COMMUNIQUÉ DE PRESSE

À Nancy, le 29 janvier 2025

CYBERSECURITÉ

Cyber Humanum Est : étudiants, militaires et entreprises réunis pour le plus grand exercice universitaire de cyberguerre, avec un scénario immersif intégrant l'IA générative.

Les cyberattaques se multiplient à un rythme alarmant, exacerbées par la montée en puissance de l'intelligence artificielle. Face aux enjeux de sensibilisation, de formation et de recrutement dans ce domaine, le COMCYBER, la Base de Défense de Nancy, l'Université de Lorraine, et Lorraine INP ont organisé une nouvelle édition du Cyber Humanum Est, l'exercice universitaire de référence en cyberguerre. Du 27 au 29 janvier 2025, cet événement a rassemblé 200 participants plongés dans une immersion totale hors-norme. Leur mission ? Résoudre un scénario inédit, conçu pour repousser les limites de leurs compétences, et intégrant pour la première fois l'intelligence artificielle générative.

Une immersion unique au cœur de scénarios réalistes

Sous le patronage du Commandement de la Cyberdéfense (COMCYBER) et en partenariat avec des acteurs académiques, industriels et institutionnels de renom, l'exercice a proposé deux thématiques majeures :

- L'intelligence artificielle (IA) : exploration des impacts de l'IA sur la manipulation d'informations via des deepfakes et des techniques avancées d'influence.
- Simulations sectorielles : des maquettes de réseaux ferroviaires, infrastructures portuaires et sites industriels illustreront les vulnérabilités critiques de secteurs stratégiques français.

Un scénario enrichi pour 2025 : un contexte géopolitique et écologique complexe

Inspiré par le contexte géostratégique actuel, le scénario de l'édition 2025 a plongé les participants dans un archipel imaginaire où les infrastructures vieillissantes et les tensions géopolitiques exacerbées mettent en péril la stabilité économique et sociale. Les enjeux incluent :

- choix stratégiques : faut-il investir dans des infrastructures critiques ou se tourner vers l'achat d'armes pour répondre à la montée des tensions régionales ?
- neutralité ou intervention : le gouvernement devra arbitrer entre un soutien à un des belligérants ou la mise en place d'une force d'interposition.
- gestion de crise sociétale : les mouvements sociaux et les perturbations logistiques complexifieront les stratégies à déployer.

Pour réussir à gérer les crises, les participants de cet exercice cyber ont dû :

- Appréhender les mécanismes de sécurité pour protéger des équipements informatiques, réseaux et physiques ;
- Déjouer des attaques cyber par la pratique ;
- Mettre en œuvre des activités d'hacking dans un cadre éthique ;
- Manager des équipes et gérer une crise cyber.

Une mobilisation exceptionnelle pour sensibiliser les talents de demain

Plus de 200 participants (dont 113 étudiants de bac+3 à bac+6) issus de divers établissements et pays se sont affrontés dans un environnement hyperréaliste, simulé par des plateformes avancées comme le Cyber-Range. Les scénarios combinent menaces cyber, économiques et physiques, offrant un cadre complet pour évaluer et développer des compétences essentielles telles que la cybersécurité, l'intelligence artificielle, l'électronique, etc. tout en se confrontant à des défis concrets inspirés du monde réel. L'exercice a débuté le 27 janvier et a inclus une journée continue exceptionnelle intégrant la nuit du mardi 28 matin au mercredi 29 soir sans interruption, offrant une immersion totale dans la gestion de crise cyber.

Près de 110 étudiants issus de 7 composantes de l'Université de Lorraine (Polytech Nancy, Mines Nancy, TELECOM Nancy, de la FST avec son Master SIRAV, de l'UFR SHS avec le Master VSOC, de l'UFR MIM avec le Master SIS, de l'IUT Nancy-Brabois avec le parcours Cybersécurité du BUT Réseaux et Télécoms) rejoints cette année par l'ENSISA - École Nationale Supérieure d'Ingénieurs Sud Alsace se sont challengés pendant 3 jours d'exercice. Une diversité et complémentarité de profils d'étudiants qui montre que la cyber concerne tout le monde.

En complément, près de 90 contributeurs venus du ministère des Armées, de pôles scientifiques et de grands groupes industriels (Siemens, Orange, Soteria Lab, Geoide, idverde, Pam Saint-Gobin, D.N.C Agency, Cyber-detect, Niryo, RootMe Pro, 3D Advance…) sont impliqués dans l'organisation, la réalisation d'épreuves et l'encadrement. Avec la présence de nombreuses entreprises partenaires, le « Cyber Humanum Est » offre aux participants une approche unique du triptyque Armée-Formation-Industrie.

À l'issue de cet événement, plusieurs distinctions ont été décernés aux équipes : prix de « la meilleure gestion de crise », « la meilleure défense », « la meilleure attaque », « la meilleure lutte d'influence », ainsi que « le grand vainqueur de l'exercice ».

L'offre de formation en cybersécurité de l'Université de Lorraine | Découvrir

Site Web : fr.cyberhumanumest.com
LinkedIn : https://www.linkedin.com/company/cyber-humanum-est/

—

CONTACTS PRESSE

Clément Dufrenne
Consultant en relations presse
07 87 07 18 06
cdufrenne@madamemonsieur.agency

Christelle LE FORT
Chargée de communication COMCYBER
06 45 97 12 74
christelle.le-fort@intradef.gouv.fr