Université de Bretagne-Sud

N° ……..

DIPLÔME D'UNIVERSITÉ
DU ☒ DIU ❑

Création	☒
Modification	❑
Renouvellement	❑
Suppression	❑

Intitulé :

Diplôme d'Université :

« Prévention des vulnérabilités Numériques Humaines »

- **Composante responsable de la formation : DSEG**

- **Lieux de la formation** :

Campus de Tohannic

- **Composante(s) associée(s) :**
  A l'avenir, possible mutualisation de l'exercice de mise en situation mis en place pour le DU Gendarmerie par l'ENSIBS Vannes et le Pôle Cyber

- **Autre(s) établissement(s) concerné(s) :**
  - Sans objet

- **Enseignants responsables :**
  - Christine Petr

Avis du Conseil de composante		Prévu autour du 11/03/2021
Avis du CFVU		En date du 01/04/2021
Avis du CA		En date du 28/04/2021

Enseignant(s) responsable(s) *(maximum deux)* Responsable de la L3 Marketing Vente	**Nom : Christine PETR** **Composante de rattachement : DSEG**	**Statut : Enseignant Chercheur titulaire (PU 6ième section)** **Téléphone : 06 41 97 09 59** **E-mail : christine.petr@univ-ubs.fr**
Responsable opérationnel de la formation	**Nom : Christine PETR** **Composante de rattachement : ENSIBS (pour la formation)**	**Statut : Enseignant Chercheur titulaire (PU 6ième section)** **Téléphone : 06 41 97 09 59** **E-mail : christine.petr@univ-ubs.fr**
Type de formation et de diplôme	Perfectionnement ❑ Acquisition de nouvelles compétences ☒ Réorientation ☒ Préparation à un concours ❑ DU ☒ DIU ❑ DIU int[1] ❑	
Code NAF	XXXX	
Niveau de sortie	**Cycle universitaire** 1er cycle ❑ 2ème cycle☒ 3ème cycle ❑ **Niveau selon la nomenclature du Ministère du travail** 3 ❑ 4 ❑ 5 ☒ (niveau M1) 6 ❑	
Objectif(s)	**Compétences recherchées :** Ce DU a pour objectif de former à l'identification et à la prévention des failles numériques liées à l'utilisation humaine (consommateurs, clients, employés, partenaires, dirigeants) des outils numériques. Cette formation permet d'acquérir les compétences nécessaires pour hiérarchiser et réduire les vulnérabilités numériques humaines en proposant des stratégies de protection et des actions correctives de type communication, sensibilisation, structuration des procédures internes, réglementation. À l'issue de la formation, les stagiaires professionnels et étudiants sont capables de réaliser un bilan de l'état de vulnérabilité numérique de leur organisation (entreprise privée, association, collectivité territoriale, structure publique ou étatique) au vu des pratiques informationnelles et fonctionnelles de ses membres. Les personnes formées peuvent alors identifier les priorités en termes d'actions correctives et préventives pour augmenter le degré de protection numérique de l'organisation et pour développer la prise de conscience des enjeux d'une bonne hygiène numérique auprès de ses partenaires et collaborateurs.	

[1] DIU international : en convention avec une université étrangère.

Métiers visés :
Les métiers en lien avec ces différentes compétences sont en construction. Il n'existe pas à ce jour d'intitulés spécifiques dédiés.
Ce sont en revanche de nouvelles compétences qui sont demandées et qui deviennent de plus en plus essentielles, avec l'accroissement généralisé de la transformation numérique et son accélération induit par la crise sanitaire de 2020.
Elles concernent en priorité :

- Les anciens CIL (correspondant Informatique et Liberté) et les nouveaux DPO (data privacy officer) sur le volet analyse des risques,
- Les informaticiens et développeurs sur le volet dérive et erreurs de manipulations des outils numériques par les usagers,
- Les responsables de marque et les chargés d'affaires et responsables de marché sur le volet risques d'attaques réputationnelles et prévention contre la surveillance concurrentielle,
- Les acteurs de la communication digitale et les community managers sur le volet maîtrise des contenus diffusés par les employés et personnels et développement de règles de « bonnes pratiques » communicationnelle sur les RSN,
- Les acteurs de l'organisation qui se positionnent à l'interface entre les services de la communication interne, des services de gestion des RH et les DSI.

UE et découpages par blocs de compétences :
Les blocs de compétences qui sont acquis sont structurés autour de 5 unités d'enseignement (UE), représentant chacune 24h eq.TD.

