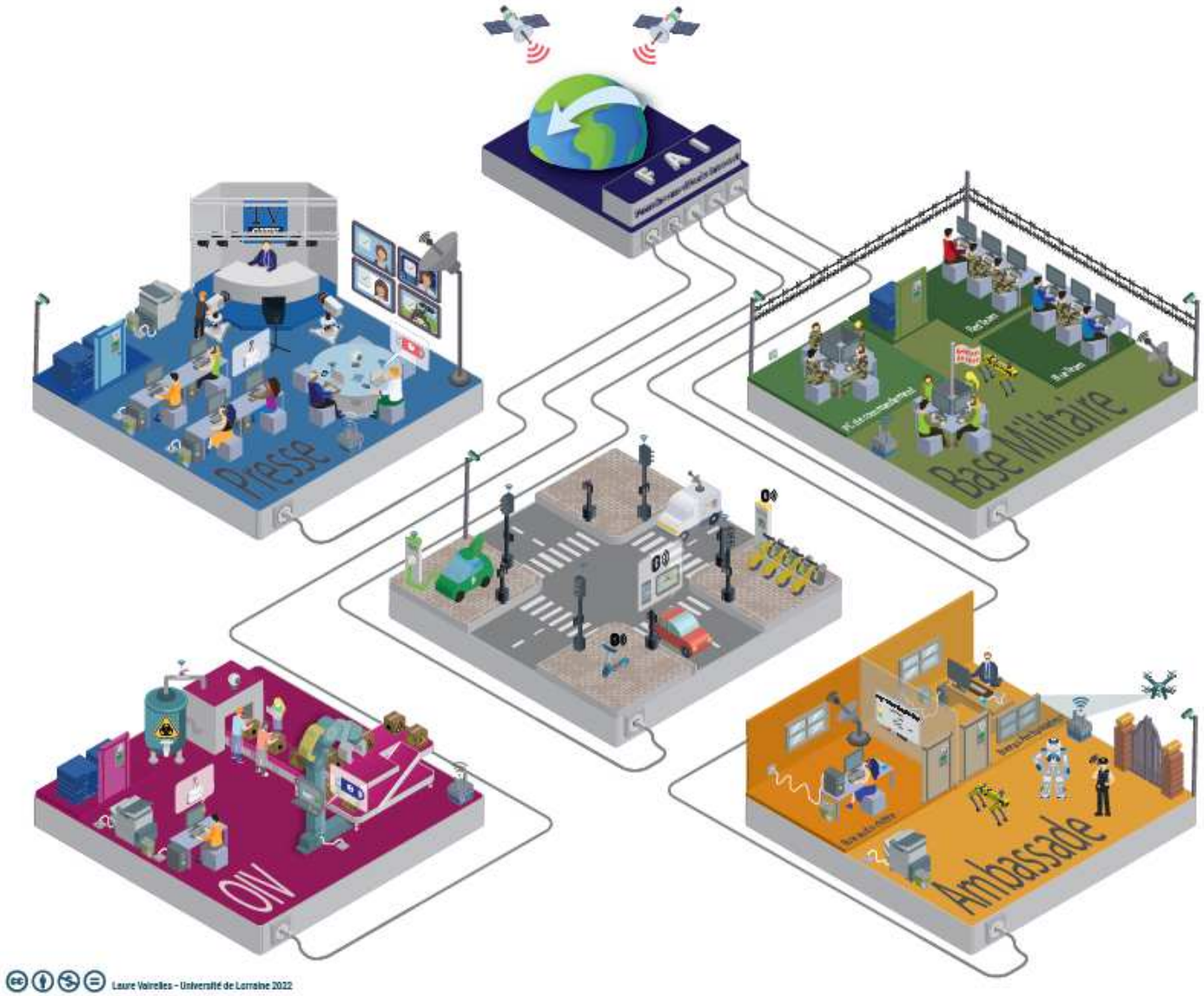
www.cyberumanumest.com

Du 6 au 10 février 2023



Contacts :

Stéphane Gégout
06 32 07 16 04
s.gegout@protonmail.com

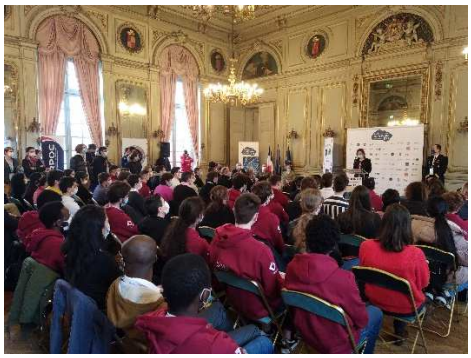
Jean-Philippe Auzelle
06 46 62 11 63
jean-philippe.auzelle@univ-lorraine.fr
www.cyberhumanumest.com

