Cybersécurité

Gildas Avoine [1] et Marc-Olivier Killijian [2]

Cet article a pour objectif de présenter quelques éléments de compréhension sur la recherche académique française en cybersécurité. L'importance de cette discipline pour notre société et les thématiques scientifiques qui la composent sont discutées dans les deux premières sections de cet article. Nous présentons ensuite les travaux de l'alliance Allistene sur la cartographie de la recherche académique française en cybersécurité, puis nous illustrons les activités de recherche de la communauté avec quelques défis scientifiques majeurs.

Cybersécurité dans la société

Évolution de la cybersécurité

L'actualité témoigne de l'importance toujours plus grande que l'on accorde à la cybersécurité, en particulier aux cyberattaques. Il ne s'agit malheureusement pas d'un biais journalistique, mais bien d'une réalité qui se traduit par un accroissement du nombre d'attaques et de leur impact.

Parmi ces attaques, il faut distinguer celles qui sont ciblées de celles qui ne le sont pas. Les premières visent des personnes ou des entités clairement identifiées et sont généralement conçues pour être efficaces sur la cible. Un exemple emblématique est le virus Stuxnet conçu pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. De manière générale, la victime peut être un individu, une entreprise, ou la société toute entière comme le laisse supposer les allégations d'ingérence dans les élections présidentielles américaines et françaises. Les attaques non

1. INSA Rennes, IRISA UMR 6074, IUF.
2. CNRS, LAAS UPR 8001.

CC BY ND

ciblées sont quant à elles des attaques de masse qui reposent sur le fait que certaines cibles seront vulnérables. L'ampleur de l'attaque peut être considérable, comme ce fut le cas avec le réseau Mariposa qui comprenait 13 millions d'ordinateurs infectés. Plus récemment, c'est le rançongiciel WannaCry qui a défrayé la chronique : en touchant plus de 300 000 ordinateurs en seulement quelques heures, WannaCry a mis en lumière le risque bien réel lié aux rançongiciels.

Le temps des hackeurs isolés comme John Draper ou Kevin Mitnick n'est peut-être pas totalement révolu, mais c'est essentiellement le crime organisé, les activités cyberterroristes et le cyberespionnage qui inquiètent aujourd'hui. En formant les étudiants à la cybersécurité, nous formons ceux qui pourront lutter contre la cybercriminalité ou le cyberterrorisme, mais nous formons aussi les cybercriminels eux-mêmes. La cybercriminalité est en effet devenue une affaire d'experts très pointus, qu'ils soient des « *black hat* » ou des « *white hat* »[3]. Comme le soulignait David Naccache [8] lors du colloque de l'INS2I sur la cybersécurité en décembre 2016 : « les fraudeurs auxquels on fait face aujourd'hui utilisent des outils extrêmement avancés, ce sont des ingénieurs doués, ils connaissent très bien les normes et les publications académiques, ils utilisent des contre-mesures anti-expertales, et si jamais vous n'avez pas ça en tête lorsque vous mettez au point une application, elle finira par être cassée. »

Paradoxalement, la cybersécurité est aussi parfois perçue comme un obstacle à la sécurité nationale car elle est utilisée par les personnes malveillantes pour communiquer de manière confidentielle. Le compromis entre surveillance de masse et protection des libertés individuelles doit alors trouver un subtil équilibre acceptable par tous.

Informatique omniprésente

Si la sécurité a connu un tel essor, en particulier durant les 15 dernières années, c'est parce que l'informatique est devenue omniprésente. Il est aujourd'hui difficile d'avoir des activités qui ne font pas appel à l'informatique, même pour les loisirs. Le talon d'Achille est qu'il n'existe généralement pas de procédure pour poursuivre une activité en cas de problème informatique majeur. C'est ainsi qu'une gare ou un aéroport peuvent se retrouver immobilisés tant que l'attaque est en cours. La résilience des systèmes est un sujet important sur lequel les attentions se concentrent et les opérateurs d'importance vitale (OIV) sont particulièrement sensibilisés au sujet.

