Défis de la recherche scientifique en cybersécurité

Par **Claude KIRCHNER** et **Ludovic MÉ**
Inria

Sécuriser un système d'information, c'est assurer la confidentialité, l'intégrité et la disponibilité des ressources qui y sont stockées et des services qui y sont offerts. À cette fin, on doit à la fois protéger ces ressources et services, mais aussi détecter d'éventuelles attaques et y réagir efficacement. Si la sécurité des systèmes et la protection des données personnelles ont globalement progressé durant ces vingt dernières années, beaucoup reste à faire, tant dans la mise en œuvre opérationnelle que dans les phases amont de recherche et développement. Dans cet article, nous nous intéressons aux défis de recherche scientifique que lancent la protection de nos systèmes d'information, la détection des attaques contre ces systèmes et la réaction à ces attaques, sans oublier les défis liés à la connaissance de la menace, à la sécurité de certains domaines particulièrement sensibles, ou aux aspects humains, économiques et sociétaux de la sécurité.

Le numérique et la sécurité

La numérisation générale de nos sociétés nous porte vers une cyber-civilisation globale dont la cybersécurité est un enjeu majeur de viabilité. Cette transformation fondamentale est portée par les avancées scientifiques, technologiques et les innovations et usages qui en résultent, en particulier mais pas seulement dans le domaine du numérique. Paradoxalement, cette situation, inédite à cette échelle, pose à son tour de nouvelles questions scientifiques dans les domaines traditionnels du numérique que sont les sciences informatique, mathématique, électronique, robotique, etc. Compte tenu de ses conséquences profondes sur l'humain et ses environnements sociaux et environnementaux, cette situation interroge aussi les sciences du droit et de l'économie, les sciences humaines et sociales et les sciences de l'environnement qui sont également mises au défi de nous aider à comprendre, maîtriser et assumer les évolutions en cours.

Pour mieux analyser les défis de la recherche en cybersécurité, examinons premièrement les principales raisons de l'impact du numérique depuis le début du siècle dernier.

Le premier point, crucial, est l'émergence scientifique du concept d'information comme un concept fondamental au même titre que la matière, l'énergie et le vivant : *"Information is information, not matter or energy. No materialism which does not admit this can survive at the present day"*(1). Cette identification de l'information en tant que concept fondamental nous permet de comprendre pourquoi la révolution numérique a tant d'impact sur nous. En effet nous sommes des systèmes de traitement biologique de l'information (et nous ne sommes pas que cela bien sûr) et, en tant que tels, nous interagissons avec les systèmes de traitement numérique de l'information que nous avons créés. Ces interactions, d'élémentaires il y a quelques dizaines d'années, sont devenues telles que ces systèmes de traitement d'information biologiques et numériques se complémentent, collaborent et maintenant se combinent avec des conséquences profondes pour l'Humain et ses organisations. La cybersécurité ne peut pas être considérée seulement comme traitant de la

(1) WIENER N. (1948), *Cybernetics: or control and communication in the animal and the machine*, 2nd revised version in 1961. The MIT Press, Cambridge, MA.

sécurité des systèmes numériques, elle doit prendre en compte l'ensemble des éléments entrant en jeu. Nous devons en effet mieux comprendre l'impact des réseaux sociaux, les mécanismes de désinformation, mais aussi appréhender les défenses comme les attaques sur l'ensemble des systèmes d'information. Ces attaques peuvent cibler le système de traitement numérique lui-même (on parlera alors de cyber-attaques) ; elles peuvent aussi utiliser une cyber-attaque pour affecter le traitement d'information biologique humain (comme dans le cas de Cambridge Analytica).

Le deuxième point réside dans l'ampleur du déploiement des systèmes numériques. Il n'est plus de système ou d'organisation qui ne soit peu ou prou informatisé **:** processus industriels, financiers, économiques, de transport ; systèmes de santé ; systèmes de production-transport-consommation d'énergie ; villes et leurs immeubles et habitats ; véhicules automatisés ; système de développement scientifique et technologique lui-même, etc. La numérisation globale de tout notre environnement induit une complexité jamais atteinte à toutes les échelles **:** personnelle, locale, nationale, continentale, globale. La défense de cet ensemble de systèmes de traitement d'information est d'une complexité ainsi jamais atteinte **: i**l n'est pas étonnant que sa maîtrise soit particulièrement difficile.

Le troisième et dernier point que nous voulons souligner ici c'est la rapidité du déploiement et des évolutions des systèmes informatisés. Le rythme de l'avancement des connaissances et des innovations qui peuvent en être issues n'a jamais été aussi rapide de toute l'histoire de l'humanité. Cette rapidité nécessite de mettre en œuvre des stratégies agiles et bien informées pour permettre une défense adaptée et jamais définitive.

Dans ce contexte complexe, intime vis-à-vis de l'humain, totalement pervasif et en évolution rapide et profonde, la cybersécurité a un rôle fondamental permettant d'établir la confiance. Le respect de la vie privée, la confiance dans nos institutions et nos modes d'organisation personnels, familiaux, collectifs, professionnels en dépendent fondamentalement. Quels sont les défis majeurs à relever dans les cinq à dix ans pour qu'en 2030 (demain !) nous puissions encore, et si possible mieux, fonder nos souverainetés numériques personnelles et collectives ?

