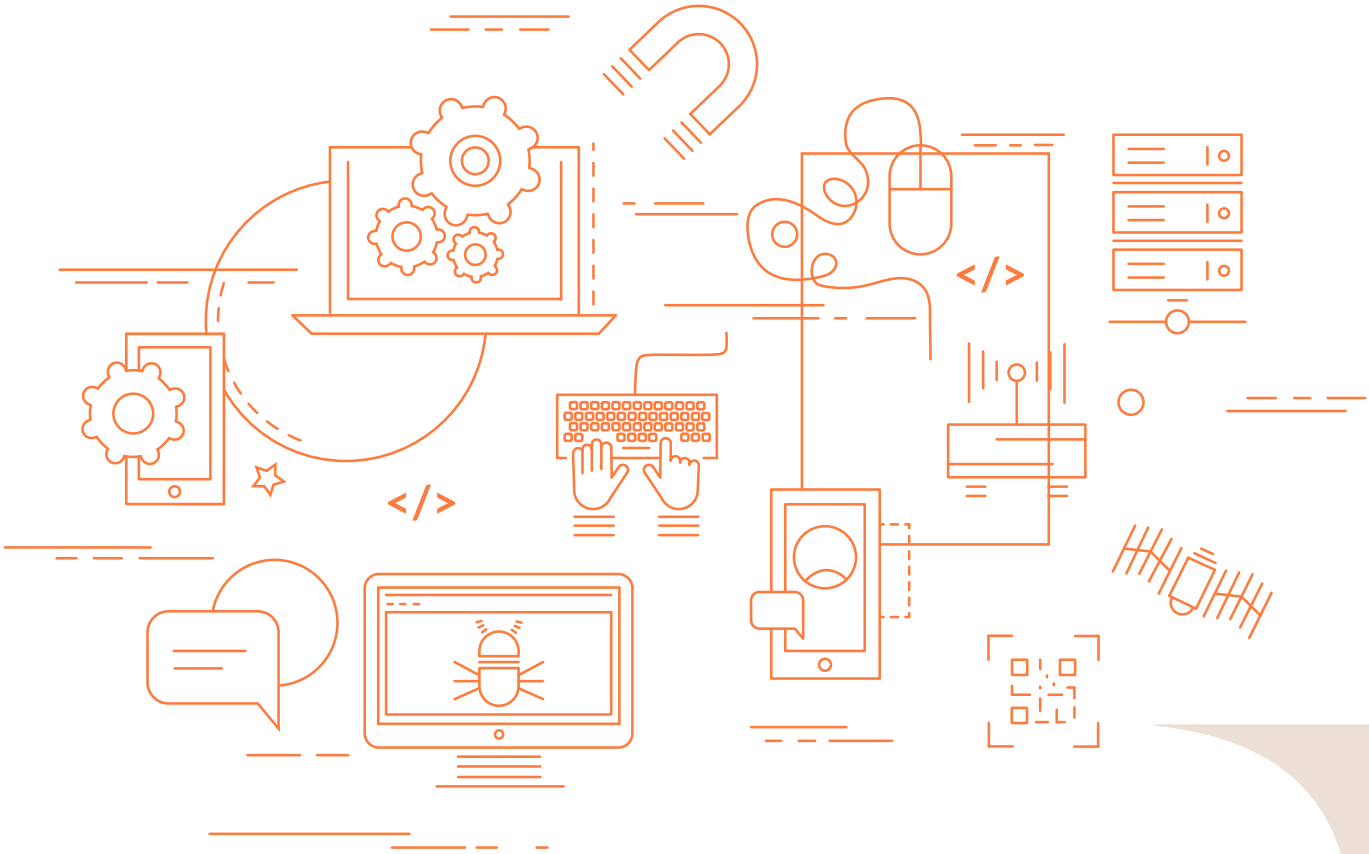
l'industrie des semi-conducteurs et conséquemment sur l'ensemble de l'industrie mondiale un risque fort de perturbations d'approvisionnements. En 2013, l'affaire « Wikileaks » a fait prendre conscience à l'Europe de l'importance de la souveraineté numérique.