L'omniprésence de l'informatique implique aussi la multiplication des produits, des services et des acteurs économiques du domaine. Développer une application

3. *Black hat* et *white hat* sont des hackeurs informatiques. Alors que les premiers accomplissent des actions illégales ou malintentionnées, les seconds conservent un comportement éthique. Les *white hat* sont typiquement des experts en cybersécurité qui réalisent des tests de pénétration ou des recherches de vulnérabilités.

informatique sécurisée est une tâche difficile qui requiert des compétences qu'une petite structure ne peut pas toujours s'offrir. La pression financière pour réduire le temps de mise sur le marché rend la tâche encore plus difficile pour les équipes de conception et de développement. C'est ainsi que de nombreuses solutions logicielles sont développées sans prendre en compte l'état de l'art scientifique. La différence entre les connaissances académiques et ce qui est réellement implémenté dépasse souvent l'imaginable. Quelques cas réels sont par exemple : un concepteur qui « mélange » les octets des données d'une carte à puce pour en assurer la confidentialité car la cryptographie est pour lui un concept obscur et inintelligible ; un chef de projet qui ne garde que deux ou trois rondes de l'algorithme de chiffrement AES pour en accélérer l'exécution ; un fabricant de cartes à puce qui continue de vendre son produit alors qu'il est totalement cassé depuis presque 10 ans ; un constructeur de voitures qui utilise la même clef cryptographique dans des millions de véhicules, et dont la clef est accessible via le bus technique de la voiture ; etc. Même les applications les plus sensibles peuvent présenter des faiblesses liées à l'ignorance, ou la volonté d'ignorance de certains industriels. Ainsi le passeport électronique qui a vu le jour en Europe en 2004 (2006 pour la France) a souffert de nombreuses erreurs de jeunesse. Des tests d'interopérabilité internationaux orchestrés en 2008 ont montré que certains logiciels commerciaux de lecture des passeports ne vérifiaient aucune des mesures cryptographiques disponibles sur le passeport ! La cybersécurité n'est donc pas qu'un problème de recherche, c'est aussi et avant tout un problème d'ingénierie, c'est-à-dire qu'il faut pouvoir exploiter les connaissances connues en dépit des contraintes économiques et sociales qui peuvent faire pression. Il serait toutefois facile pour les chercheurs de lancer la pierre aux industriels en se dédouanant de toute responsabilité. Force est de constater qu'il y a aussi un combat qui doit être mené auprès des chercheurs pour rendre plus aisé le transfert de connaissances entre le monde académique et le monde industriel.

Il résulte de cette situation le sentiment que les problèmes vont plus vite que les solutions. C'est en partie vrai. Les primitives qui permettent d'assurer la sécurité sont de plus en plus sûres et les individus sont beaucoup mieux sensibilisés au problème. En revanche, l'omniprésence de l'informatique et de ses conséquences, ainsi que la découverte de nouvelles techniques d'attaque, par exemple celles reposant sur les canaux cachés, qu'ils soient matériels ou logiciels, augmente la surface d'attaque.

Thématiques scientifiques

Contours de la cybersécurité

Selon l'Union internationale des télécommunications (ITU), la cybersécurité est « l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité,

lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement » [7].

Le terme *cybersécurité* est en fait apparu assez récemment, aussi bien en France qu'à l'étranger. Il était à l'origine peu usité par les scientifiques en raison de son manque de précision, mais il devient le terme moderne pour désigner ce que l'on appelait autrefois la sécurité des systèmes d'information ou la sécurité informatique. Il faut souligner que les frontières de la *sécurité informatique* ont beaucoup évolué ces vingt dernières années et que cette terminologie ne recouvre plus l'ensemble des disciplines concernées, notamment sur les aspects humains, sociétaux, économiques et juridiques. La désignation *sécurité du numérique* n'est pas non plus totalement appropriée ; par exemple la protection contre les signaux compromettants [4] n'est pas limitée au monde numérique. La *sécurité de l'information* ne convient pas non plus car la cryptographie, par exemple, peut être utilisée pour du contrôle d'accès physique, sans qu'il y ait nécessairement une information à protéger à proprement parler. Face à cette difficulté de nommer cette discipline à part entière, le terme *cybersécurité* fait son chemin et s'impose progressivement dans la communauté scientifique.

