**Conseil d'administration**
**Séance du 27 mai 2025**
**Délibération n°2025-057**

SERVICE DES AFFAIRES STATUTAIRES ET JURIDIQUES

# IAE – Ouverture d'un diplôme d'université Influence et Contre Influence dans le cyber espace, en partenariat avec le ministère des armées à la rentrée universitaire 2025-2026

## Le conseil d'administration

*Vu le Code de l'éducation, notamment l'article L613-2 ;*
*Vu les statuts de l'Université Bretagne Sud ;*
*Vu les statuts de l'IAE ;*
*Vu l'avis de la CFVU du 3 avril 2025 ;*

Cette formation en 1 an s'adresse aux personnels opérationnels de la lutte d'influence informatique (L2I) du Ministère des Armées afin d'acquérir les concepts indispensables à leurs missions.

Ce DU a pour objectif de former à la détection et à la protection contre les stratégies d'influence et les techniques de captation de l'attention sur les espaces du web et via des objets informatiques. Chaque personne formée doit pouvoir participer à la prévention des démarches d'influence délétères pour son organisation. Ce DU a également pour objectif fournir les outils pour devenir experts en gestion de la cyber influence.

Ce DU a pour objectif de former à la détection et à la protection contre les stratégies d'influence et les techniques de captation de l'attention sur les espaces du web et via des objets informatiques. Chaque personne formée doit pouvoir participer à la prévention des démarches d'influence délétères pour son organisation. Ce DU a également pour objectif fournir les outils pour devenir experts en gestion de la cyber influence.

**Les compétences qui sont acquises sont les suivantes** :

- comprendre et connaître les concepts de l'influence, en particulier sur la circulation de l'information et les différents facteurs d'influence ;
- analyser l'environnement entourant les informations et les influences inhérentes ;
- maîtriser les techniques de segmentation et de ciblage des individus et des groupes sociaux ;
- comprendre le fonctionnement des applications web et des IoT et savoir observer scientifiquement leurs usages et les pratiques de ces technologies par les individus et acteurs clefs (responsables, dirigeants, décideurs officiels et officieux) d'une organisation ;
- connaître les principes des normes et influence sociales ainsi que leur exploitation par les techniques d'ingénierie sociale ;
- connaître les techniques de captation de l'attention et d'enfermement dans les systèmes cybernétiques dont les réseaux sociaux numériques ;
- développer la résistance et la prise de conscience des stratégies d'influence cyber et d'altération de la prise de décision ;
- savoir repérer des protocoles de navigation web exploitants les heuristiques erronées de simplification, les biais cognitifs, affectifs et perceptuels, et les techniques persuasives ;
- identifier les sources de failles liées au fonctionnement opérationnel et informationnel d'une organisation et de ses individus clefs dans le cyberespace ;
- analyser le niveau de risque et les modalités d'attaque de réputation d'une organisation ou d'un de ses individus clefs dans le cyberespace ;
- être capable de suggérer et de réaliser des améliorations dans les modes de sensibilisation des personnels, des partenaires-clients entreprises et des fournisseurs ;

**Transmission à la Rectrice, Chancelière des universités et publication sur le site de l'UBS : 3 juin 2025**

**Service des Affaires Statutaires et Juridiques**
Campus de Tohannic – rue André Lwoff – CS60573
56017 VANNES CEDEX
sasj@listes.univ-ubs.fr
**www.univ-ubs.fr**

- savoir proposer un programme de veille et de prévention autour de la vulnérabilité d'une organisation et de ses individus clefs ;
- connaitre les normes juridiques et règlementaires en vigueur concernant la matière de l'influence dans le cyber espace.

À l'issue de la formation, les étudiants auront la capacité de se positionner comme conseillers et opérateurs de la mise en œuvre d'actions de contre-influence dans le cyberspace.

Toutes les organisations sont aujourd'hui challengées par la numérisation des organisations et la systématisation de l'utilisation d'outils numériques individuels (Smartphones, IoT-Objets connectés) par les membres de ces organisations, employés et dirigeants. Ces évolutions en faveur de l'équipement et la connectivité individuelle conduisent à démultiplier les risques encourus par les organisations dans lesquelles évoluent les personnels, employés, cadres et dirigeants. En effet, la transposition des techniques de captation de l'attention ainsi que celles permettant d'influencer des individus et d'aller jusqu'à la manipulation des idées sont rendues beaucoup plus efficaces et faciles à mettre en œuvre dans le cyberespace.