La Chine et les États-Unis devraient donc capter la part de plus en plus importante de la création de richesse dans le monde, non seulement grâce à un cercle vertueux de création de valeur pour des entrepreneurs qui réinvestissent dans le tissu local, mais aussi grâce à des entreprises qui, en répondant à des besoins dans le monde entier, tendent vers des positions monopolistiques au détriment d'acteurs locaux. Le cabinet PricewaterhouseCoopers estime ainsi que la diffusion de l'intelligence artificielle va accroître le PIB mondial de 15 700 milliards de dollars entre 2020 et 2030. La Chine seule capterait près de 7 000 milliards de dollars de cette valeur ajoutée[37]. La création de valeur économique se polarise donc sur la tech, et le poids de ce secteur dans l'économie mondiale est tel que ce phénomène modifie les rapports de force et menace la souveraineté de l'ensemble des pays du monde. Il n'est pas étonnant, dans ce contexte, de voir les deux leaders demander aux États et à leurs entreprises de « choisir leur camps ». Ainsi, en 2021, au sommet de l'OTAN à Bruxelles, les Alliés ont entériné une nouvelle politique de cyberdéfense globale qui contribue aux tâches fondamentales de l'OTAN et à sa posture globale de dissuasion et de défense et qui renforce encore la résilience de l'Alliance. **Cette tendance est susceptible non seulement d'accentuer les tensions entre ces deux pays, mais aussi de modifier profondément leur rapport aux pays tiers, notamment dans le domaine de la souveraineté numérique.**

> LA CHINE ET LES ÉTATS-UNIS DEVRAIENT DONC CAPTER LA PART DE PLUS EN PLUS IMPORTANTE DE LA CRÉATION DE RICHESSE DANS LE MONDE.

> LA DIFFUSION DE L'INTELLIGENCE ARTIFICIELLE VA ACCROITRE LE PIB MONDIAL DE 15 700 MILLIARDS DE DOLLARS ENTRE 2020 ET 2030.

37. Sizing the prize – PwC, Anand Rao, Gerard Verweij, Juin 2017



Dans ce contexte, il est probable que l'ensemble des entreprises du secteur soient confrontées au rapport qu'elles entretiennent avec les États sur les sujets géostratégiques. Jusqu'où leur nationalité peut-elle les conduire à servir leur pays d'origine ? Dans quelles mesures leur engagement dans ce domaine menacera leur capacité à se développer en dehors de leur pays ? Quel sera le rapport de force entre des sociétés capables d'investir massivement dans des programmes stratégiques et des gouvernements devant tenir compte de la capacité de nuisance sociale de ces acteurs ?

Dans ce domaine, l'alliance entre l'Américain Google et le Français Thales est intéressante. Les deux entreprises ont annoncé en octobre 2021 la création d'une entreprise commune pour offrir un service de « cloud souverain » en France. C'est à ce jour l'une des rares initiatives de coopération transnationale sur un sujet de souveraineté informatique. L'objectif est de permettre aux entreprises et aux institutions publiques françaises de migrer leurs applications critiques et leurs données sensibles - en bénéficiant d'un ensemble de services cloud opérés par une société de droit français. Cette société majoritairement détenue par Thales, est hébergée en France - au sein d'une infrastructure séparée de celle de Google Cloud dont le réseau et les serveurs seront contrôlés et opérés par cette nouvelle entité. Le support client et la sécurité des services seront réalisés en local par la nouvelle société. Il s'agit notamment de la gestion des identités, du chiffrement des données, de l'administration ou encore de la supervision.

Sauver les démocraties et le débat d'idées

60 % de l'humanité dispose d'un accès à Internet. Il est donc possible pour cette population conséquente d'échanger avec un nombre de personnes dans le monde jamais atteint auparavant, mais aussi d'accéder à une masse d'informations gigantesque. Dans des sociétés moins ouvertes, l'autorité publique incarnait la protection des populations par les pouvoirs régaliens de l'État. Le pacte démocratique tacite documenté par les Grecs et les Romains, consistant pour la population à se soumettre à l'autorité publique en échange de protection, est aujourd'hui mis à mal par l'accès à une information pléthorique. À l'heure où les démocraties doivent faire face à l'épreuve des tentatives de manipulation de l'information, la sécurité des données et des accès à l'information semble essentielle à la défense du modèle démocratique. Car l'accès illimité à l'information rend en réalité plus difficile l'expression des opinions. La mondialisation de l'information aboutit à un appauvrissement du débat d'idées, le nombre de sujets dont on peut débattre diminuant proportionnellement au degré de susceptibilité de tel ou tel groupe de pensée, fusse-t-il situé à l'autre bout du monde. Les tentatives de déstabilisation par manipulation, de production d'informations erronées ou de harcèlement sur les réseaux sociaux sont beaucoup plus simples à mettre en œuvre que lorsque l'information était diffusée exclusivement par la presse ou la télévision. Le réalisme des derniers exemples de « deepfakes » en est l'exemple[38]. Ces phénomènes représentent une menace pour les régimes démocratiques. L'ingérence de puissances étrangères orchestrant une

60 %

DE L'HUMANITÉ A ACCÈS À INTERNET.

38. https://fr.wikipedia.org/wiki/Deepfake

campagne de désinformation en période électorale peut, par ailleurs, influencer l'issue d'un scrutin. Le modèle démocratique semble vulnérable et doit être protégé en partie par une législation forte en termes de cybersécurité mais surtout par des capacités techniques de défense sophistiquées et performantes, voire par une force de dissuasion cyber.

