Face au défi Cyber : entreprises et écoles, un duo essentiel

Par Sylvain GOUSSOT
Directeur général de l'EPITA, École d'ingénieurs en informatique

Et Marie MOIN
Directrice de SECURESPHERE, le centre de formation continue de l'EPITA

Volume et complexité croissants, évolutions technologiques majeures, risques économiques et réputationnels, tous ces éléments constituent le cocktail explosif des cybermenaces. Les entreprises et les institutions ont l'impérieuse nécessité de disposer de ressources suffisantes, compétentes et à l'état de l'art. Les dirigeants le savent bien : quand les compétences manquent et que l'exposition aux risques croît, il faut des plans d'action vigoureux et se tourner vers les acteurs proposant des ressources compétentes : c'est le cas des écoles d'ingénieurs du numérique, qui disposent à la fois d'une offre de formations initiales mais aussi d'une offre de formations continues. De l'autre côté du miroir, les écoles du numérique ont besoin des acteurs économiques pour adapter leurs formations et répondre à la demande. Ce duo apparaît comme indispensable pour former les équipes et contrer les menaces cyber d'aujourd'hui et de demain.

Les multiples facettes des professions de la « filière cyber »

La « filière cyber » désigne l'ensemble des métiers, compétences et acteurs qui contribuent à la sécurité des systèmes d'information et à la protection des données et infrastructures numériques. Elle englobe aujourd'hui un spectre extrêmement large de fonctions : de l'opérateur de supervision assurant le *monitoring* en temps réel d'un SOC (Security Operations Center), jusqu'au chercheur en cryptographie post-quantique, en passant par les analystes en réponse à incident, les ingénieurs en sécurité applicative, les architectes sécurité, les *pentesters*[1], les experts en *forensic*[2], les RSSI ou encore les conseillers en gouvernance et conformité réglementaire (RGPD, NIS2, DORA, etc.).

Cette diversité tient à la profonde transversalité de la cybersécurité : elle mobilise des savoirs et savoir-faire relevant de l'informatique, des télécoms, des mathématiques, mais

[1] Ou « *hacker* éthique », le pentester (de l'anglais "penetration testing" teste la résilience d'une entreprise ou organisation ou d'un système aux attaques cyber en jouant le rôle de l'attaquant pour détecter les failles.

[2] L'analyse forensique consiste à investiguer des systèmes d'information après un incident cyber, comme un piratage ou un vol de données. Elle analyse l'ensemble des données du SI pour comprendre ce qu'il s'est passé et en déduire les remédiations nécessaires.

aussi du droit, de la gestion des risques, de la psychologie comportementale ou encore de la communication de crise.

Loin de se limiter à un domaine purement technique, la filière cyber est devenue une filière stratégique, au croisement de multiples disciplines, qui irrigue l'ensemble des secteurs économiques et industriels.

Du point de vue des acteurs économiques, il serait contre-productif de n'aborder la filière cyber qu'à travers le prisme des formations d'ingénieurs. Les besoins en cybersécurité sont massifs et concernent tous les niveaux d'expertise :

- des profils opérationnels de niveau bac+2/bac+3 capables d'exécuter des procédures, de surveiller des journaux d'événements et de maintenir une infrastructure sécurisée ;
- des profils de niveau intermédiaire (bac+3/bac+4) capables de conduire des projets, d'automatiser des tâches de supervision, de configurer des politiques de sécurité ou d'administrer un SOC ;
- et des profils experts ou de pilotage stratégique (bac+5/doctorat) qui conçoivent des architectures sécurisées, auditent, innovent ou orientent la politique globale de cybersécurité d'une organisation.

Le ComCyber (Commandement de la cyberdéfense), rattaché à l'État-major des armées, illustre parfaitement cette logique : il recherche activement des titulaires de bachelors, et pas seulement des ingénieurs. Il a compris que le maillon opérationnel est le plus critique en volume et que le temps de montée en compétence de ces profils est bien plus court, ce qui en fait un levier essentiel pour résorber la pénurie.

