

[Cybersécurité] « Un sujet qui n'est plus cantonné aux directions informatiques » (P-A. Muller, France U)

News Tank Éducation & Recherche -
Paris - Actualité n°454460 - Publié le 06/10/2026 à 09:42

Imprimé par - abonné # - le 09/10/2026 à 09:46



Pierre-Alain Muller - © Valentine Poulain

« Les gouvernances des universités ont globalement pris conscience que la cybersécurité n'est plus un sujet cantonné aux directions informatiques. Nos missions fondamentales sont avant tout l'enseignement et la recherche, mais on ne peut pas mettre la cybersécurité de côté. C'est une question de continuité de service public et de protection du patrimoine scientifique des universités, et donc de plus en plus aussi une question de souveraineté », déclare [Pierre-Alain Muller](#), référent numérique de France Universités, à News Tank le 20/09/2026.

Président de l'Université de Haute Alsace et président du Cines (Centre informatique national de l'enseignement supérieur), il présente la vision de la cybersécurité portée au sein de la conférence des présidents d'établissements. « Nous avons pris conscience que les universités sont des cibles particulièrement exposées aux cyberattaques, avec une particularité : parfois, les attaquants sont chez nous. Beaucoup d'organisations sont attaquées de l'extérieur, alors que nous, on est aussi attaqués par nos propres "apprentis hackers" qui sont chez nous. »

En matière de défense contre les menaces et les attaques, il estime que « la réponse doit être collective : les établissements, France Universités, l'Anssi (Agence nationale de la sécurité des systèmes d'information), l'Ofac (Office français anti-criminalité), Renater (Réseau national de télécommunications pour la technologie l'enseignement et la recherche), etc. C'est un écosystème, ça ne peut pas être une juxtaposition d'acteurs qui font chacun des choses différentes de leur côté ».

Cet entretien paraît dans le cadre d'une série d'articles que News Tank consacre aux enjeux de cybersécurité dans les établissements d'enseignement supérieur et de recherche.

« Nous ne sommes pas en capacité de promettre le risque zéro »

« Nous ne sommes pas en capacité de promettre le risque zéro aujourd'hui. Il faut donc s'entraîner à être résilient, se préparer à l'idée qu'on va être attaqué, s'entraîner à redémarrer, et savoir communiquer sur le fait qu'on est attaqué », déclare Pierre-Alain Muller.

Dans cette perspective, le sujet de la cybersécurité dépasse les seuls informaticiens. « Protéger une université, c'est protéger le patrimoine scientifique de la Nation : les données et résultats de recherche, la propriété intellectuelle, les infrastructures, avec l'IA, le calcul intensif, les données massives, et demain les outils quantiques. » À ces enjeux s'ajoute celui de la sobriété, « parce qu'on se pose légitimement la question de ce que tout ça va consommer ».

Mutualiser les efforts

Le référent numérique de France Universités constate que tous les établissements « n'ont pas le même niveau de cybersécurité en interne ».

« Il faut donc que nous utilisions aussi des dispositifs mutualisés qui viennent renforcer la cybersécurité. C'est important d'avoir des compétences en interne, mais aussi que des éléments viennent en soutien, de structures qui peuvent se spécialiser davantage sur ces aspects de sécurité, à l'image de Renater. »

Renater est, en France, le réseau de télécommunications reliant les différents établissements d'enseignement supérieur et de recherche publique entre eux en métropole et dans les départements d'outre-mer.

L'impact de la directive NIS-2

Il évoque également l'impact de la directive européenne NIS-2 (Network and Information Security), adoptée en décembre 2022, dont l'objectif est de mettre en place des mesures destinées à assurer un niveau élevé commun de cybersécurité.