La cybersécurité se situe ainsi à la croisée de nombreuses disciplines telles que l'informatique, les mathématiques, l'électronique et le traitement du signal. Récemment, les dimensions humaine, sociale, économique et juridique se sont ajoutées à l'équation car la sécurité n'a de sens au final que si elle est traitée dans sa globalité. À défaut, certaines dimensions du problème risquent d'être omises, conduisant à une sécurité réelle totalement caduque.

Classification

Les thématiques de la cybersécurité sont extrêmement variées. Plusieurs classifications existent car elles peuvent reposer sur les disciplines sous-jacentes (informatique, mathématiques, électronique...), sur les outils utilisés (méthodes formelles, cryptographie...), sur les objectifs à atteindre (protection de la vie privée, authentification, tatouage numérique...), ou encore sur les champs d'application (contrôle de processus industriels, contrôle d'accès...). Par exemple, la sécurité et la protection de la vie privée (*security and privacy*) est l'une des douze grandes thématiques de l'informatique qui apparaît dans le système de classification de l'ACM (CCS 2012). La sécurité et la protection de la vie privée est ensuite divisée en (1) cryptographie,

4. Les signaux compromettants sont des signaux électromagnétiques parasites – émis par un système logiciel ou matériel – qui peuvent laisser fuir de l'information sensible par rayonnement ou conduction. Il peut s'agir par exemple de signaux émis par un écran ou un clavier connecté par Bluetooth.

(2) méthodes formelles et aspects théoriques de la cybersécurité, (3) cybersécurité au niveau des services, (4) détection d'intrusion et protections contre les programmes malveillants, (5) sécurité des systèmes matériels, (6) sécurité des systèmes logiciels, (7) sécurité des réseaux, (8) sécurité du stockage de l'information et des bases de données, (9) sécurité des logiciels et des applications, (10) aspects humains, sociétaux et éthiques. Il est important de souligner qu'aucune classification ne peut faire l'unanimité et qu'il est difficile de concevoir une classification qui soit une partition de l'ensemble des thématiques.

Le GDR Sécurité informatique [2] (actuellement, pré-GDR), créé par l'Institut des sciences de l'information et de leurs interactions (INS2I) du CNRS en janvier 2016, considère quant à lui sept thématiques, assez proches de celles de la classification ACM, mais qui sont adaptées au paysage de la recherche française. Ces thématiques, déclinées en groupes de travail au sein du (pré-)GDR, sont les suivantes :

— *Codage et cryptographie*
— *Méthodes formelles pour la sécurité*
— *Protection de la vie privée*
— *Sécurité et données multimédias*
— *Sécurité des réseaux et des infrastructures*
— *Sécurité des systèmes logiciels*
— *Sécurité des systèmes matériels*

L'interdisciplinarité de la cybersécurité s'illustre pleinement ici, puisque trois groupes de travail (GT) sont communs avec d'autres GDR : le GT *Codage et cryptographie* (C2) est commun avec le GDR *Informatique mathématique* (IM), le GT *Sécurité et données multimédias* est commun avec le GDR *Information, Signal, Image et ViSion* (ISIS), et le GT *Sécurité des systèmes matériels* est commun avec le GDR *System-On-Chip, System-In-Package* (SoC-SiP).

Thématiques

Afin de comprendre la classification utilisée par le (pré-)GDR Sécurité informatique, chacune des thématiques mentionnées est succinctement présentée dans cette section.

Codage et cryptographie.

La cryptographie vise à garantir la confidentialité, l'authenticité et l'intégrité des informations et des communications. Ces besoins remontent à la nuit des temps mais ce n'est que récemment que l'on peut parler de science. La cryptographie s'est d'abord mécanisée, puis informatisée, et ce sont enfin les mathématiques, dans les années soixante-dix, qui ont révolutionné ce champ disciplinaire. La recherche française en cryptographie est très bien développée et structurée, et elle possède une reconnaissance internationale incontestable. Dire qu'il existe une école française de la cryptographie n'est pas exagéré, et les figures de proue de cette école ont remporté de nombreuses reconnaissances nationales et internationales. Historiquement,

la recherche en cryptographie et en codage s'est structurée en France autour du GT *Codage et cryptographie* qui regroupe environ 450 personnes. Ce GT est affilié aujourd'hui au GDR IM et au (pré-)GDR Sécurité informatique, mais sa création est en fait bien antérieure à celle de ces deux structures.