UE1 : Théories des comportements individuels, sociaux et organisationnels
Cette UE 1 est construite autour de 3 modules :
Module 1 - Comportements individuels
Module 2 - Comportements sociaux
Module 3 - Comportements organisationnels et incidences règlementaires

<u>Cette UE1 vise à acquérir les compétences suivantes :</u>

- Connaître les théories du comportement individuel et de la prise de décision et comprendre le pouvoir de l'information et des corrélations illusoires sur les croyances et représentations des entités individuelles
- Connaître les principales théories des relations sociales et les principes des normes et influences sociales pour comprendre les phénomènes et les mouvements sociaux
- Connaître les modes de prise de décision dans les organisations
- Prendre la mesure des incidences de la loi et de la réglementation (Droits fondamentaux, Données personnelles, RDPD ...) sur ces comportements organisationnels

UE2 : Méthodologies de segmentation et de ciblage des groupes, auditoires et individus

Cette UE 2 est construite autour de 3 modules :

Module 1- Segmentation et ciblage
Module 2- Géolocalisation et traçage
Module 3- Méthodes statistiques

Cette UE2 vise à acquérir les compétences suivantes :

- Maîtriser les techniques de segmentation, de caractérisation et de ciblage des groupes (collectifs d'intérêt, groupes sociaux, …) et des individus (micro ciblage et one-to-one)
- Envisager les possibilités de ciblage par l'exploitation de la géolocalisation et des outils et solutions permettant le traçage individuel en temps réel et différé
- Pouvoir effectuer des requêtes pour utiliser de manière combinée et cumulative les informations disponibles dans l'environnement réel et les traces numériques laissées par les utilisateurs d'outils connectés (historiques de navigation, contribution aux web 2.0, utilisation de services, d'applications mobiles ou de wearables, …)
- Pourvoir appréhender les techniques de micro-profilage sur des acteurs individuels clefs d'une organisation (responsables, dirigeants, décideurs officiels et officieux)
- Maitriser les fondamentaux des principales méthodes statistiques permettant des analyses explicatives et prédictives des typicités et profilage réalisés

UE3 : Stratégies d'influence, techniques de captation de l'attention, verrouillage fonctionnel et émotionnel

Cette UE 3 est construite autour de 3 modules :

Module 1- L'influence
Module 2- La captologie
Module 3- Le verrouillage

Cette UE3 vise à acquérir les compétences suivantes :

- Connaître les fondamentaux de la manipulation mentale et de l'influence
- Pouvoir typer et distinguer les principales stratégies d'influence qui sont régulièrement utilisées dans le monde économique et militaire
- Avoir un panorama sur les biais cognitifs individuels qui sont sous-jacents à la mise en place réussie de techniques d'altération de la prise de décision (nudge, ingénierie sociale) et aux processus cognitifs de tromperie
- Savoir dans quelles situations et comment sont mises en place des techniques de manipulation et de contre-déception d'acteurs stratégiques dans le monde militaire et civil
- Connaître les principaux leviers de la captation de l'attention
- Avoir des bases sur les techniques de rhétorique et la PNL et comprendre pourquoi et comment ils sont rendus plus efficace dans le contexte numérique
- Savoir comment les logiques de captologie permettent d'amener et d'enfermer un individu dans une bulle informationnelle qui entretiennent et le réconforte dans ses croyances

- Connaître les principales techniques de verrouillage fonctionnels, comportementaux et émotionnels et savoir comment il est possible de mesurer leur efficacité
- Être conscient du poids de la dépendance fonctionnelle et de l'addiction comportementale aux outils et du potentiel de la dépendance affective par l'attachement et la création du sentiment de familiarité envers l'environnement et l'outil numériques

UE4 : Analyser les failles et vulnérabilités des utilisateurs d'outils et solutions numériques

Cette UE 4 est construite autour de 2 modules :

Module 1- Identifier et catégoriser des vulnérabilités numériques humaines

Module 2- Analyser les vulnérabilités numériques d'usage et d'appropriation

Cette UE4 vise à acquérir les compétences suivantes :