Cette réalité du terrain explique l'essor des formations professionnalisantes dans la filière :

- BTS CIEL (Cybersécurité, Informatique et réseaux, Électronique), qui forment en 2 ans des techniciens capables de mettre en œuvre les bases de la sécurité réseau et système ;
- BUT Réseaux et Télécoms ou Informatique, qui permettent en 3 ans d'acquérir des compétences avancées en supervision, administration système et sécurité ;
- Bachelors cybersécurité dans les écoles spécialisées ou d'ingénieurs, qui forment en 3 ans des profils directement opérationnels sur les postes d'analyste SOC, de technicien sécurité ou de gestionnaire d'incidents.

Ces formations courtes sont très recherchées par les entreprises et les administrations, qui les perçoivent comme un réservoir immédiat de talents. Elles répondent aussi à une nécessité structurelle : le besoin de main-d'œuvre qualifiée dépasse très largement le vivier d'ingénieurs disponibles.

Lutter efficacement contre les cybermenaces, une affaire de management ?

En première approche, la cybersécurité est souvent perçue comme une affaire exclusivement technique. Cette représentation s'explique : les attaques informatiques exploitent des vulnérabilités complexes, et leur neutralisation requiert des compétences de haut niveau en réseau, cryptographie, développement sécurisé ou architecture système.

Mais cette image est réductrice. Elle occulte un élément essentiel : la cybersécurité n'est pas qu'un défi technologique, c'est avant tout un défi organisationnel et humain. Les incidents majeurs montrent systématiquement que les failles les plus critiques ne proviennent pas uniquement de faiblesses techniques, mais de dysfonctionnements dans

la gouvernance, l'anticipation, la coordination, la prise de décision, la formation des employés et la gestion du changement.

Autrement dit : renforcer la cybersécurité d'une organisation, c'est mener une transformation managériale à part entière.

Les entreprises et institutions qui parviennent à bâtir une cybersécurité robuste partagent une caractéristique commune : elles ont su mobiliser un arsenal de compétences transverses en complément de l'expertise technique. Ces compétences sont souvent sous-estimées mais décisives :

- management stratégique : définition d'une vision, articulation entre les enjeux *business* et les priorités sécurité, allocation des ressources, pilotage par les risques ;
- conduite du changement : planification et accompagnement des évolutions organisationnelles nécessaires (nouvelles procédures, nouvelles équipes, nouveaux outils), formation continue, communication interne ;
- ressources humaines et GPEC : anticipation des besoins en compétences, cartographie des savoir-faire existants, construction de parcours professionnels en cyber, fidélisation des talents rares ;
- éthique et responsabilité sociétale : prise en compte des impacts sur la vie privée, les libertés individuelles, la confiance numérique et la réputation de l'entreprise.

Ces dimensions relèvent directement du management de haut niveau, et non du seul champ de l'ingénierie. Elles conditionnent pourtant l'efficacité et la pérennité des investissements techniques.

Les dirigeants d'entreprise, les décideurs publics ou les responsables de grandes organisations ont une expérience précieuse : ils ont souvent eu à mener de profondes transformations industrielles, technologiques et humaines (transition numérique, automatisation, réorganisations, fusions, etc.).

Ces expériences leur ont appris une réalité fondamentale : aucune transformation durable ne réussit sans placer l'humain au cœur.

La cybersécurité n'échappe pas à cette règle. La mise en place d'une politique cyber efficace implique :

- d'obtenir l'adhésion des équipes ;
- de faire évoluer les pratiques et les comportements ;
- de créer un climat de confiance autour des enjeux de sécurité ;
- et de construire un écosystème de compétences collaboratif, où experts techniques, responsables métiers et instances dirigeantes coopèrent étroitement.

Lutter contre les cybermenaces suppose donc de passer d'une logique de conformité technique à une logique de culture organisationnelle.