Méthodes formelles pour la sécurité.

Lors du colloque sur la cybersécurité organisé par l'INS2I en décembre 2016, Hubert Comon [3] débute son intervention en faisant référence aux précédents exposés qui étaient principalement axés sur les attaques : « (...) On n'est pas seulement dans ce cycle infernal où il y a des hackeurs qui cherchent des attaques, je trouve des contre-mesures et je recommence, etc. On peut imaginer autre chose. Par exemple, on prouve la sécurité. Si je prouve la sécurité, point final. » Le domaine des méthodes formelles pour la sécurité vise ainsi à définir de manière formelle les propriétés qu'un système doit garantir, dans le but de mieux les comprendre et de les prouver. Le domaine des méthodes formelles pour la sécurité est très prometteur et il a déjà montré son efficacité sur des protocoles cryptographiques, notamment pour l'authentification dans le passeport biométrique et pour les protocoles de vote électronique. Le chemin est toutefois encore long avant de pouvoir prouver la sécurité d'un système dans sa globalité car une difficulté majeure est de clairement identifier les hypothèses de la preuve. Ainsi, Hubert Comon dans son exposé précise humblement : « Vous allez voir qu'il y a des bémols, ce n'est pas si simple que ça. »

Protection de la vie privée.

Malgré un arsenal législatif relativement fort (au moins en Europe) autour de la protection des données personnelles et une prise de conscience des individus de plus en plus prégnante, nous avons tous le sentiment que nos données personnelles et notre vie privée ne sont pas concrètement protégées. Il existe en effet différentes sources de risques pour la vie privée dans le monde d'aujourd'hui. En particulier, la publicité ciblée sur Internet est devenue une source de financement importante et passe par la collecte massive de données sur les utilisateurs. Les profils des internautes obtenus à partir des nombreuses traces numériques (laissées par les individus eux-mêmes de façon passive, ou collectées activement) intéressent également les acteurs traditionnels de l'économie, telles les banques et les assurances. Enfin ces profils et données personnelles peuvent être utilisés à des fins crapuleuses comme du chantage ou de l'escroquerie par ingénierie sociale. La protection de la vie privée est une question transdisciplinaire où les aspects humains, légaux, mathématiques et informatiques doivent être considérés dans leur globalité et ne peuvent pas être traités séparément.

Sécurité et données multimédias.

La protection de l'information passe aussi par le traitement du signal, notamment mais pas seulement, le traitement des images. Il s'agit d'une thématique importante de la cybersécurité qui traite par exemple de la protection des droits sur les images

et de la stéganographie [5]. La biométrie, qui consiste à utiliser les caractères biologiques intrinsèques à une personne pour garantir certaines propriétés de la sécurité, comme l'authentification, se retrouve également dans la communauté des données multimédias. Il existe évidemment une interaction forte entre cette thématique et la cryptographie.

Sécurité des réseaux et des infrastructures.

La communauté de la sécurité des réseaux et des infrastructures se retrouve en partie dans les communautés de la cryptographie de la sécurité des systèmes logiciels. Il existe toutefois des sujets bien spécifiques à cette thématique, comme, de façon non-exhaustive : la surveillance des réseaux (dénis de service distribués, menaces persistantes...), la gestion des identités et des clefs (cycles de vie), la sécurisation des protocoles distribués (par exemple, la sécurisation du protocole BGP), ou encore la sécurisation des réseaux de nouvelle génération (IoT/M2M, SDN, CDN...).

Sécurité des systèmes logiciels.

La sécurité des systèmes logiciels porte sur la conception de systèmes sécurisés et sur l'analyse des vulnérabilités. Il est essentiel dans cette thématique d'avoir un point de vue vertical qui va du logiciel jusqu'à son interface avec le matériel, mais aussi une approche horizontale qui cherche à couvrir toutes les plateformes déployées. Il faut pour cela prendre en compte la variété des attaques par logiciels malveillants (vers, virus, botnets, rançongiciels, chevaux de Troie...) mais aussi les vulnérabilités liées notamment à des canaux cachés et des corruptions de mémoire. La recherche de vulnérabilités se fait en analysant les programmes de manière statique ou dynamique et doit faire face aux protections logicielles mises en place par les fraudeurs, à savoir l'obfuscation de code [6], le chiffrement et toutes les méthodes d'auto-modification.