Dès lors, la question n'est plus de savoir s'il y aura espionnage ou attaque réputationnelle, mais quand et avec quels effets. Il est donc essentiel de proposer des bases pour réduire en fréquence et en criticité les impacts de ces crises et attaques.

Face à ce phénomène, il n'y a pas encore à ce jour, à notre connaissance, de formation orientée sur la connaissance des stratégies d'influence afin de permettre leur prévention.

Selon les éléments publics de la doctrine militaire de lutte informatique d'influence (L2I), la lutte informatique d'influence correspond aux : « Opérations militaires conduites dans la couche informationnelle du cyberespace pour détecter, caractériser et contrer les attaques, appuyer la StratCom, renseigner ou faire de la déception, de façon autonome ou en combinaison avec d'autres opérations ».

La L2I est alors une réponse à la décentralisation des médias, et notamment à l'omniprésence et à l'influence grandissante des médias sociaux.

La L2I propose à la fois des capacités offensives et défensives.

Conscient des besoins de compétences et de formation à la L2I, la réponse proposée ici en termes de dispositif pédagogique ( DU ICI) ont été définis conjointement entre le Centre Cyber de Préparation Opérationnelle (COMCYBER/GCA/C2PO) du Ministère de Armées et l'Université Bretagne Sud. Plus précisément, la section Formation du C2PO (Centre Cyber de Préparation Opérationnelle, qui devient en 2025 l'Académie de Cyberdéfense) qui a la charge de proposer aux forces les formations cyber dont elles ont besoin, a confirmé le besoin de compétences et de formation.

Dans le contexte de la Lutte Informatique d'Influence (L2I), le C2PO a identifié qu'il manque une formation intégrée permettant aux opérationnels d'acquérir les concepts indispensables.

Le DU Prévention des Vulnérabilités Numériques Humaines, qui s'est déroulé en 2022, répondait très largement à ce besoin. Dans cette continuité, sa nouvelle version (DU ICI) sera proposée en 2025.

**Caractéristiques de la formation :** Formation continue au profit des personnels du ministère des armées.

**120 heures en face à face étudiant** réparties en sessions (de 3 jours, soit 6 sessions, ou de 5 jours, soit 4 sessions, étalées sur chaque année universitaire. Cette modalité d'organisation sera établie après dialogue avec les unités et les participants.

Lieu :

Le C2PO déménage en juillet 2025 dans son nouveau bâtiment en périphérie de Rennes, et les enseignements seront dispensés dans son amphithéâtre.

Le ministère des Armées entend ainsi assurer une montée en compétences à ses personnels et en priorité les personnels issus de la section Formation du C2PO (Centre Cyber de Préparation Opérationnelle, qui deviendra en 2025 l'Académie de Cyberdéfense.

**Capacité d'accueil** : 12 étudiants minimum – 32 maximum

**Ouverture** : rentrée en novembre 2025

**La maquette est jointe en PJ.**

**Analyse financière selon étude du service contrôle de gestion jointe :** Le Ministère des Armées versera annuellement à l'UBS les droits d'inscription de niveau master fixés par arrêté ministériel (250€ pour 2024/25) et une contribution forfaitaire de 500€ pour les 12 premiers étudiants inscrits puis 250 € pour les suivants.

Un avenant financier sera signé annuellement par les deux parties.

Le projet de convention est joint en annexe.

## Après en avoir délibéré,

Approuve à l'unanimité des suffrages exprimés l'ouverture d'un diplôme d'université Influence et Contre Influence dans le cyber espace, en partenariat avec le ministère des armées à la rentrée universitaire 2025-2026.

## Documents en annexe :

- Dossier DU influence
- Maquette DU ICI
- Modèle économique - DU Influence
- Projet convention DU influence

| | | | |
|---|---|---|---|
| ***Décompte des votes :*** | | *Suffrages exprimés :* | *22* |
| *Membres en exercice :* | *31* | *Pour :* | *22* |
| *Membres présents :* | *14* | *Contre :* | *0* |
| *Membres représentés :* | *9* | *Abstentions :* | *1* |

Visa du président, David MENIER
Par délégation, Michel GENTRIC

Signé électroniquement par : Michel GENTRIC
Date de signature : 02/06/2025
Qualité : VP CA, RSE et RH

UNIVERSITÉ BRETAGNE SUD
Par délégation
Le Vice-Président du
Conseil d'administration
M. GENTRIC

**Service des Affaires Statutaires et Juridiques**
Campus de Tohannic – rue André Lwoff – CS60573
56017 VANNES CEDEX
sasj@listes.univ-ubs.fr
**www.univ-ubs.fr**