Des menaces aux défis de recherche

La démarche de sécurisation consiste à d'abord identifier les menaces puis à concevoir des mécanismes de protection et de détection pour les contrer. Un mécanisme essentiel est la cryptographie. Cependant, bien que les primitives et les protocoles cryptographiques soient des éléments fondamentaux de la sécurité, des services de sécurité supplémentaires sont nécessaires, tels que l'authentification et le contrôle d'accès. Ces services de sécurité, généralement fournis par le système d'exploitation ou les périphériques réseau, peuvent eux-mêmes être attaqués et parfois contournés. Par conséquent, les activités entreprises sur le système d'information doivent être supervisées afin de détecter toute violation de la politique de sécurité. Enfin, comme les attaques peuvent se propager extrêmement rapidement, les systèmes de protection doivent réagir automatiquement ou au moins se reconfigurer pour éviter de propager les attaques. Tous ces mécanismes de sécurité doivent être soigneusement intégrés dans les applications critiques pour la sécurité. Ces applications doivent prendre en compte tous les systèmes de traitement et de communication d'information, qu'ils soient humains ou numériques. Outre l'humain dans toutes ses capacités, ils comprennent les systèmes informatiques traditionnels, mais aussi les systèmes industriels et les nouvelles infrastructures distribuées dont en particulier l'informatique en nuage (*Cloud)* et l'Internet des Objets (IoT) dans des déploiements dont la taille va bientôt dépasser le millier de milliards d'objets (tera-objets).

Chaque étape de l'amélioration de la sécurité pose des défis spécifiques. Dans cet article, nous nous intéressons aux défis scientifiques auxquels fait face le monde de la recherche pour chacune de ces étapes, sans prétendre à l'exhaustivité. Les défis que nous présentons ici reprennent en partie des éléments du Livre blanc Inria sur la sécurité numérique [(2)].

Connaître la menace

Rechercher et analyser systématiquement les vulnérabilités

La compromission de la cybersécurité est avérée et malheureusement bien plus profonde que ne le laisse apparaître le sommet de l'iceberg que représentent les attaques détectées. Elle peut avoir des conséquences dramatiques pouvant aller jusqu'à des impacts létaux massifs (qui n'ont pas encore été observés, mais dont on sait qu'ils sont possibles) et des destructions irréversibles à court (cinq ans) ou moyen terme (vingt ans) sur les ouvrages humains et plus globalement l'environnement. Les attaques sont de plus en plus sophistiquées en conception, en moyens déployés pour leur exécution et en capacité destructive.

Connaître son ennemi est un défi toujours aussi important. Une implication plus massive du monde académique des sciences dures comme des sciences humaines et sociales, dans tous les éléments de compréhension et de conception d'attaques existantes ou nouvelles, est souhaitable. L'étude géostratégique des conditions de la cybersécurité présente et à venir (dans les vingt prochaines années) pourra éclairer les décisions politiques à prendre. Cette implication renforcée doit permettre le développement de sciences expérimentales dans le domaine de la cybersécurité, appliquant des méthodologies scientifiques appropriées (éthique, reproductibilité, partage). Quelques laboratoires académiques en haute sécurité informatique existent de manière similaire aux laboratoires P3 et P4 en biologie. Les renforcer sera déterminant pour notre capacité en cybersécurité à observer, mesurer, attribuer, auditer, certifier et contribuer le cas échéant à la standardisation ou la normalisation.

Attaquer le matériel à partir de logiciels

Une catégorie d'attaques relativement nouvelles et évoluées se développe. Elle consiste à exploiter ou produire des vulnérabilités dans les éléments matériels des systèmes de traitement d'information, en commençant par les processeurs. Ces attaques se basent typiquement sur les propriétés physiques de la matière et exploitent l'utilisation dans les processeurs modernes de mécanismes d'optimisation pour gérer les caches, prédire les branchements ou exécuter du code en avance de phase afin de gagner du temps (exécution spéculative). Rowhammer et Spectre en sont des exemples récents. Rowhammer exploite les interactions électriques entre des cellules voisines pour inverser des bits de la mémoire pendant la lecture ou l'écriture d'une autre cellule. Spectre exploite la prédiction de branchement et l'exécution spéculative pour exfiltrer des informations au travers d'un canal caché basé sur l'accès au cache. Ces attaques sont particulièrement dangereuses puisqu'elles permettent d'atteindre les matériels à distance.

Ces attaques reposent sur une cause commune : l'abstraction. Typiquement, quand on propose un mécanisme de sécurité à un niveau donné d'abstraction, on a tendance à considérer que les niveaux inférieurs sur lesquels on s'appuie sont corrects et sûrs, ce qui n'est évidemment pas toujours le cas. Les attaques portent ainsi de plus en plus sur des niveaux d'abstraction de plus en plus proches des aspects physiques, allant des applications vers l'OS, le noyau, le *firmware* et maintenant le matériel.

(2) Coordonné par S. Kremer, L. Mé, D. Rémy et S. Roca, ce Livre blanc, publié en janvier 2019, dresse un tableau global de la sécurité numérique, identifie des défis scientifiques et présente les contributions des équipes-projets Inria : https://files.inria.fr/dircom/extranet/LB_cybersecurity_WEB.pdf

La prévention de ce type d'attaque est particulièrement coûteuse puisqu'elle passe par exemple par la limitation de la réduction de la surface des composants ou le rafraîchissement périodique des cellules par des opérations de lecture ou d'écriture. La détection de ces attaques est elle-même difficile du fait de l'absence de trace disponible au niveau de l'OS ou des applications.