Sécurité des systèmes matériels.

La sécurité n'a de sens que si elle est assurée dans sa globalité, on parle d'ailleurs de sécurité de bout en bout. Cela signifie qu'il n'est pas suffisant de concevoir des primitives qui sont sûres sur le papier, il faut qu'elles le restent après leur implémentation sur un système matériel, par exemple une carte à puce. L'informatique est aujourd'hui embarquée dans de nombreux objets de la vie de tous les jours (abonnement aux transports publics, clef de démarrage de voiture, télécommande de garage, téléphone portable...), ce qui illustre l'importance de ce champ disciplinaire. La recherche française est aux avant-postes de la sécurité des systèmes matériels et elle s'est structurée autour de l'axe « confiance matérielle » du GDR SoC-SiP. Ce GDR

5. La stéganographie consiste à dissimuler un message dans un autre message, par exemple insérer un identifiant invisible dans une image.

6. L'obfuscation est une technique de protection de code source contre les attaques par rétro-ingénierie. L'obfuscation consiste typiquement à rendre le code source incompréhensible à un attaquant, sans pour autant impacter les fonctionnalités du programme.

est rattaché à l'Institut des sciences de l'ingénierie et des systèmes (INSIS) et à l'Institut des sciences de l'information et de leurs interactions (INS2I).

Cartographie de la cybersécurité

Depuis quelques années, il y a un besoin significatif en recrutement en cybersécurité en raison d'une pénurie de techniciens et d'ingénieurs formés à ce domaine. À titre d'illustration, le nombre d'offres d'emploi en cybersécurité diffusé par l'APEC est passé de 315 en 2014 à 1133 en 2016 [1]. Il est important de souligner qu'il y a un manque d'experts en cybersécurité, mais aussi un manque d'ingénieurs formés à la sécurité sans pour autant en être experts. Cette pénurie impacte les entreprises privées, les services étatiques, mais aussi les laboratoires publics de recherche. Il est aujourd'hui difficile de recruter des enseignants-chercheurs et des doctorants car les candidats sont happés par le monde professionnel de la cybersécurité.

Bien qu'il n'y ait pas de chiffre officiel, il semble également que les étudiants à fort potentiel s'orientent majoritairement vers des thématiques en lien avec des questions théoriques. Plusieurs champs disciplinaires de la cybersécurité qui ne possèdent pas la même maturité scientifique bénéficieraient pourtant aussi de pouvoir recruter de tels profils. La situation évolue toutefois et on peut se réjouir de voir que le nombre de formations en cybersécurité a explosé ces dernières années et, surtout, qu'elles sont particulièrement attrayantes pour les étudiants.

À partir de ces constatations, il est intéressant de s'interroger sur la répartition des forces académiques en France dans le domaine de la cybersécurité. Depuis 2015, l'alliance Allistene [6] (Alliance des sciences et des technologies du numérique) s'est dotée d'un groupe de travail « Cybersécurité » dont l'une des missions a été le recensement des forces académiques en cybersécurité.

La méthodologie suivie pour réaliser cette cartographie a reposé sur l'envoi d'un questionnaire aux responsables des équipes identifiées *a priori* ou qui se sont déclarées *a posteriori*. Le questionnaire comportait essentiellement deux parties : la première, quantitative, visait à évaluer les forces en termes de chercheurs, enseignants-chercheurs, doctorants, post-doctorants et ingénieurs ; la seconde partie, qualitative, visait à identifier plus spécifiquement les domaines scientifiques de chaque équipe.

Les résultats de cette étude [5] sont riches en instructions. L'étude montre notamment que la recherche française en cybersécurité est composée, à la date du recensement (année académique 2016-2017), d'environ 852 *équivalents temps-plein pour la recherche* (ETP). Notons que cette étude a porté sur l'ensemble des employeurs académiques français : CEA, CNRS, écoles d'ingénieurs, Inria et universités. Les équivalents temps-plein pour la recherche ont été calculés de la manière suivante : un chercheur déclarant travailler à 80 % sur la cybersécurité est comptabilisé à hauteur de 0,8 ETP, alors qu'un enseignant-chercheur également impliqué à hauteur de 80 % sur la cybersécurité est comptabilisé à hauteur de 0,4 ETP.