Marion Gilson
06 32 07 16 04
marion.gilson@univ-lorraine.fr

Sous l'égide du Commandement de la Cyberdéfense (COMCYBER) du ministère des Armées et de l'Université de Lorraine, la Base de Défense de Nancy et Lorraine INP organisent, pour la 3e année consécutive, un exercice de cyberdéfense « Capture The Flag/WarGame » mélangeant virtuel, réel et lutte d'influence informationnelle : le ***Cyber Humanum Est***. Il se déroula sur 3 jours du **6 au 10 Février 2023**. Avec une infrastructure étendue et un scénario plus ambitieux, cet exercice multisites se jouera également dans la nuit du 7 au 8 février. Il s'adressera à plus de 100 étudiant(e)s et se poursuivra le 10 février avec un forum métiers cyber et l'annonce des prix des gagnants.
Cet évènement cyber est soutenu par de nouveaux partenaires comme Siemens, Pont A Mousson/Saint Gobain, Orange, Geoide… et d'autres majeurs à venir.

Les objectifs de Cyber Humanum Est sont :

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

Forum des métiers cyber le 10 février 2023 dans le cadre prestigieux du palais du gouvernement

Par qui et pour qui ?

Par le Ministère des Armées (COMCYBER) avec la Base de Défense (BDD) Nancy et L'Université de Lorraine avec le collégium Lorraine-INP .
Au profit de l'Ecole des Mines de Nancy, de Télécom Nancy, de Polytech Nancy, de l'Ecole Nationale Supérieure d'Electricité et de Mécanique) et d'autres composantes de l'Université de Lorraine comme l'IUT Nancy - Brabois - Licence pro Cyber, l'UFR MIM - Mathématiques Informatique et Mécanique avec le Master SIRAV et l'UFR SHS avec son Master VSOC de l'UFR Sciences Humaines et Sociales.

Contacts :

Stéphane Gégout
06 32 07 16 04
s.gegout@protonmail.com

Jean-Philippe Auzelle
06 46 62 11 63
jean-philippe.auzelle@univ-lorraine.fr
www.cyberhumanumest.com

Marion Gilson
06 32 07 16 04
marion.gilson@univ-lorraine.fr

Ça se passe où ?

A la caserne Blandan pour la Base de Défense (BDD) de Nancy, à Polytech Nancy, à Télécom Nancy, à l'Ecole des Mines de Nancy et au Palais du Gouvernement (Place de la Carrière dans le prolongement de la place Stanislas).

Composition des équipes :

Composition aléatoire avec mélange des étudiants. Une fois affecté à un pays, un étudiant ne peut plus en changer. Il est possible de participer dans la blue team et dans la red team en même temps. Une équipe L2I et gestion de crise est dédiée à chaque pays avec des étudiants en master SHS.

Théâtre des opérations :

Réalisé avec le soutien de la réserve opérationnelle de cyberdéfense, de personnels de l'université et d'experts en cybersécurité locaux, ce CTF/WARGAME se jouera en simultané sur trois sites distincts : la caserne Verneau Blandan à Nancy, Polytech Nancy et Télécom Nancy. Il mettra en concurrence des étudiants de plusieurs composantes d'enseignement (Mines Nancy, Polytech Nancy, Télécom Nancy, IUT de Brabois, UFR SHS et UFR MIM).

Avec plus de 500 jours hommes de préparation, la mobilisation de plus de 130 personnes (organisateurs et participants), l'exercice met en scène trois pays fictifs avec des ambassades, des PC tactiques, des OIV (Organismes d'Importance Vitale), des journaux, le groupe d'attaquants APT54, plus de 200 équipements virtuels, 1 drone militaire avec son pilote, 3 systèmes mécatroniques (scada), des robots, des attaques par les ondes radio, des malwares dédiés…

Contacts :

Stéphane Gégout
06 32 07 16 04
s.gegout@protonmail.com

Jean-Philippe Auzelle
06 46 62 11 63
jean-philippe.auzelle@univ-lorraine.fr
www.cyberhumanumest.com

Marion Gilson
06 32 07 16 04
marion.gilson@univ-lorraine.fr

Scénario de l'exercice 2023 :

- Suite au réchauffement climatique, dans l'archipel des Maladives, l'île **Les Riverchelles** a vu l'effondrement complet de son économie basée sur le tourisme.
- La découverte récente de ressources minières pourrait sauver l'île de la banqueroute.
- Deux pays voisins, le Cryptanga et l'Anumeric sont en concurrence pour obtenir le précieux permis d'exploitation.

➔ Pour être l'heureux acquéreur de l'île, les deux États en concurrence usent de tous les moyens à leur disposition pour discréditer leur adversaire afin de remporter la mise avec des attaques informatiques. Ils utilisent attaques et luttes d'influence afin de nuire à l'image ou de collecter des renseignements permettant de discréditer l'État adverse. Ainsi la LID (Lutte Informatique Défensive), la LIO (Lutte Informatique Offensive) et la LII (Lutte d'Influence Informationnelle) sont mis en œuvre par chacun des pays voisins, sans compter sur un groupe APT qui n'aura de cesse d'attaquer sans distinction les deux pays simultanément.