« C'est une bonne nouvelle. Cela remet en avant les préoccupations de sécurité, et permet d'arrêter certaines discussions sans fin qu'on peut avoir en interne sur ces sujets. Ce serait un peu la même chose que pour la décision prise par le Premier ministre concernant la visioconférence : il y avait de nombreuses solutions différentes, et une décision a été prise d'adopter celle déployée par la Dinum (Direction interministérielle du numérique). »

« Chaque fois qu'on fait ce genre de chose, je pense que c'est positif. On peut être des établissements autonomes, tout en n'étant pas obligés de réinventer la roue chacun de son côté. Si on a des directives ou des recommandations, je pense que c'est globalement une bonne chose. »

Le cas de l'Université de Haute-Alsace : « une organisation de plus en plus stabilisée, avec du personnel permanent dédié »

« Dans les universités, quand une problématique émerge, on nomme un chargé de mission ou un vice-président. Ce dernier commence à travailler, puis on se rend compte que cela représente plus de travail que ce qu'un vice-président peut assumer seul. Ensuite, on recrute du personnel permanent, de type Biatss (Bibliothèques, Ingénieurs, Administratifs, Techniciens, Social, Santé), qu'on place dans les services et qui consacre son temps à assurer une permanence de la mission », indique-t-il.

« Sur mes deux mandats, nous avons suivi exactement cette trajectoire. Nous avons déjà une direction du numérique, nous avons déjà un RSSI (Responsable de la sécurité des systèmes d'information), mais qui faisait cela en plus de sa mission de base d'enseignant-chercheur. Il en a été de même pour le rôle de FSD (Fonctionnaire sécurité et défense) (fonctionnaire sécurité défense), qui faisait aussi cela en plus de son poste. »

« Aujourd'hui nous avons transitionné vers une organisation de plus en plus stabilisée, avec du personnel permanent dédié. »

Une responsabilité collective

Il indique avoir identifié au début de son mandat plusieurs éléments de sécurité qui ont parfois mis du temps à être déployés, à l'image de la double authentification. « Cela a pris, à mon sens, trop de temps. Or on a vu une vraie différence dès qu'on l'a mise en place. Avant, tous les jours, des étudiants ou des enseignants se faisaient piquer leur code d'accès, et ensuite notre université servait de relais pour des envois de spam, ce qui nous faisait blacklister. Depuis la double authentification, cela a baissé considérablement. »

« Les équipes techniques étaient au départ très concentrées sur la sécurité des réseaux. Maintenant, nous essayons d'expliquer aux collègues que ce n'est pas un sujet réservé à un service : c'est nous tous, en tant que communauté, qui devons apprendre à nous défendre. Cela devient une responsabilité collective liée à la capacité du service public à être résilient face aux cyberattaques. »

Un cas vécu de cyberattaque réputationnelle

Pierre-Alain Muller évoque une cyberattaque qu'il a vécue lors de sa réélection à la tête de son université en 2024 : « du contenu généré en grande quantité sur internet, relayé par les réseaux sociaux, puis par de la presse militante ».

« À la fin, les enquêteurs spécialisés en cybercriminalité se sont rendu compte que c'était un collègue en interne qui en était à l'origine. C'est une cyberattaque réputationnelle, pas une attaque pour voler des données. Je pense qu'il faut qu'on s'y prépare. Je ne suis pas le seul président d'université à avoir eu ce genre de problème de réputation. Et cela nuit globalement à l'image de l'université, c'est pourquoi j'y suis sensible. »

Dans le cadre d'une attaque visant les systèmes d'information, le plus difficile est de se rendre compte de cette attaque, indique Pierre-Alain Muller : « Cela peut prendre plusieurs jours. Ensuite, redémarrer un minimum d'informatique peut prendre plusieurs mois, et revenir à un état stable peut prendre jusqu'à trois ans. » Il cite les cas de l'INP (Institut national polytechnique) de Grenoble ou de l'Université de Paris-Saclay.

« On est tous les jours attaqués et en face on durcit notre système tous les jours un peu plus. »

Les différents niveaux de cybersécurité

Pierre-Alain Muller liste les différents niveaux de cybersécurité. « Si on regarde les infrastructures en différentes strates :

- tout en haut, vous avez les supercalculateurs et les infrastructures européennes, qui ont un très bon niveau de sécurité ;
- ensuite les datacenters labellisés, qui sont également très robustes ;
- en dessous, il y a les 70 universités, chacune devant se défendre un peu toute seule, ce qui est potentiellement problématique ;
- et enfin il y a les machines, que chacun gère de son côté. Là, il faut faire œuvre de pédagogie, il faut par exemple expliquer aux gens qu'on ne peut pas ouvrir des réseaux wifi pirates. »