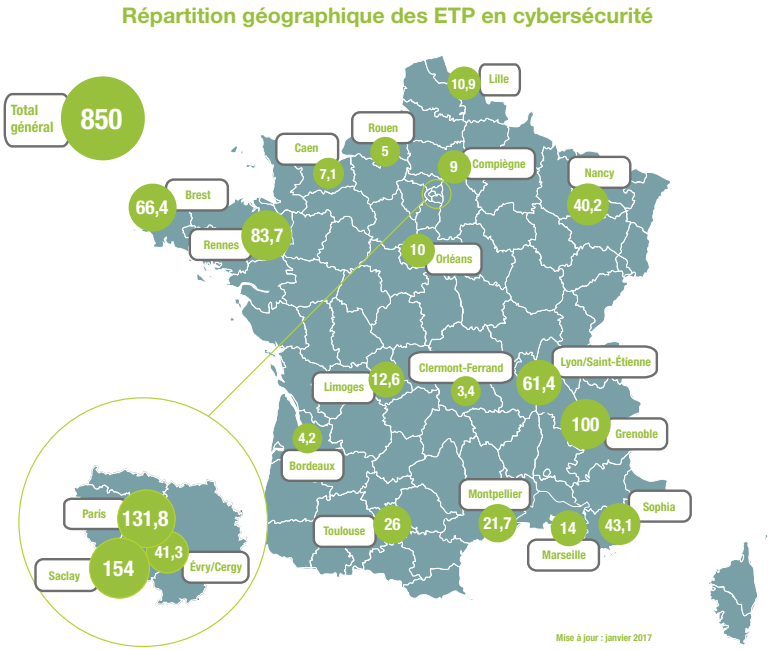

FIGURE 1. Répartition géographique des ETP de la recherche académique française en cybersécurité (janvier 2017).

Les 852 ETP correspondent à 143 ETP chercheurs, 130 ETP enseignants-chercheurs, 126 ETP ingénieurs, 82 ETP post-doctorants et 371 ETP doctorants, répartis sur 1 101 personnes physiques. Les répartitions géographiques de ces ETP et des personnes physiques sont illustrées sur les figures 1 et 2.

La répartition des forces selon les thématiques de la cybersécurité est également une information pertinente, fournie dans la table 1.

Défis scientifiques

Pour illustrer les défis scientifiques auxquels la recherche en cybersécurité devra faire face dans les années à venir, nous avons consulté les responsables des groupes de travail du (pré-)GDR Sécurité informatique. La liste présentée ne prétend pas être exhaustive. Elle n'a pour ambition que d'illustrer le domaine avec quelques défis d'envergure qui occupent les esprits des chercheurs en cybersécurité.