De manière plus pernicieuse, l'accumulation de données sur les habitudes de consommation mais aussi sur ce qui attire l'attention des internautes permet de construire des bulles filtrantes qui menacent le débat d'idées essentiel à la démocratie. L'intelligence artificielle est probablement capable de détecter des biais cognitifs et d'influencer la prise de décision en fonction de ces déductions. En exploitant le biais cognitif incitant l'individu à privilégier et à se satisfaire des informations qui confirment son propre point de vue, ces entreprises enferment le consommateur dans ce qu'Eli Pariser[39] appelle « une bulle filtrante », c'est-à-dire un mécanisme proposant en priorité des produits ou des contenus satisfaisant les orientations, les goûts ou les envies identifiés par l'algorithme. La possibilité pour chacun de choisir sa propre vérité et de se voir conforté dans ses convictions par l'exposition à des opinions non contradictoires présente un risque de cloisonnement détruisant le dialogue. **Dans ce domaine, la cybersécurité n'est qu'une condition nécessaire mais pas suffisante à la préservation du modèle démocratique. Elle ne peut évidemment pas tout, mais la préservation contre les tentatives de falsification de données, de manipulation de vote ou de propagation de fausses informations fait partie de l'arsenal nécessaire à la défense de la souveraineté nationale. C'est le cas pour les démocraties comme pour les autres régimes.**

Pour conserver son intégrité, le cyberespace doit demeurer un espace de liberté et d'échange. La cybersécurité fait désormais partie des stratégies de puissance et des rapports de force qui régissent les relations internationales. L'Appel de Paris pour la confiance et la sécurité dans le cyberespace[40], initiative française dans le domaine de la cyberdiplomatie fixant 9 grands principes, a été signé par 81 pays. L'Organisation des Nations Unies travaille depuis 2004 sur les questions liées à la sécurité et à la stabilité du cyberespace, avec l'objectif d'éviter que le cyberespace ne devienne une zone de non-droit. L'applicabilité du droit international au cyberespace s'impose. Le site Internet du gouvernement français[41] mentionne que l'accent est désormais mis sur l'aide aux pays les moins avancés pour qu'ils puissent élever leur niveau global de cybersécurité dans des domaines comme la protection des infrastructures de télécommunication ou la formation des personnels. Pour contribuer à ces objectifs, la France promeut, avec 53 autres États et l'Union européenne, la mise en place d'un Programme d'action des Nations unies sur la cybersécurité.

39. Eli Pariser – The Filter Bubble, what the internet is hiding from you, 2011
40. https://pariscall.international/en/
41. https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/garantir-la-cybersecurite/

Cyber, espionnage d'État et outil militaire

Les cyberattaques passées menées par des acteurs étatiques ont principalement été utilisées pour la collecte d'informations et non pour la destruction d'équipements ou de données. Il est donc difficile d'estimer l'impact potentiel d'une cyberguerre entre gouvernements. Quelques études ont tenté de modéliser les coûts économiques potentiels de cyberattaques technologiquement possibles contre les infrastructures critiques américaines[42]. Une étude de la Fed de New York estime qu'une attaque réussie contre l'une des plus grandes banques américaines pourrait interrompre 5% à 35% des paiements quotidiens. Une étude de Lloyds estime qu'une attaque extrême contre le réseau électrique du Nord-Est des États-Unis pourrait causer des dommages économiques de 250 millions à 1 milliard de dollars.

En matière de menace cyber, dès 2011, lors du Forum international de la cybersécurité, le vice-président de la Commission européenne Margarítis Schinás avait alerté sur la « situation critique » dans laquelle se trouve l'Europe sous l'effet de la recrudescence des cyberattaques. Lors de ce même événement, la ministre française de la Défense Florence Parly avait annoncé le recrutement de « 770 cyber-combattants en plus prévus pour atteindre 5000 personnels en 2025 au sein des armées, de la Direction générale de l'armement (DGA) et du service de renseignement extérieur français DGSE ». Le général Lecointre, ancien Chef d'État-Major des armées françaises, reconnaissait dès juin 2019, lors d'une audition devant le Sénat français, l'usage de l'arme cyber : « Concernant les opérations extérieures et le danger pour nos forces, là où l'adversaire est capable d'agir dans le champ cyber, nous utilisons cette arme comme une arme du champ de bataille. Nous savons désorganiser un ennemi, le positionner, le traiter. Nous utilisons couramment cet outil. Il y faut des moyens et des spécialistes, mais nous donne un avantage très net au Sahel ou au Levant ».