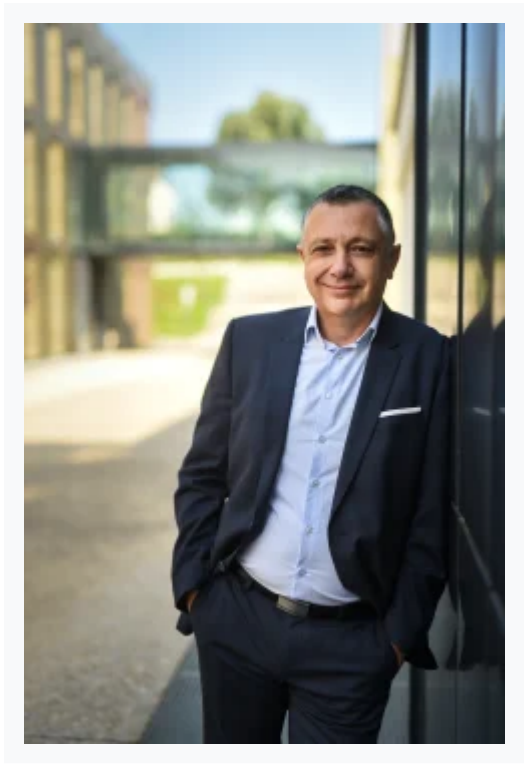
« Certains types de données sont plus sensibles que d'autres, les données de *santé* étant les plus délicates. Il y a des labellisations spécifiques pour ça. Le Cines, par exemple, est en train de devenir un centre national d'hébergement pour les données de santé », ajoute-t-il.

« La souveraineté est un bon vecteur pour sensibiliser les communautés »

Concernant les réactions des personnels quant aux mesures de cybersécurité mises en place à l'université, le président de l'UHA (Université de Haute-Alsace) indique : « très attachés à la liberté, ils peuvent ressentir les mesures de sécurité comme un frein ».

« Il doit encore y avoir des collègues qui n'ont leurs données stockées que sur leur ordinateur personnel. Nous essayons évidemment de leur fournir des espaces de stockage sauvegardés dans les datacenters, avec du stockage à froid en plus du stockage à chaud, pour pouvoir repartir sur des bases à partir de bandes si on est attaqué. »

« Mais dans l'esprit du chercheur, je vois plutôt une soif de liberté qu'un rejet de la sécurité en tant que telle. Ce qui marche assez bien dans le discours actuel - et l'on peut remercier Donald Trump [président des États-Unis] pour cela - c'est d'aborder le sujet sous l'angle de la souveraineté. Elle peut être plus facile à expliquer que la sécurité, qui peut sembler lointaine ou technique. C'est un bon vecteur pour sensibiliser les communautés aux besoins de cybersécurité. »



Pierre-Alain Muller

Président du CA @ Centre informatique national de l’enseignement supérieur (Cines)

Président @ Université de Haute-Alsace (UHA)

Professeur @ Université de Haute-Alsace (UHA)

Parcours

Depuis avril 2025	Centre informatique national de l'enseignement supérieur (Cines) Président du CA
Depuis janvier 2021	Université de Haute-Alsace (UHA) Président
Depuis mars 2010	Université de Haute-Alsace (UHA) Professeur
Juin 2012 - janvier 2021	Université de Haute-Alsace (UHA) Vice-président innovation
Février 2015 - août 2018	Université de Haute-Alsace (UHA) Directeur de l'École du numérique UHA 4.0
Septembre 2008 - mars 2010	Université de Haute-Alsace (UHA) Vice-Présidente exécutif
Juillet 2007 - août 2008	Université de Haute-Alsace (UHA) Vice-président Systèmes d'informations
Septembre 2004 - août 2006	Institut national de recherche en informatique et en automatique (Inria) Chercheur senior
Juillet 2002 - août 2004	École supérieure des sciences appliquées pour l'ingénieur de Mulhouse Maître de conférences
Juillet 1999 - juin 2002	Objexion Software SA P-DG
Décembre 1994 - juin 1999	Université de Haute-Alsace (UHA) Maître de conférences
Décembre 1993 - novembre 1994	École supérieure des sciences appliquées pour l'ingénieur de Mulhouse Ater

Établissement & diplôme

Novembre 2006

[Université de Rennes 1](#)
Habilitation à diriger des recherches

1990 - novembre 1993

[Université de Haute-Alsace \(UHA\)](#)
Doctorat

Fiche n° 26110, créée le 29/09/2017 à 15:07 - Màj le 05/10/2026 à 15:49



Université de Haute-Alsace (UHA)

L'Université de Haute-Alsace (UHA, Université de Mulhouse) est une université pluridisciplinaire hors santé.