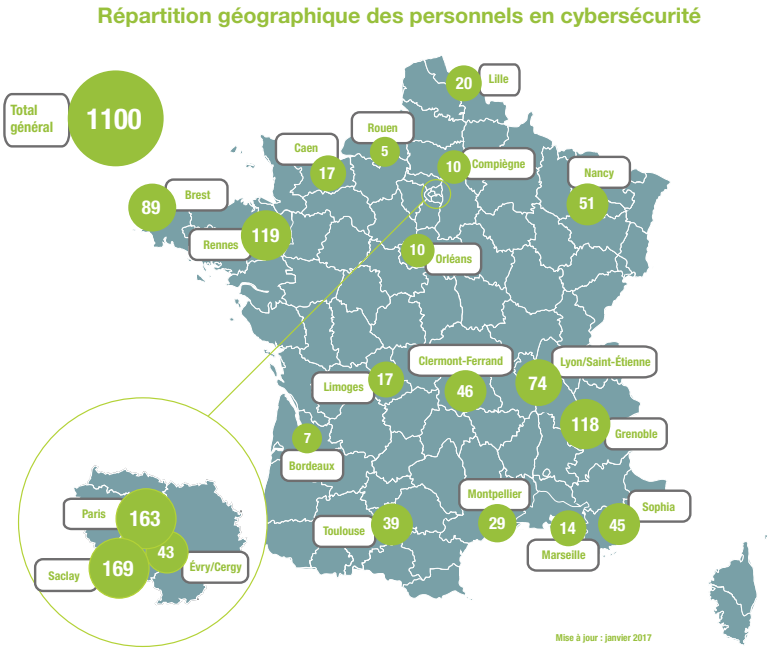

FIGURE 2. Répartition géographique des personnes physiques de la recherche académique française en cybersécurité (janvier 2017).

Logiciels malveillants. Un facteur déterminant pour mener une attaque est la présence de vulnérabilités dans le système visé. La conception d'un système sûr constitue donc un élément primordial de défense. En particulier les attaques ciblées vers une personne ou un groupe de personnes peuvent être sophistiquées, avec des codes d'attaques qui sont obfusqués, chiffrés et auto-modifiants (par exemple, le code ne se déploie qu'après une suite de décompressions et de déchiffrements). Un autre aspect à prendre en compte est la masse de codes malveillants produite, le plus souvent en réemployant une souche connue. Face à cela, un défi majeur de la cybersécurité est d'identifier une attaque en déployant et combinant des approches formelles, des heuristiques d'analyse et des méthodes d'apprentissage.

Attaques physiques. Dans le domaine de la sécurité des systèmes matériels, de nouvelles technologies d'implantation microélectronique (FDSOI, MRAM, RRAM, nanotubes...) doivent être évaluées vis-à-vis des attaques physiques existantes et vis-à-vis de leur capacité à intégrer des éléments essentiels de la sécurité, comme la

Thématique de la cybersécurité	
Cryptographie	20 %
Sécurité des systèmes matériels	17 %
Méthodes formelles et aspects théoriques de la cybersécurité	16 %
Sécurité des systèmes logiciels	10 %
Cybersécurité au niveau des services	8 %
Détection d'intrusion et protections contre les logiciels malveillants	8 %
Sécurité des réseaux	8 %
Sécurité des logiciels et des applications	6 %
Sécurité du stockage de l'information et des bases de données	3 %
Science forensique (analyse du système après un incident)	3 %
Aspects humains, sociétaux et éthiques	2 %
	100 %

TABLE 1. Répartition des activités à travers les thématiques de la cybersécurité, exprimée en pourcentage du nombre d'ETP total.

génération de nombres aléatoires (TRNG et PUF), la mémorisation sécurisée de données sensibles et les services cryptographiques. La recherche de failles de sécurité inhérentes à ces technologies doit être l'un des objectifs prioritaires des travaux à conduire dans les années à venir.

Sécurité matérielle par conception. Un autre objectif fort de ce domaine est le développement de méthodes de sécurité par conception des systèmes sur puces complexes et hétérogènes, avec de nouveaux enjeux comme la gestion des droits de propriété des composants virtuels et des circuits, la protection vis-à-vis de matériels malicieux, la surveillance comportementale des systèmes, la résilience des systèmes matériels sensibles, la garantie des fonctions de test, de diagnostic et de débogage sans préjudice sur la sécurité et la proposition de mécanismes sophistiqués d'authentification et d'identification intrinsèque du matériel (cas des fonctions physiques non clonables, PUF).

Cryptographie post-quantique. Concevoir des algorithmes cryptographiques résistants à l'ordinateur quantique, tel est l'objectif de la cryptographie post-quantique. Étant donné que les problèmes de factorisation et de logarithme discret peuvent être résolus facilement avec un ordinateur quantique, il est important de concevoir des algorithmes alternatifs. Des solutions reposant notamment sur des réseaux euclidiens, des codes correcteurs et des polynômes multivariés existent. Le défi consiste à en améliorer l'efficacité, en réduisant notamment la taille des clefs.