Les défis sont donc ici particulièrement difficiles et aujourd'hui largement ouverts. Ils consistent à élaborer une typologie claire de ces attaques, à obtenir une meilleure compréhension de leur *modus operandi*, et à concevoir des contremesures implantées au niveau logiciel ou au niveau des composants matériels. Ce travail se fera dans un contexte difficile qui peut demander de revisiter des optimisations cruciales et utilisées depuis longtemps telles que l'exécution spéculative.

Protéger

Renforcer continûment la confiance dans le chiffrement

La confiance dans le chiffrement est centrale. Elle repose bien entendu sur la maîtrise des primitives cryptographiques, mais aussi très largement sur la crypanalyse. Pendant de la cryptographie (science de la conception des primitives cryptographiques), la crypanalyse est la science de l'attaque de ces primitives. C'est par une recherche duale en conception et en attaque, s'enrichissant l'une l'autre, que la confiance peut se renforcer.

Le défi est ici d'une part d'organiser la recherche de nouvelles attaques sur les algorithmes de chiffrement, conduites avec des moyens de calcul classiques ou quantiques, en se basant en particulier sur des mesures physiques corrélées aux secrets manipulés algorithmiquement ; d'autre part d'établir formellement des propriétés de robustesse des algorithmes et de leur implantation.

Prouver les protocoles cryptographiques

Les protocoles cryptographiques permettent, par échanges d'informations chiffrées, d'établir des propriétés de sécurité, comme par exemple l'authenticité de l'identité déclarée d'une entité agissant sur le réseau. La sécurité de ces protocoles, qui sont utilisés par exemple pour valider les transactions bancaires effectuées depuis un téléphone portable, est particulièrement délicate. Ces preuves sont en effet longues et complexes, faisant intervenir des interactions multiples entre différents cas. Les preuves réalisées « à la main », même par des informaticiens ou des mathématiciens confirmés, peuvent ainsi contenir des erreurs. La formalisation des protocoles et des propriétés à prouver, associée à l'automatisation des preuves, est la seule manière de parvenir à des preuves sans erreur et donc à un haut degré de sécurité.

Le défi est ici à composantes multiples. La première consiste à spécifier formellement les protocoles au niveau d'abstraction approprié. Ceci nécessite de modéliser l'environnement dans lequel s'exécute le protocole et le niveau d'abstraction, par exemple au niveau langage machine ou au niveau symbolique. Par ailleurs, il faut aussi modéliser les capacités de l'attaquant, son influence sur l'environnement dans lequel le protocole s'exécute, ses connivences éventuelles avec d'autres entités malveillantes. Ce travail permet de détecter et de corriger des erreurs de conception dans les protocoles et éventuellement dans leurs implémentations. Il apparaît aujourd'hui particulièrement important de le conduire dans le contexte de la 5G.

Calculer sur les données chiffrées

L'utilisation pervasive de l'informatique en nuage amène en particulier à considérer l'utilisation du chiffrement homomorphe. Ce dernier permet, par exemple pour l'opération d'addition, de rendre compatible cette opération avec une fonction de chiffrement au sens où la somme des chiffrés est exactement le chiffré de la somme des opérantes. Le chiffrement homomorphe permet donc de travailler directement sur les données chiffrées et d'éviter d'avoir à transmettre ou à

mettre à disposition sur le *cloud* des données non chiffrées. Toute la confiance réside donc dans la qualité de l'algorithme de chiffrement.

La difficulté principale dans ce contexte est de mettre au point des primitives de chiffrement homomorphes qui soient aussi universelles que possible au sens où elles sont homomorphes pour toutes les opérations utiles ou imaginables : on parle alors de chiffrement homomorphe universel ou complet. On sait aujourd'hui construire de telles primitives, mais elles sont de performances (en temps et en espace) faibles si bien qu'il n'est pas réaliste de les utiliser sur les machines et réseaux actuels.

Le défi majeur ici, difficile mais crucial pour renforcer la confiance dans l'utilisation des *clouds*, est de découvrir des primitives cryptographiques homomorphes fiables et efficaces en temps et en espace pour de larges classes d'opérations, si ce n'est universelles.

Chiffrer à l'heure de l'ordinateur quantique

Le passage du modèle de calcul classique de von Neumann à celui du calcul quantique peut changer la complexité de l'exécution d'un programme implantant dans chacun de ces deux modèles une fonction donnée. Les algorithmes tels que RSA, dont la complexité est exponentielle lorsqu'il s'exécute sur un modèle de calcul classique, sont de complexité polynomiale sur une architecture quantique. Dès que des machines quantiques disposant de suffisamment de qubits seront disponibles, RSA ne sera définitivement plus utilisable et les secrets mémorisés aujourd'hui avec RSA deviendront facilement lisibles.

De nouvelles primitives cryptographiques, dites post-quantiques, d'une complexité suffisante pour les deux modèles de calcul, ont été découvertes. Elles reposent sur différentes difficultés mathématiques, comme trouver un vecteur de faible dimension dans un réseau euclidien, ou encore décoder un code linéaire arbitraire.

Le défi est ici aussi particulièrement clair et important. Il consiste à trouver, à analyser et à faire les preuves de complexité pour ces nouvelles primitives cryptographiques. Il faudra aussi gérer en amont le fait que dans les vingt prochaines années (2040 dans le meilleur des cas), la plupart des primitives cryptographiques actuelles devraient ne plus être utilisables, si bien que toutes les informations chiffrées par ces moyens et actuellement conservées deviendront alors vulnérables.