- Connaître et pouvoir identifier les principales sources de vulnérabilités humaines et techniques
- Identifier les sources de failles liées au fonctionnement opérationnel et informationnel d'une organisation et de ses individus clefs dans le cyberespace
- Identifier les vulnérabilités au renseignement obtenu par manipulation humaine (sources humaines, ingénierie sociale, élicitation), celles liées aux sources techniques et opérationnelles (Interception et intrusion, piégeages, risques IoT), celles favorisées par les sources ouvertes et le déficit de contrôle de son exposition médiatique et numérique
- Être conscient des effets variables de la sensibilité individuelle et culturelle aux groupes d'influence politiques et idéologiques ainsi que de l'influence de la pression temporelle et des conditions de stress sur les déterminants de l'acceptation d'une requête
- Pouvoir relever les spécificités des vulnérabilités numériques induites par les effets d'usage et d'appropriation des utilisateurs d'outils et solutions numériques (usage quotidien, détourné et simplifié des outils numériques de travail côté employés, utilisation de portion de codes ne suivant les principes de la privacy-by-design côté développeurs, usages usuels d'exposition de soi sur les réseaux sociaux numériques, utilisation des historiques de navigation internet, …)

UE5 : Anticipation, prévention et résilience face aux menaces économiques et réputationnelles

Cette UE 5 est construite autour de 3 modules :

Module 1- Anticiper les menaces d'origine humaine sur les intérêts de l'organisation

Module 2- Réagir et se préparer aux attaques économiques et réputationnelles

Module 3- Réduire le risque en animant la politique de prévention et en augmentant la résistance des personnels

	Cette UE5 vise à acquérir les compétences suivantes : • 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 • Savoir effectuer un audit de l'état de vulnérabilité d'une organisation formelle ou d'un collectif informel au vu des pratiques numérisées de la structure et des pratiques individuelles de ses membres • Classifier les faiblesses de protection d'une organisation selon l'objet des menaces (attaques réputationnelles vs économiques) • Mesurer la criticité et la probabilité d'occurrence des différentes menaces pour l'organisation • Etablir une priorisation des intérêts à protéger compte tenu de la stratégie et de la mission de l'organisation • Formaliser la participation du facteur humain en situation de gestion de la crise • Savoir reconnaitre une attaque d'influence • Lancer et organiser les procédures de gestion des crises économiques et réputationnelles • Proposer un plan de prévention des failles humaines dans une organisation privée, une structure étatique, une collectivité territoriale ou une association • Être capable de concevoir un programme de veille et de prévention autour de la vulnérabilité d'une organisation et de ses individus clefs • Concevoir des documents informationnels encadrant les usages numériques dans l'organisation (codes de bonnes pratiques, charte éditoriale des réseaux sociaux numériques) • Développer la résistance et la prise de conscience des stratégies d'altération de la prise de décision auprès des personnels, fournisseurs et acteurs clefs d'une organisation • Animer la politique et la communauté des acteurs impliqués dans la gestion de l'hygiène numérique au sein de l'organisation • Pouvoir proposer des améliorations dans les modes de sensibilisation des personnels, des partenaires-clients entreprises et des fournisseurs impliquant un processus constant de test-re tests de techniques permettant d'accroitre le niveau d'adhésion des personnels, fournisseurs et acteurs clefs d'une organisation à l'hygiène numérique **Niveau visé :** À l'issue de la formation, les professionnels formés seront en capacité de se positionner comme des conseillers extérieurs ou des managers internes qui pourront **organiser, exécuter et superviser** la réalisation des bilans de la vulnérabilité numérique humaine des organisations qui les solliciteront. Sur la base des analyses et bilans ainsi effectués, ils pourront proposer des plans de mesures correctives à court terme et des programmes de prévention à long terme pour réduire les vulnérabilités identifiées dans ces organisations.
Opportunités et originalités	Précisez comment se situe la formation par rapport à l'offre de la composante, de l'université et extérieure à l'université. Précisez les besoins des milieux professionnels.