Chiffrement complètement homomorphe. Un défi important dans le domaine de la cryptographie est aussi la conception de chiffrement complètement homomorphe utilisable dans des applications réelles. L'objectif d'une telle primitive est de permettre d'appliquer tout type de fonction calculable sur des messages, sans nécessiter pour cela leur déchiffrement. Une telle primitive permet par exemple de déléguer à une tierce partie (par exemple un serveur dans le *cloud*) l'exécution d'opérations sur des messages, sans pour autant lui révéler le contenu de ces messages.

Vote électronique. Un autre défi important pour notre société est le vote électronique [4]. Le vote électronique présente de nombreux avantages mais il soulève aussi de nombreux défis scientifiques, même si des avancées récentes ont été obtenues dans ce domaine. Par exemple, lors d'un vote par Internet, une difficulté est de s'assurer de l'identité de l'électeur afin de garantir que ce dernier est bien la personne à l'origine du vote et que c'est bien le choix de celui-ci qui a été pris en compte. Cette difficulté doit également faire face aux logiciels malveillants potentiellement installés sur l'ordinateur de l'électeur.

Manipulation d'images. Dans le domaine de la sécurité des données multimédias, garantir une fiabilité très élevée de détection de manipulation d'images (copier-coller, effacement de zones, stéganographie...) constitue l'un des sujets majeurs pour les années à venir. Garantir qu'une image n'a pas été manipulée est, par exemple, fondamental pour les experts judiciaires afin qu'elle puisse constituer une preuve recevable. Plus généralement, l'image prend une place de plus en plus importante dans le monde numérique et CISCO prévoit que les données visuelles (images, vidéos...) représenteront 80 % du trafic sur Internet en 2019.

Conclusion

La recherche scientifique en cybersécurité est étonnante car elle mêle des communautés scientifiques bien établies, structurées et reconnues depuis longtemps, avec des communautés qui posent les premières briques de leur structuration. Afin d'animer ces communautés et leur offrir la possibilité de mieux se connaître, le CNRS a décidé de créer un (pré-)GDR Sécurité informatique. Cette structure qui recouvre des chercheurs de tous horizons permet de mettre en place un réseau scientifique national à travers ses groupes de travail, qui ont d'ores et déjà organisé plusieurs événements scientifiques en 2017. Le (pré-)GDR a aussi mis en place des activités transverses aux groupes de travail, notamment les journées nationales, organisées au siège du CNRS à Paris en 2017, une école pour jeunes chercheurs organisée à Rennes en 2016 et à Bourges en 2017, une semaine de rencontre entre entreprises et doctorants (REDOCS) organisée dans les locaux du CNRS à Gif-sur-Yvette en 2016 et 2017, et enfin un colloque ouvert à un plus large public, « Sécurité informatique : mythes et réalité », en décembre 2016. Prochainement, c'est aussi un club de

partenaires qui verra le jour pour renforcer les liens entre recherche académique et recherche industrielle.

Références

[1] APEC. Cybersécurité en Bretagne : l'enjeu des compétences. Juin 2017.

[2] CNRS/INS2I. Groupement de recherche (pré-GDR) Sécurité informatique. (http://gdr-securite.irisa.fr).

[3] Hubert Comon. Peut-on prouver la sécurité des communications ? Colloque du CNRS sur la sécurité informatique : mythes ou réalité (http://gdr-securite.irisa.fr/colloque.html), décembre 2016.

[4] Véronique Cortier. Vote électronique. *1024 – Bulletin de la société informatique de France*, (9):95–109, novembre 2016 (http://www.societe-informatique-de-france.fr/wp-content/uploads/2016/11/1024-no9-vote-electronique.pdf).

[5] Groupe de travail Cybersécurité de l'alliance Allistène. Cartographie de la recherche académique française en cybersécurité. (https://www.allistene.fr/files/2015/04/2017-06-10-cartographie_final.pdf), 2017.

[6] Allistene (Alliance des sciences et technologies du numérique). (https://www.allistene.fr/).

[7] ITU. X.1205 série X : Réseaux de données, communication entre systèmes ouverts et sécurité – sécurité du cyberespace – cybersécurité – présentation générale de la cybersécurité, avril 2008.

[8] David Naccache. De la puce au cloud, comment fonctionne l'expertise judiciaire ? Colloque du CNRS sur la sécurité informatique : mythes ou réalité (http://gdr-securite.irisa.fr/colloque.html), décembre 2016.