Notons aussi qu'indépendamment du modèle de calcul quantique, l'utilisation de canaux de communication quantiques permet la communication de secrets dont la sûreté repose sur les propriétés quantiques de la matière, ce qu'on considère actuellement comme inviolable. Le défi est ici différent, la capacité à mettre en œuvre de tels protocoles de communication « parfaitement sûrs » étant aujourd'hui opérationnelle sur des distances de moins de 100 km, par exemple entre certaines banques suisses. Le défi, en particulier pour les physiciens, consiste à passer sur des distances plus importantes, par exemple pour communiquer entre le sol et les satellites ou entre sites terrestres éloignés de plusieurs milliers de kilomètres.

Formaliser et prouver pour sécuriser sûrement les systèmes

Actuellement, la sécurité des systèmes d'information repose principalement sur des approches d'ingénierie classiques, non formelles. Cette approche a bien entendu fait ses preuves, mais elle montre aussi des limites, comme les nombreuses attaques rendues publiques le prouvent. Les méthodes formelles apparaissent donc clés pour la mise en œuvre du concept de « sécurité à la conception ». Il s'agit de s'assurer par construction et de prouver de manière formelle et automatisée que telle ou telle propriété de sécurité (par exemple le fait que l'information contenue dans tel ou tel fichier ne puisse être lue que par tel ou tel utilisateur) est garantie par le système et les mécanismes de sécurité qui y sont déployés. Le système contient bien entendu à la fois des

dispositifs de traitement et de transport de l'information. On note d'ailleurs que ces dispositifs tendent à se confondre de par la virtualisation de plus en plus poussée des mécanismes réseau (*Software defined Network,* SDN).

Peut-être encore plus dans ce contexte que dans un autre, les défis sont ici importants et difficiles. Les méthodes formelles ont montré leur efficacité pour prouver la correction des protocoles cryptographiques, comme nous l'avons indiqué ci-dessus. Pour prouver le fonctionnement correct de logiciels (système d'exploitation complet, superviseur et hyperviseur, mécanisme réseau, etc.), il reste cependant encore beaucoup à faire. Un point résidera dans le passage à l'échelle, puisque des codes très volumineux et particulièrement complexes devront être validés. En outre, il faudra être capable de prouver toute la « pile » informatique, depuis les applications jusqu'au *hardware* (on l'a vu, les attaques ciblent de plus en plus les couches basses), en tenant compte aussi, bien entendu, des interactions entre les différentes couches. Les mécanismes de sécurité préventifs et réactifs (voir paragraphe suivant) devront eux-mêmes être prouvés. Pour ne donner qu'un exemple, on peut imaginer prouver qu'un système de détection d'intrusions assure la détection de telle ou telle classe d'attaque. Ce travail complexe aura un coût, qui reste à évaluer précisément, et à mettre en regard du coût de l'insécurité. Ce n'est qu'ainsi que les méthodes formelles pourront s'imposer, à moins que la régulation ne rende leur usage obligatoire, au service de la sécurité et de la protection des données, en particulier personnelles, comme cela est le cas pour la disponibilité de service dans les environnements critiques.

Détecter, diagnostiquer et endiguer les attaques

Détecter intrusions et anomalies

Comme expliqué précédemment, les activités réalisées sur un système d'information doivent être supervisées afin de détecter les atteintes à la sécurité de ce système. Deux approches sont actuellement utilisées : la détection de symptômes connus d'attaques connues (on parle alors de détection d'intrusions) et la détection de déviations d'usage des services informatiques offerts par le système, déviations qui pourraient être un marqueur d'attaques connues ou inconnues (on parle alors de détection d'anomalies). De tels mécanismes sont aujourd'hui largement déployés et utilisés, dans les antivirus, les IDS (*Intrusion Detection Systems*) ou les EDR (*Endpoint Detection and Response*). Cependant, l'efficacité de ces mécanismes reste souvent médiocre. D'une part, rien ne garantit que toutes les attaques seront détectées (risque de faux négatifs), d'autre part (et surtout), les retours d'expérience terrain montrent que des fausses alertes (faux positifs) sont émises, parfois tellement nombreuses qu'elles noient les vraies alertes qui deviennent alors difficiles à identifier par l'administrateur du système.

Actuellement, la détection d'intrusions s'appuie principalement sur l'analyse, paquet par paquet, du trafic réseau. Cette approche est insuffisante. En effet, chaque paquet pris indépendamment est trop pauvre en informations, ce qui limite l'efficacité de la détection, même si divers mécanismes d'agrégation d'informations ont été proposés. En outre la proportion de trafic chiffré augmente (les évaluations existantes laissent à penser que, déjà, de 50 à 80 % du trafic serait chiffré), ce qui rendra à terme obsolète une approche basée sur la recherche de *patterns* dans du trafic en clair. Dans ce contexte, deux défis sont à explorer : d'une part en s'appuyant sur les possibilités que pourrait offrir le calcul sur les données chiffrées (voir ci-dessus), envisager un traitement directement sur le trafic réseau chiffré. D'autre part en considérant que l'information n'est plus disponible sur le réseau, envisager d'autres sources d'information, par ailleurs plus riches sémantiquement, au niveau des applications ou des systèmes d'exploitation par exemple.