Cela implique :

- d'aligner la cybersécurité sur la stratégie globale de l'entreprise ;
- d'intégrer les considérations de sécurité dans toutes les décisions managériales (achats, RH, innovation, relations clients) ;
- et de responsabiliser l'ensemble des parties prenantes, y compris les comités de direction et les conseils d'administration.

C'est à ce niveau que se joue aujourd'hui la différence entre les organisations vulnérables et les organisations résilientes : celles qui réussissent à faire de la cybersécurité un levier

de performance et non une contrainte, et qui transforment leurs collaborateurs en acteurs conscients, compétents et engagés de la sécurité numérique.

Aux fins de relever ces défis humains et organisationnels, les écoles d'ingénieurs ont depuis longtemps des programmes de formation qui intègrent ces dimensions dans l'acquisition de compétences. Les étudiants et futurs jeunes diplômés manqueront certes d'expérience dans ces champs de compétence mais auront *a minima* les premiers réflexes qui ne les cantonneront pas à l'exercice de leur savoir-faire technique. Les programmes de formation continue ne sont plus seulement destinés à des collaborateurs, cadres et managers des fonctions techniques mais également à toutes les forces vives des organisations.

Acquérir des compétences ou former ses équipes ? Un choix souvent présenté… mais artificiel

Face à l'ampleur des cybermenaces et à la pénurie de talents disponibles, les dirigeants se trouvent souvent face à un dilemme apparent : recruter des experts déjà opérationnels ou former leurs équipes existantes pour les faire monter en compétences.

En réalité, cette opposition est trompeuse. L'un ne peut plus se concevoir sans l'autre :

- les profils « prêts à l'emploi » sont rares et chers ;
- et les formations longues prennent du temps à produire leurs effets.

La seule stratégie soutenable consiste à articuler acquisition et développement des compétences dans une logique d'écosystème. Autrement dit, intégrer en continu de nouveaux talents tout en faisant évoluer en parallèle les collaborateurs en poste, pour créer une dynamique d'apprentissage permanent.

Or, cet objectif suppose que les formations elles-mêmes soient extrêmement réactives et étroitement connectées aux besoins du terrain.

La cybersécurité est un domaine qui évolue à une vitesse inédite : nouvelles attaques, nouvelles réglementations, nouvelles technologies (IA générative, *cloud* souverain, quantique, etc.).

Les cursus doivent donc s'actualiser en permanence, anticiper les compétences émergentes et proposer des formats flexibles, adaptés aussi bien aux jeunes en formation initiale qu'aux professionnels en reconversion ou en formation continue. Cela exige un modèle pédagogique qui dépasse les silos traditionnels et qui associe étroitement tous les acteurs de la filière.

Les écoles d'ingénieurs et de spécialité occupent une position singulière et stratégique dans cet écosystème. Elles se trouvent au croisement de tous les flux de savoirs et de besoins. Elles captent les signaux faibles de l'innovation scientifique et technologique grâce à la recherche. Elles traduisent les besoins opérationnels et les contraintes réglementaires en compétences grâce à leurs liens étroits avec les entreprises et institutions. Elles s'alignent sur les priorités de souveraineté, de résilience et de sécurité économique en réponse aux recommandations des gouvernements et agences nationales. Elles préparent les futurs experts et cadres dirigeants en formation initiale. Elles assurent la montée en compétences et la réorientation des professionnels déjà en activité vers les métiers en tension.

Ce positionnement en fait de véritables « maillons d'adaptation », capables d'agréger les tendances, d'orienter les contenus et de déployer rapidement les formations adéquates. Ce sont, en somme, des capteurs et des catalyseurs : elles perçoivent les besoins émergents, mobilisent leurs réseaux académiques et industriels, et transforment ces signaux en offres de formation concrètes et opérationnelles.