Programme de la semaine de l'exercice 2023 :

- **Lundi 6 février** : préparation des étudiants à l'exercice (mise en situation, scénario…)
- **Mardi 7 et mercredi 8 février** : CTF/WARGAME avec H24 la nuit
- **Jeudi 9 février fin d'après-midi** : débriefing de l'exercice et repas VIP en soirée
- **Vendredi 10 février matin** : une journée job dating *« et si la cybersécurité était votre avenir »* est organisée au palais du gouvernement avec une vingtaine de partenaires, annonce des prix et remise des attestations de participation sous le haut patronage du COMCYBER, le maire de Nancy et président de la métropole du Grand Nancy, le président de l'Université de Lorraine et le commandant de la Base de Défense de Nancy.

Rappel du contexte nancéien :

La **Base de Défense de Nancy** a signé le **3 juillet 2018** avec la **Métropole du Grand Nancy** une convention dans le cadre de la politique publique « compétitivité et rayonnement, atouts du Grand Nancy » autour des problématiques de cybersécurité.

La Base de Défense de Nancy a mené le projet qui a permis :

- La mise en place d'un laboratoire cyber « cyber range » au sein de la caserne Verneau, Base de Défense ;
- Le recrutement d'une quinzaine de réservistes opérationnels cyber de haut niveau, issus du tissu industriel et académique régional. Leur emploi est du ressort du COMCYBER qui valide tout engagement.
- L'interopérabilité des plateformes cyber de Nancy, à savoir le cyber range de Nancy Telecom, le cyber range mobile de Verneau et la salle de reverse engineering de l'École Nationale Supérieure des Mines de Nancy ;
- La mise en réseau des différents acteurs régionaux cyber dans le cadre du mandat de correspondant de la réserve cyber pour le Grand Est donné par le COMCYBER au commandant de la Base de Défense de Nancy.

Le **24 juin 2020,** une **convention de partenariat** a été signée entre la Base de Défense de Nancy et l'Université de Lorraine, représentée par les 11 écoles d'ingénieurs de Lorraine-INP.

Contacts :

Stéphane Gégout
06 32 07 16 04
s.gegout@protonmail.com

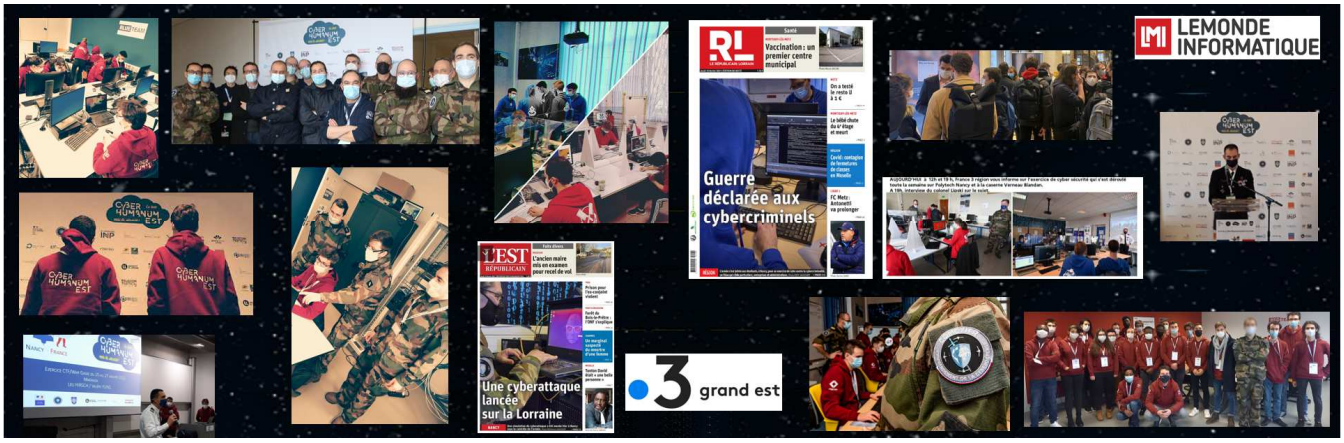
Jean-Philippe Auzelle
06 46 62 11 63
jean-philippe.auzelle@univ-lorraine.fr
www.cyberhumanumest.com

Marion Gilson
06 32 07 16 04
marion.gilson@univ-lorraine.fr

Cette convention a pour objet d'**améliorer la formation des étudiants des écoles d'ingénieurs de Lorraine INP, des personnels militaires ou civils en favorisant la meilleure utilisation collective des plateformes de Nancy, dont le laboratoire Cyber Range de Verneau**.

Partenaires 2022 :

Retours sur les exercices 2021, 2022 et préparation exercice 2023 :



Contacts :

Stéphane Gégout
06 32 07 16 04
s.gegout@protonmail.com

Jean-Philippe Auzelle
06 46 62 11 63
jean-philippe.auzelle@univ-lorraine.fr
www.cyberhumanumest.com

Marion Gilson
06 32 07 16 04
marion.gilson@univ-lorraine.fr