ENJEUX DE CYBERSÉCURITÉ DANS L'ENSEIGNEMENT SUPÉRIEUR ET LA RECHERCHE

PAR PATRICK HETZEL, DÉPUTÉ DU BAS-RHIN

La cybersécurité concerne aujourd'hui de très nombreux secteurs. Ainsi, l'enseignement supérieur et la recherche sont fortement concernés. À la fois, parce que l'on attend que l'enseignement supérieur et la recherche développent des outils de protection grâce à des recherches de pointe dans le secteur, qu'ils puissent transmettre les connaissances et les savoirs y afférents et enfin, qu'ils diffusent une véritable culture de la protection dans un milieu où l'on sous-estime fréquemment les risques.

À l'ère du numérique, la cybersécurité est devenue un enjeu stratégique pour tous les secteurs. L'enseignement supérieur et la recherche (ESR), en France, n'échappent évidemment pas à cette dynamique. Si ce domaine est parfois perçu comme moins exposé que d'autres, il constitue pourtant une cible privilégiée, comme le rappellent plusieurs rapports de l'ANSSI (2022) et du ministère de l'Enseignement Supérieur et de la Recherche (MESR, 2021).

Un secteur à la fois ouvert et vulnérable et une recrudescence des attaques ciblées

L'ESR repose sur une culture d'ouverture, de coopération internationale et de diffusion libre du savoir. Or, cette ouverture entre en tension avec les exigences de sécurité numérique (Barlatier et Meissonier, 2020). En effet, les universités et instituts de recherche gèrent de nombreuses données sensibles : résultats de recherche, informations personnelles, brevets, données médicales, etc. Une étude de la Cour des comptes (2022) souligne que ces établissements sont désormais très vulnérables, notamment du fait d'une gouvernance parfois lacunaire des systèmes d'information et d'une sous-estimation du risque réel qui lui, n'a cessé de croître.

C'est ainsi que depuis 2020, plusieurs attaques spectaculaires ont touché les universités françaises, notamment à Montpellier, Lyon ou Versailles (CERT-ESR, 2023). Le rapport de Thales (2023) sur les menaces cyber identifie l'ESR comme secteur à risque croissant, notamment pour l'espionnage scientifique. Le recours croissant aux ransomwares, phishing ou attaques par déni de service distribué (DDoS) s'inscrit dans une tendance mondiale (ENISA, 2023) et les organismes de recherche d'une part et les établissements d'enseignement supérieur et de recherche d'autre part, ne sont pas épargnés.

Les attaquants, parfois liés à des États, cherchent à s'emparer d'informations stratégiques sur des domaines sensibles : IA, quantique, défense, santé. Une note de l'Institut Montaigne (2021) évoque les liens entre cybersécurité et souveraineté scientifique, soulignant que le monde académique est devenu un champ d'affrontements géopolitiques de plus en plus important.

Des moyens humains encore limités et l'impérieuse nécessité d'une vraie réponse institutionnelle

Malgré une prise de conscience, les établissements manquent souvent de ressources humaines et techniques. Les DSI (directions des systèmes d'information) peinent à recruter des profils qualifiés, la concurrence du privé étant forte (Peyrat et Boudinet, 2021). La fragmentation des outils, l'hétérogénéité des réseaux, ou encore le maintien de systèmes obsolètes fragilisent l'ensemble (ANSSI, 2022). À cela s'ajoute un déficit de culture de cybersécurité chez de nombreux usagers. Un rapport

du Haut Conseil de l'évaluation de la recherche et de l'enseignement supérieur (HCERES, 2022) rappelle que la sensibilisation reste inégale, en particulier dans les laboratoires peu connectés aux DSI centrales.

Face à ces défis, plusieurs dispositifs ont vu le jour. Le CERT-ESR, piloté par RENATER, coordonne les réponses aux incidents depuis 2022. L'ANSSI publie des guides pratiques adaptés au secteur académique, dont le « Guide de cybersécurité pour les établissements d'enseignement supérieur » (2023). La stratégie nationale « Campus Cyber », lancée par l'État en 2022, ambitionne de structurer l'écosystème cyber en favorisant la synergie entre monde académique, industriel et institutionnel (SGDSN, 2022). Des appels à projets comme ceux du programme PEPR « Cybersécurité » financent la recherche sur la sécurisation des systèmes critiques, ou encore sur les aspects éthiques et juridiques de la cyberdéfense (CNRS, 2023). Lorsque j'étais ministre de l'enseignement supérieur et de la recherche, conscient des enjeux, j'avais veillé à ce que le secrétariat d'Etat au numérique et à l'intelligence artificielle me soit rattaché, car cela permettait d'agir très en amont pour améliorer notre souveraineté non seulement en matière économique et industrielle mais aussi en matière de recherche. Seule façon de lutter efficacement par rapport à des acteurs mondiaux comme les Etats-Unis, la Chine ou encore la Russie.

Trouver l'équilibre entre sécurité et ouverture

Former à la cybersécurité devient une priorité. Certaines universités ont lancé des formations dédiées (par exemple des masters dédiés à la cybersécurité), mais les besoins dépassent les cursus techniques. La mission Bothorel (2021) recommandait d'introduire une culture numérique et sécuritaire dès la licence, voire avant dans chaque cursus universitaire. Des modules de sensibilisation se mettent en place pour les personnels administratifs et enseignants-chercheurs mais d'importantes marges de progression subsistent. Il s'agit aussi de former des citoyens : comprendre le fonctionnement des technologies, leurs vulnérabilités, et les responsabilités qu'elles impliquent (Floridi, 2016). Le développement de formations interdisciplinaires (cyber-éthique, droit, géopolitique) est un levier majeur pour l'autonomie stratégique de la France dans le concert des nations.

La particularité du monde académique impose une approche équilibrée. Sécuriser les systèmes sans nuire à la liberté académique suppose une gouvernance souple, une mutualisation des ressources, et une co-construction des politiques de sécurité. Une étude récente de l'université Paris-Saclay (2022) souligne l'importance d'une approche « orientée usages », prenant en compte les besoins des chercheurs.

La cybersécurité n'est plus un enjeu secondaire ou purement technique. Elle touche à la capacité même de l'université, des grandes écoles et des organismes de recherche à remplir leurs missions. Protéger les données, les infrastructures et les personnes est devenu un impératif académique qui nécessite un véritable pilotage institutionnel. Plus que jamais, les enjeux liés à la cybersécurité doivent être pris très au sérieux et traités méthodiquement.

Références bibliographiques

ANSSI (2022). Cybersécurité dans l'enseignement supérieur : état des lieux et recommandations.

Barlatier, P.-J., & Meissonier, R. (2020). Cybersécurité et culture académique : une tension organisationnelle. Revue Française de Gestion.

CERT-ESR (2023). Rapport annuel sur les incidents dans l'ESR.

Cour des comptes (2022). La gestion des systèmes d'information dans les universités.

ENISA (2023). Threat Landscape Report 2022–2023.

Floridi, L. (2016). The Ethics of Information. Oxford University Press.

HCERES (2022). Sécurité numérique et qualité de la recherche

Institut Montaigne (2021). Souveraineté numérique : pour un réveil européen.

SGDSN (2022). Stratégie nationale pour la cybersécurité 2021-2025.

Thales (2023). Cyber Threat Intelligence Report.