La détection d'anomalies est moins utilisée que la détection d'intrusions, même si divers mécanismes ont été proposés pour construire des modèles de référence du comportement du

système d'information. Les activités réalisées sur le système sont confrontées à la référence et une alerte est émise en cas de non-concordance. Il apparaît ici que les approches à succès de l'apprentissage statistique (*machine learning*) sont susceptibles de révolutionner ce domaine, comme elles ont pu révolutionner par exemple celui du traitement d'image. Cependant, l'application de ces techniques aux données à traiter en sécurité n'est pas triviale. Définir précisément ce qui peut être fait et ce qui est hors de portée est un défi en tant que tel. En outre, deux difficultés apparaissent : d'une part, les données qui permettraient de réaliser l'apprentissage sont rarement publiques ; d'autre part, nombre d'approches (*deep learning*, par exemple) souffrent d'un défaut considéré comme majeur en sécurité : on ne sait pas expliquer aujourd'hui les résultats qu'elles livrent. Ces deux difficultés devront être contournées. Une piste de recherche orthogonale serait d'éviter au contraire tout apprentissage : le modèle de référence serait alors fixé, par exemple *via* les spécifications des services offerts, ou *via* la spécification de la politique de sécurité. On analyserait alors la conformité des activités observées par rapport à ces spécifications.

Le test des mécanismes de détection, voire éventuellement leur certification, pose aussi des défis importants. Sur un plan très pratique, il n'existe pas aujourd'hui de plateforme de test librement accessible par les acteurs académiques pour tester leurs idées et les confronter à celles des autres. Une telle plateforme reste donc à construire, ce qui n'est pas simple. Sa disponibilité rendra les expérimentations reproductibles, alors qu'elles ne le sont généralement pas aujourd'hui (on dispose très rarement du code de détection et des données de test utilisées). Nous avons évoqué précédemment la possibilité de prouver les mécanismes réactifs, par usage des méthodes formelles. Les propriétés à certifier pourront par exemple être que telle classe d'attaque est détectable ou, plus généralement, que tel mécanisme est apte à détecter toute violation de telle politique de sécurité.

Par définition, analyser toutes les activités des utilisateurs est potentiellement attentatoire à leur vie privée. Un dernier défi de recherche en lien avec la détection est relatif à la conception de mécanismes de détection respectueux de la vie privée.

Diagnostiquer les violations de sécurité

Aujourd'hui, des *Security Operation Centers* (SOC) reçoivent des alertes (dont beaucoup de fausses, comme mentionné ci-dessus) que des opérateurs humains tentent de caractériser et d'enrichir. Ils utilisent pour ce faire la corrélation d'alertes, fonction importante des SIEM (*Security Information and Event Management*), qui permet par exemple de regrouper dans une même méta-alerte les informations disponibles sur une même attaque qui aurait été détectée par plusieurs outils de détection. Cette forme de corrélation (en fait de fusion d'informations) est utile mais n'offre pas une analyse fine de l'attaque avec reconstruction des étapes du scénario d'attaque et identification des objectifs réels de l'attaquant.

Pour parvenir à ce niveau d'analyse, il est important de prendre en compte, d'une part la nature même du système surveillé (les machines, leurs liens, les services offerts, les outils de sécurité en place et leur configuration, les vulnérabilités connues mais qui n'ont pas pu ou pas encore pu être corrigées, etc.), d'autre part des informations plus globales telles qu'un activisme observé dans telle ou telle partie du monde ou la recrudescence de telle ou telle forme d'attaque. Par ailleurs, le corrélateur doit aussi disposer de la description de scénarios d'attaques possibles, tels que donnés par exemple par une analyse de risque sous la forme d'un arbre d'attaque. Disposant de l'ensemble de ces informations, un défi de recherche important consiste à concevoir un mécanisme automatique de raisonnement sur le flux d'alerte, en mettant par exemple en œuvre des approches relevant de l'IA symbolique.

De manière complémentaire, il est important de conduire des travaux de recherche sur la visualisation de l'ensemble des informations relatives à la sécurité, dont les alertes, bien entendu. Ces informations sont de nature très diverses et sont fortement structurées, certaines étant beaucoup plus importantes

que d'autres. Il faut donc proposer à l'opérateur humain une image la plus pertinente possible de ce qui est en train de se passer sur le système. Il faut en outre lui permettre de naviguer efficacement dans ces données, qui sont extrêmement volumineuses. Au-delà du travail de visualisation, une recherche des bonnes formes d'interaction est donc aussi nécessaire.

Automatiser le déploiement des contre-mesures

Comme les attaques peuvent se propager extrêmement rapidement, les systèmes de protection doivent réagir automatiquement ou au moins se reconfigurer pour éviter la propagation des attaques. Les mécanismes existants aujourd'hui permettent par exemple la fermeture automatique d'un port sur un *firewall* (afin de bloquer une source d'attaque) ou encore la terminaison d'un processus système (là encore, pour stopper une attaque en cours *via* ce processus). Il n'y a pas d'évaluation de l'impact de la contre-mesure et, surtout, pas de raisonnement global sur la politique de sécurité et la manière dont il conviendrait de la modifier.