La crise russo-ukrainienne montre comment la cyber vient complémenter l'arsenal militaire conventionnel dans la désorganisation voire la neutralisation des capacités de l'ennemi. Ainsi,

42. The economic impact of cyberattacks – Goldman Sachs US economics analyst, March 7, 2022

dès le 14 janvier 2022, le site d'actualité militaire Opex 360 mentionnait que l'Ukraine a été la cible d'une cyberattaque ayant visé une quinzaine de sites Internet gouvernementaux, dont celui de son ministère des Affaires étrangères. Avant qu'il ne soit devenu inaccessible, celui-ci avait affiché un texte invitant les Ukrainiens à se « préparer au pire » car toutes leurs données personnelles avaient été « téléchargées sur le réseau public »[43]. L'usage de diverses nouvelles souches de Wiper, malwares de sabotage capables de détruire toutes les données ou les systèmes sur leur passage, a été détecté[44]. Dès le début du conflit, des groupes de hackers ont commencé à s'impliquer des deux côtés. Le célèbre collectif de hackers Anonymous a affirmé qu'il était à l'origine d'une attaque par déni de service distribué (DDoS) qui a rendu inopérant le site d'information russe RT et mené des intrusions dans d'autres chaînes de télévision russes pour diffuser l'hymne ukrainien. Certains groupes de hackers se sont rangés du côté de la Russie comme Conti, The Red Bandits, SandWorm et l'UNC1151 biélorusse. En réponse, Conti a été frappé par une fuite de données interne massive (60 000 messages internes, y compris le code source, ont été rendus publics). Le 24 février 2022, le gouvernement ukrainien a fait appel à des volontaires de la communauté souterraine de piratage du pays pour aider à protéger les infrastructures critiques et mener des missions de cyberespionnage contre les troupes russes. Le 26 février 2022, le vice-Premier ministre ukrainien Mykhailo Fedorov a annoncé la création de la « cyber-armée volontaire ». Parallèlement, la Russie aurait également intensifié ses efforts pour exploiter son propre Internet, dans l'idée de le déconnecter de l'infrastructure mondiale.

Dans l'ensemble, ces cyberattaques ont eu jusqu'à présent des impacts limités, mais le risque de dommages collatéraux sur le cyberespace international existe. Par exemple, le 28 février 2022, la société américaine de communications par satellite Viasat a annoncé qu'elle enquêtait sur une cyberattaque qui a provoqué une panne partielle de son réseau de connexion Internet haut débit résidentiel couvrant l'Europe, y compris l'Ukraine. Les modems terrestres assurant la connectivité entre les satellites et les utilisateurs ont été compromis. Cette attaque a provoqué des dommages collatéraux importants notamment sur le contrôle à distance de réseaux d'éoliennes représentant une capacité de production de 11 gigawatts en Europe centrale.

La crise russo-ukrainienne confirme donc que la cyber fait désormais partie intégrante des nouveaux conflits militaires. A ce titre, il n'est pas étonnant de noter le souhait des États-Unis de créer un « OTAN de la cyber »[45].

43. http://www.opex360.com/2022/01/14/une-attaque-informatique-a-paralyse-une-quinzaine-de-sites-internet-gouvernementaux-ukrainiens/
44. https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/
45. https://www.nato.int/cps/fr/natohq/topics_78170.html

La cybersécurité est au centre de la nouvelle révolution industrielle amenée par l'utilisation de la donnée et de l'intelligence artificielle. Elle est un secteur stratégique dans les politiques industrielles de tous les États au XXIe siècle. Mais l'enjeu cyber va plus loin que les simples considérations défensives et de souveraineté.

Pour assurer sa pérennité sur le long terme et adresser son extraordinaire vulnérabilité mise en exergue par la crise de la COVID-19 puis la crise russo-ukrainienne, l'économie mondiale doit réinventer entièrement son modèle de croissance et créer de la résilience. Au même titre que la transition énergétique, la cybersécurité fait partie de la solution pour apporter de la résilience au système économique. Une économie plus durable passe par l'apport d'une technologie permettant à la fois de rétablir la confiance entre les acteurs économiques et de renforcer la résilience et l'efficience de l'appareil de production. Renforcer la qualité et la traçabilité des biens et des services, préserver les emplois par une bonne résilience des écosystèmes et utiliser la technologie pour recréer du lien social nécessite des investissements massifs dans la cybersécurité. Sans la cybersécurité, pas de confiance. Et la confiance crée de la valeur économique.

La cybersécurité est donc au cœur de la révolution industrielle de la data, dont les enjeux environnementaux, sociaux et de gouvernance sont considérables. Pour la première fois dans l'histoire de l'humanité, les intérêts long terme de l'ensemble de la population mondiale sont alignés. Le risque cyber crée probablement l'une de plus importantes opportunités d'investissement des prochaines décennies.

MAI 2022

CIO letter

TIKEHAU CAPITAL

32, rue de Monceau 75008 Paris - FRANCE

Tél. : +33 (0)1 53 59 05 00
Fax : +33 (0)1 53 59 05 20