Catégorie : Universités
Entité(s) affiliée(s) : [Ensisa \(École nationale supérieure d'ingénieurs Sud Alsace\)](#)

Adresse du siège
Learning Center
4 Rue des Frères Lumière
68093 Mulhouse Cedex 2 France

Général

Date de création	1975
Statut	EPCSCP (Établissement public à caractère scientifique, culturel et professionnel)
Tutelles	Ministère chargé de l'ESR
Implantations (dont siège)	Mulhouse (siège) et Colmar
Alliance d'universités européennes	Epicur (membre fondateur en 2019)
Présidence	Président : Pierre-Alain Muller (réélu le 02/12/2024)

Effectifs étudiants

2006-07	7 511
2007-08	7 618
2008-09	7 673
2009-10	7 941
2010-11	8 134

2011-12	7 991
2012-13	7 738
2013-14	7 586
2014-15	7 842
2015-16	8 050
2016-17	8 186
2017-18	9 493
2018-19	10 203
2019-20	10 423
2020-21	10 448
<i>Source(s) : Open Data Esri</i>	

Inscriptions principales et secondes (source : Open data du Mesri)

Effectifs de doctorants contractuels

2021-22	72
2020-21	72
2019-20	70
2018-19	65
2017-18	66
2016-17	58
2015-16	54
2014-15	55
2013-14	58
2012-13	57
<i>Source(s) : Open Data Mesri</i>	

Effectifs E-C titulaires

2023-24	325
2022-23	332
2021-22	338
2020-21	338
2019-20	331

2018-19	325
2017-18	327
2016-17	326
2015-16	332
2014-15	330
2013-14	333
2012-13	335
2011-12	337
2010-11	335
Source(s) : Open Data MESR	

Maîtres de conférences et professeurs des universités exclusivement.

Produits encaissables (M€)

Budget initial 2023	121,2 M€
2022	116,1 M€
2021	109,1 M€
2020	105,8 M€
2019	97,0 M€
2018	92,4 M€
2017	91,5 M€
2016	91,6 M€
2015	93 M€
2014	90,2 M€
2013	89,7 M€
2012	86,9 M€
Source(s) : Open data MESR	

Les produits encaissables correspondent aux produits de fonctionnement de l'exercice qui se traduisent par un encaissement (à différencier des produits sans flux de trésorerie). Ils comprennent essentiellement la subvention pour charges de service public et les ressources propres.

Dépenses de personnel (M€)

Budget initial 2023	82,8 M€
2022	77,4 M€

2021	75,2 M€
2020	73,1 M€
2019	71,4 M€
2018	69,7 M€
2017	68,5 M€
2016	67,3 M€
2015	67,0 M€
2014	66,6 M€
2013	66,8 M€
2012	65,1 M€
2011	63,7 M€
2010	61,5 M€
Source(s) : Open data MESR	

Fonds de roulement (en jours)

Budget initial 2023	84,2
2022	129,9
2021	118,6
2020	108,0
2019	95,8
2018	95,0
2017	95,9
2016	81,3
2015	77,0
2014	63,0
2013	48,3
2012	56,5
2011	77,3
2010	82,1
Source(s) : Open data MESR	

Résultats PIA

Excellences

Vague 1 (2021) : 10,7M€

NCU

Projet ELAN (2017) : 6,85M€

AMI Demoos (2021)

Projet Demo UHA : 6M€

Saps

Vague 3 (2024) : 251k€

Fiche n° 1494, créée le 19/02/2014 à 11:42 - MàJ le 30/09/2026 à 17:08

© News Tank Éducation & Recherche - 2026 - **Code de la propriété intellectuelle** : « La contrefaçon (...) est punie de trois ans d'emprisonnement et de 300 000 euros d'amende. Est (...) un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une oeuvre de l'esprit en violation des droits de l'auteur. »