Si une attaque a réussi, c'est que la configuration des outils préventifs était incorrecte, auquel cas cette configuration doit être revue. Typiquement, la politique de sécurité elle-même était incorrecte ou incomplète, auquel cas cette politique doit être amendée et de nouvelles configurations des mécanismes de sécurité préventifs déployés. On a donc deux types de réactions possibles, l'un portant sur les configurations des mécanismes de sécurité, l'autre sur la politique et ces mêmes configurations. Le défi de recherche est ici d'être capable de diagnostiquer très rapidement l'incident en cours (voir paragraphe précédent), pour déclencher la réaction au plus vite. Un autre défi est de prouver, d'une part que les propriétés de sécurité que la police est censée garantir sont effectivement atteintes, tant au niveau de la politique qu'à celui de son implémentation, d'autre part que les modifications proposées ne perturbent pas les services offerts par le système. En outre, il serait bien entendu intéressant de pouvoir générer automatiquement l'implémentation de la politique (la configuration des outils de sécurité préventifs) à partir de son expression. Pour l'ensemble de ces travaux, les méthodes formelles apparaissent comme l'outil indispensable à la construction de systèmes capables de se défendre eux-mêmes et de s'adapter automatiquement à l'évolution des menaces, dans une forme d'*autonomic computing* que l'on préférera nommer ici « sécurité autonome ».

Notons pour conclure ce paragraphe que nous n'abordons pas ici une autre forme de réaction : la contre-attaque. Les enjeux éthiques, techniques et géopolitiques soulevés sont ici extrêmement délicats. En l'état actuel des connaissances et des capacités techniques, la contre-attaque automatique n'est absolument pas souhaitable et la présence d'humains « dans la boucle » indispensable.

Protéger les données personnelles et la vie privée

Mettre en œuvre le RGPD

Le Règlement général pour la Protection des Données (RGPD) est une avancée fondamentale européenne qui promeut des concepts et objectifs fondamentaux, en particulier pour le respect de la vie privée et la protection des données personnelles, incluant notamment les données de santé. Mais leur implémentation doit encore être développée très largement pour passer de l'énoncé de la régulation à sa mise en œuvre : trop de services et de dispositifs se comportent actuellement comme des boîtes noires, manquant ainsi l'objectif de transparence voulu par le Règlement. Par ailleurs les utilisateurs manquent d'informations et d'interfaces appropriées pour exprimer leur consentement ou leur opposition.

Les défis de recherche qui en résultent consistent premièrement à élaborer des outils d'analyse des risques de mise en cause du respect de la vie privée, et à élaborer des cadres formels permettant

de garantir la correction et l'auditabilité des solutions mises en œuvre. Ils consistent ensuite à concevoir les moyens permettant aux individus de maîtriser leurs données personnelles tout en permettant de gérer l'équilibre délicat entre utilisabilité, partage et respect de la vie privée. Cela implique en particulier de créer de nouveaux moyens, en particulier automatisés, pour exprimer les consentements ou refus et ce, de manière robuste et ergonomique.

Anonymiser les données personnelles

Le respect des données privées repose sur la gestion sécurisée de leur politique d'accès. Leur accès direct doit être préservé ; on retombe là sur les techniques de sécurisation par chiffrement ou par l'utilisation de politiques de sécurité appropriées. Cependant, ces données peuvent aussi être dévoilées indirectement, soit du fait de leur communication à des fins d'exploitation (on aura alors recours à des techniques d'anonymisation reposant typiquement sur la k-anonymisation ou sur la *differential privacy*), soit encore du fait de leur utilisation pour entraîner des algorithmes de reconnaissance basés sur l'apprentissage machine (les données d'entraînement peuvent être dévoilées, au moins partiellement, en ayant accès à l'algorithme de classification issu de l'entraînement initial ou continu).

On aboutit alors à des défis de recherche concernant la conception de techniques d'anonymisation robustes. Le sujet est difficile compte tenu de la diversité des données disponibles permettant des recoupements multiples. Par ailleurs, la distribution des données, évitant *a priori* le bénéfice pour les attaquants d'un accès centralisé, impose de trouver des stratégies de distribution minimisant le coût de l'accès aux données pour les algorithmes d'apprentissage ou d'exploitation.

Assurer la sécurité des contextes sensibles

Nous avons choisi d'illustrer ici l'importance de prendre en compte les spécificités de certains contextes applicatifs sensibles au travers des trois exemples de l'Internet des Objets, des systèmes industriels et des systèmes à base d'intelligence artificielle. Il va cependant de soi que d'autres contextes sensibles sont aussi à considérer, comme celui de la santé ou celui, transverse, de la robotique.

Sécuriser l'Internet des Objets (IoT)

Les attaques contre les dispositifs relevant de l'IoT (les objets connectés) sont relativement faciles, essentiellement car la sécurité n'est généralement pas prise en compte dès la conception de ces objets et des fonctionnalités qu'ils offrent. En outre, le nombre des objets démultiplie les possibilités d'attaques, qui peuvent avoir des conséquences particulièrement graves, tant pour les données personnelles que sur le monde physique, car les objets connectés sont déjà et seront de plus en plus présents dans tous les aspects de nos vies et dans tous les contextes dans lesquels nous évoluons (maison, bureau, voiture, ville, usine, hôpital, etc.).

Les défis de recherche sont ici nombreux. En premier lieu, il faut absolument prendre en compte la sécurité dès la conception des objets, de leur matériel, de leurs systèmes d'exploitation, de leurs capacités de communication courte distance et basse énergie. Comme les ressources de calcul disponibles sur ces objets sont restreintes, la frugalité et la légèreté des mécanismes de sécurité sont essentielles. Ceci vaut bien entendu pour les mécanismes cryptographiques, dont il faut étudier des versions adaptées. Un point particulièrement délicat réside dans la possibilité de mise à jour des logiciels s'exécutant sur les objets (par exemple, suite à la découverte d'une faille de sécurité) et à la sécurisation de ces mises à jour, qui doit certainement s'appuyer sur la cryptographie. Enfin, comme dans les contextes informatiques plus classiques, l'indispensable prévention sera sans doute insuffisante. Il faut donc étudier comment la supervision de l'IoT pourra être réalisée de manière efficace mais légère et autonome (de nombreux contextes d'usage ne disposent pas d'administrateur), afin de permettre la détection d'attaques ou de comportements anormaux de

certains objets de manière plus au moins massive, des centaines de millions d'objets pouvant être impliqués dans les attaques.