Dans un domaine où les menaces se réinventent chaque semaine, cette capacité à aller plus vite est déterminante. Elle seule permet de réduire le temps de latence entre l'apparition d'une nouvelle menace et la disponibilité de compétences adaptées, de renforcer la souveraineté numérique et de garantir la résilience des organisations. C'est cette agilité systémique, à la fois académique, scientifique et industrielle, qui doit guider l'action publique et les choix d'investissement en matière de formation cyber.

Aller à la rencontre les uns des autres : une dynamique collective et sociétale

Renforcer la filière cyber ne peut pas reposer sur un modèle linéaire et cloisonné de formation puis d'embauche. Il faut dépasser la relation « école → stage → emploi » pour bâtir de véritables partenariats continus et intégrés entre les écoles et les entreprises.

Concrètement, cela suppose que les entreprises :

- interviennent tout au long du parcours des étudiants, dès les premières années (conférences, projets tutorés, situations d'apprentissage et d'évaluation (SAE), mentorat, participation aux jurys) ;
- ouvrent leurs environnements techniques à travers des challenges, des immersions, des visites ;
- et co-développent des contenus pédagogiques avec les équipes enseignantes.

Dans ce modèle, les étudiants ne sont plus seulement formés pour rejoindre le marché, ils sont acteurs du marché dès leur formation : ils participent à des *hackathons* ou des CTF (Capture The Flag, les *hackathons* de la cyber), des compétitions techniques et des projets concrets, en collaboration directe avec les entreprises, les institutions et les chercheurs.

C'est cette approche immersive et partenariale qui permet d'accélérer leur professionnalisation tout en nourrissant l'innovation pédagogique.

Encore faut-il que les jeunes générations aient envie d'investir ce champ exigeant.

Les signaux sont encourageants : dans l'enquête de rentrée menée par l'EPITA auprès de ses nouveaux entrants, 65 % d'entre eux considèrent que la cybersécurité est le domaine qui les attirent le plus.

Plusieurs leviers peuvent expliquer selon nous cet attrait croissant :

- la forte présence de la cyber dans les séries et les films, qui en donnent une représentation positive et valorisante ;
- l'engagement citoyen et de défense, qui motive de nombreux jeunes à contribuer à la protection des institutions et des infrastructures ;
- et une sensibilité accrue à l'importance des données personnelles et aux considérations éthiques, très marquée dans cette génération.

Cet intérêt spontané est un atout majeur, mais il doit être entretenu et canalisé par une pédagogie qui met en valeur le sens et l'impact sociétal des métiers du numérique sécurisé.

Former des experts cyber ne suffit pas : encore faut-il que leurs compétences diffusent et irriguent l'ensemble du tissu économique et institutionnel. C'est ici que le rôle sociétal des écoles et des grandes institutions prend tout son sens.

À travers leurs réseaux et leurs dispositifs, elles doivent contribuer à : essaimer les compétences dans les territoires, accompagner les PME, les collectivités, les hôpitaux,

les administrations qui sont souvent les plus vulnérables aux cyberattaques, mettre à disposition leurs ressources pédagogiques et leurs expertises, et soutenir les initiatives de montée en compétences collectives portées par les pouvoirs publics.

Un programme comme CYBIAH piloté par le Campus Cyber, lieu totem de la cybersécurité qui rassemble les principaux acteurs nationaux et internationaux du domaine, accompagne gratuitement les TPE, PME, structures de l'économie sociale et solidaire et collectivités franciliennes dans leur montée en maturité cyber, en proposant un parcours complet allant de la sensibilisation à la mise en œuvre de solutions personnalisées, illustre cette logique de mobilisation nationale coordonnée, où chaque acteur, écoles, entreprises, institutions, État, contribue à la protection de l'écosystème numérique français.

Conclusion

Former à la cybersécurité devient alors un acte citoyen, qui vise à protéger non seulement les grandes entreprises stratégiques, mais aussi les services hospitaliers, les infrastructures territoriales et l'ensemble des usagers du numérique.