Sécuriser les systèmes industriels

Les systèmes industriels reposent de plus en plus, en particulier pour des raisons économiques, sur des mécanismes logiciels et des standards ouverts. Ils peuvent donc être attaqués, comme n'importe quel autre système d'information. Le contexte est bien entendu extrêmement sensible, les conséquences d'une attaque pouvant être catastrophiques. En outre, certains dispositifs actuels seront utilisés encore de longues années, alors qu'ils n'ont pas été sécurisés à la conception. Ils offrent peu de ressources de calcul, ce qui rend difficile voire impossible l'ajout de mécanismes cryptographiques de protection des échanges, par exemple. Leurs spécifications ne sont pas toujours publiques, ce qui rend les dispositifs de sécurité standards (*firewalls*, détecteurs d'intrusions) incapables de traiter leurs flux réseaux.

Les défis de recherche sont bien entendu liés à l'adaptation des mécanismes de sécurité à ce contexte très spécifique, qui nécessite notamment un fonctionnement en temps réel. La coexistence entre des dispositifs modernes sécurisés et des dispositifs anciens qui n'auront pas pu être modifiés doit être soigneusement étudiée ; les protocoles de communications sont particulièrement concernés, car il faudra assurer l'interopérabilité. Enfin, dans un contexte où il sera difficile d'intégrer de nouveaux mécanismes et dispositifs, la supervision apparaît essentielle : l'étude de mécanismes de détection efficaces et spécifiques, aptes à être déployés dans ce contexte sans le perturber, est donc cruciale.

Sécuriser en présence d'apprentissage machine

Les systèmes dits d'intelligence artificielle s'appuient souvent aujourd'hui sur l'apprentissage statistique. Deux grandes menaces sont apportées par ces systèmes. La première est relative à la protection des données personnelles : quelles informations sur les données d'apprentissage est-il possible de tirer d'un réseau de neurones entraîné sur ces données, selon que l'attaquant ait ou n'ait pas accès aux valeurs internes de ce réseau ? La seconde menace est relative à la confiance que l'on peut avoir dans les sorties de ces systèmes. On sait en effet que l'ajout à une image d'un bruit soigneusement choisi et indiscernable à l'œil nu peut entraîner une classification incorrecte de cette image et ainsi conduire à une prise de décision erronée (on parle d'apprentissage antagoniste, ou *adversarial learning*).

Un défi de recherche pour s'assurer de la protection des données d'apprentissage consiste à étudier comment ces données peuvent/doivent être modifiées avant stockage et utilisation. Bien entendu, cette modification ne doit pas (trop) impacter les éléments indispensables à l'apprentissage et donc à la réalisation de la tâche que l'on attend du réseau entraîné. On peut aussi noter ici de manière connexe qu'une autre piste de recherche consiste à étudier une forme d'apprentissage distribué, afin de ne pas avoir à stocker toutes les données d'apprentissage au même endroit et, par là même, de limiter les conséquences d'une attaque potentielle.

La lutte contre l'apprentissage antagoniste nécessite dans un premier temps de comprendre les faiblesses des stratégies d'apprentissage, afin de déterminer précisément les attaques possibles, leur mode opératoire, puis la manière de les contrer. Il convient également d'étudier comment la supervision des interactions internes entre les couches d'un réseau permettrait d'observer et de caractériser d'éventuels artefacts illégitimes. Une telle étude permettra aussi de comprendre comment rendre ces interactions entre couches plus robustes.

Prendre en compte l'humain et ses organisations

Dans les interactions intégrant humains et machines, l'humain comme la machine peuvent être l'attaquant, le vecteur ou la victime. Comme nous le décrivons dans l'introduction, il est donc crucial de maîtriser les interactions, coopérations, combinaisons entre les systèmes humains de traitement de l'information et les systèmes numériques. Les défis de la recherche sont ici multipliés par la diversité des champs disciplinaires concernés, allant des sciences dures aux sciences douces, comme les nomme Michel Serres. Nous présentons ici succinctement quatre défis qui nous semblent importants.

En lien avec la manière dont l'humain traite les informations, un premier défi concerne la compréhension des interactions sociales humaines dans le contexte d'évolution continuelle du média numérique et d'encapacitation numérique globale de la société. Par ailleurs, comme des biais cognitifs peuvent être induits (c'est-à-dire engendrés par manipulation) à l'aide des systèmes d'information numériques, l'instillation de dis-informations (souvent appelées *fake news*) constitue un champ d'étude. L'adaptation fine de ces dis-informations aux cibles humaines visées s'appuie en particulier sur l'usage des réseaux sociaux. Le scandale Cambridge Analytica en est un exemple avéré. Détecter et analyser ces phénomènes est important, mais les contre-mesures seront difficiles à prendre. Elles pourront s'appuyer en particulier sur les avancées issues des points que nous traitons ci-dessous.

Le deuxième défi concerne la compréhension et l'anticipation des impacts géopolitiques, économiques et sociétaux de la cybersécurité. Ces éléments sont bien élaborés par le monde anglo-saxon, moins voire beaucoup moins dans les pays latins et en particulier en France. Des travaux existent, mais il faut aujourd'hui savoir se préparer pour élaborer des stratégies au niveau national et savoir ensuite les défendre au niveau international, en cohérence avec nos alliés. La défense de nos valeurs, mais aussi de nos savoir-faire et de nos entreprises, est à cette condition. Avoir une représentation française étoffée, préparée et cohérente dans les instances de standardisation et de normalisation est un défi en soi.

Le troisième défi important, c'est l'éducation. Les utilisateurs, trop peu conscients des enjeux, sont en conséquence souvent le maillon faible de la chaîne globale de cybersécurité. Une seule réponse technique est insuffisante ; elle doit être accompagnée de la construction d'une culture forte de la cybersécurité. L'éducation en est donc une composante essentielle. Des efforts importants de sensibilisation et de diffusion des connaissances doivent donc être faits, et ce, à destination de tous les publics : citoyens (y compris les enfants et adolescents), techniciens, ingénieurs, experts en sécurité et décideurs économiques ou politiques. Le déficit de compétence en cybersécurité est un handicap majeur pour les souverainetés nationale, numérique, entrepreneuriale et individuelle. Dès l'école, chacun devrait être initié aux bases de l'informatique et de la cybersécurité. Tout au long de la vie, chaque citoyen devrait être (re-)sensibilisé aux « bonnes pratiques » et à la « cyber-hygiène ». Bien entendu chaque utilisateur professionnel devrait être capable d'appréhender les risques liés aux cyber-attaques dans son contexte de travail et devrait connaître les parades possibles ; il devrait donc être formé en conséquence. Les administrateurs systèmes devraient quant à eux être régulièrement formés aux nouvelles menaces et aux nouvelles parades. Enfin, le pays et l'Europe ont besoin de davantage d'experts en cybersécurité : même si des formations sont aujourd'hui proposées par de nombreuses institutions publiques ou privées, des efforts majeurs doivent encore être faits.

Dernier défi évoqué ici, le développement multidisciplinaire d'interactions homme-machine de qualité. Si la technique seule est insuffisante, comme nous venons de le souligner, elle est cependant indispensable. Elle doit être rendue la plus simple d'utilisation possible, les erreurs humaines étant l'une des principales sources des problèmes de sécurité. Ces erreurs sont aussi souvent imputables

à la médiocrité des interactions et des interfaces humains-machines. Ces dernières devraient toujours être conçues pour éviter les erreurs involontaires et s'assurer que l'utilisateur est bien conscient des conséquences de ses actions. La conception de tels systèmes demande encore des travaux de recherche interdisciplinaires entre experts informaticiens et en sciences cognitives.

Conclusion

Il n'y a pas de petit défi en cybersécurité **:** la solidité de la chaîne est celle de son maillon le plus faible. Pour autant, les défis scientifiques liés à chacun des maillons sont de difficultés et de conséquences très variées. Par exemple, l'utilisation de techniques dites d'intelligence artificielle ou de calcul quantique induisent et induiront des disruptions particulièrement importantes et visibles.

Concernant spécifiquement la recherche scientifique, la France a un système académique contribuant au meilleur niveau international à l'avancée des connaissances pour la cybersécurité. C'est tout particulièrement vrai dans les domaines de la cryptologie et des méthodes formelles [3]. Les avancées qui en sont ou en seront issues irriguent un tissu très riche d'entreprises petites, moyennes ou grandes, très bien reconnues internationalement pour leur compétences et leurs savoir-faire. Un défi organisationnel et culturel consiste à ce que les compétences académiques et les compétences d'innovations qui en sont issues collaborent et s'inter-stimulent plus efficacement et facilement, et à ce que les entreprises, les centres de recherche, les écoles et les universités collaborent et innovent ensemble.

À plusieurs reprises nous avons évoqué les valeurs sous-jacentes à notre société. Un défi global, concernant chacun des éléments mentionnés ici, est le développement des réflexions éthiques sur tous les aspects de la cybersécurité. Un tel travail devra puiser ses réflexions aux niveaux individuel, entrepreneurial, local, régional et national et se coordonner au niveau d'un CCNE (comité consultatif national d'éthique) des sciences, technologies, usages et innovations du numérique [4]. Il devra aussi irriguer les réflexions européennes et internationales dans une démarche permettant à toutes ces entités d'expliciter leurs hiérarchies de valeurs et permettant en particulier aux usages et innovations de s'appuyer sur des corpus de réflexions éthiques partageables et, si possible, consistants.

La réflexion que nous avons conduite dans cet article est, par essence de l'exercice, courte et nécessairement schématique et incomplète. Elle s'appuie, outre sur le Livre blanc d'Inria déjà cité, sur de nombreuses feuilles de route dont les lecteurs intéressés pourront continuer à s'enrichir [5]. Enfin, concluons en notant qu'au niveau européen, des projets comme SPARTA [6] visent à bâtir une vision synthétique globale, intégrant notamment l'analyse de feuilles de route au niveau mondial.

(3) https://www.allistene.fr/files/2018/03/VF_cartographie_2017-06-13.pdf
(4) Voir les travaux de la CERNA sur « La souveraineté à l'ère du numérique. Rester maîtres de nos choix et de nos valeurs » http://cerna-ethics-allistene.org/digitalAssets/55/55708_AvisSouverainete-CERNA-2018.pdf
(5) Par exemple : www.ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies, https://it-security-map.eu, etc.
(6) "Re-imagining the way cybersecurity research, innovation, and training are performed in the European Union", https://www.sparta.eu