	• Cette formation répond initialement à un besoin exprimé par le Ministère des Armées. Si le DU répond prioritairement aux besoins de ce partenaire, il est probable qu'il puisse être par la suite proposé aux corps militaires à l'échelle nationale et via le centre des armées. • Cependant, le contenu pédagogique proposé répond de manière étendue et systématique aux besoins de toutes les organisations du monde civil qui se trouvent engagées dans le phénomène généralisé, et accéléré par la crise sanitaire, de la transformation numérique de la société. • La formation s'adresse ainsi à tous les professionnels en activité et étudiants qui visent l'acquisition d'un socle de connaissances et d'automatismes comportementaux en termes d'hygiène numérique et qui doivent acquérir des savoirs et savoir-faire pour analyser et agir en faveur de la prévention des failles humaines dans l'utilisation des outils numériques. • Dans le cadre récent du RGPD, un public prioritaire à considérer et cibler est celui des DPO (les délégués à la protection des données) dont le nombre désigné officiellement auprès de la CNIL est en explosion depuis l'application de la règlementation européenne en mai 2018. Ils ne sont pas, à ce jour, formés en analyse des risques liés à l'usage humain des outils et solutions numériques. • Toutes les organisations sont aujourd'hui potentiellement en danger face à l'accroissement du phénomène de transformation numérique et à la systématisation de l'utilisation d'outils individuels (Smartphones, IoT-Objets connectés) par les membres de ces organisations (employés et dirigeants). La question n'est plus s'il y aura espionnage ou attaque réputationnelle, mais quand et avec quels effets ? Dès lors, il est essentiel de proposer des bases permettant aux employés et décideurs des organisations de réduire au plus bas (en fréquence et en criticité) les impacts de ces crises et attaques en favorisant la mise en place d'une bonne hygiène numérique individuelle parmi tous les acteurs et partenaires des organisations. • 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. Or, face à ce phénomène, il n'y a pas encore à ce jour, à notre connaissance, de formation orientée sur la connaissance de ces nouvelles modalités numérisées afin de permettre leur prévention. Cette formation remplit donc un vide actuel. • Enfin, d'un point de vue sociétal, il est crucial pour l'ensemble des individus et citoyens d'être formé a minima afin de pouvoir se prémunir personnellement (respect de ses libertés fondamentales individuelles) mais aussi collectivement (protection de la société civile, des principes démocratiques) et professionnellement (protection des entreprises privées et publiques) des risques inhérents aux usages d'objets, d'outils et de services numériques.		
Capacité d'accueil	16	**Seuil d'ouverture**	12 minimum (12 financièrement)
Conditions d'inscription	Précisez les pré-requis, les conditions d'admission (diplôme, financement, entreprise pour un stage ou sujet de mémoire de recherche par exemple) ainsi que, le cas échéant, les modalités (dossier, entretien, test…)		

	Le stagiaire doit : • Bénéficier d'une expérience professionnelle dans une organisation où la transformation numérique a été mise en place et/ou est en cours de mise en place ou avoir le projet de travailler dans une organisation où la numérisation des outils, des pratiques et des supports est une contrainte d'adaptation aux besoins des clients et usagers visés. • Le candidat doit proposer une rédaction personnelle sur la présentation d'un cas organisationnel et/ou un épisode de l'histoire locale ou mondiale récente (attaque d'un pays, cas de manipulation de vote tel Cambridge Analytica, cyber attaque du Quotidien Ouest France, etc.). Dans sa rédaction (10 pages maximum, T12, interligne1,5), le candidat doit exposer sa perception argumentée de la place de la vulnérabilité humaine et proposer a posteriori des actions qui auraient pu remédier à certaines des vulnérabilités humaines qu'il a relevées et qu'il jugerait prioritaire de prévenir.
Durée totale de la formation	120 heures équivalent TD réparties sur 8 mois (octobre à mai) à raison d'un module de 2 jours ouvrés par mois (jeudi et vendredi).
Modalités de formation	Formation initiale ❑ Formation par apprentissage ❑ Formation continue ☒
Frais de formation *(hors apprentissage)*	Formation continue avec financement : 3330 euros par stagiaire Formation continue sans financement : Formation initiale :

Organisation détaillée des enseignements : Voir Annexe + détails dans le fichier Excell joint

Indiquez en annexe l'équipe pédagogique pressentie, programme, volume horaire, stages)

Moyens	Précisez les moyens disponibles, les équipements le cas échéant. • Salle de TD (DSEG) • Mise à disposition des logiciels de l'Institut de Management (Sphinx IQ, Sphinx Lexica) • Mise à disposition des salles d'informatique pour l'UE

Modalités de contrôle des connaissances :

Matières, nature et durée de l'épreuve, coefficients

Le contrôle continu est privilégié via un suivi individuel de l'implication des stagiaires dans l'apport d'illustrations et de fiches de synthèses et mini-rapports (CC).
Ce contrôle continu par enseignement pourra se terminer par un test de connaissance et de compréhension qui est réalisé à l'issu de chaque enseignement (via un QCM sur Moodle ou un écrit ou oral selon la nature de l'épreuve).
Selon la pertinence pédagogique, l'enseignant d'une matière peut proposer en complément un travail analytique ou applicatif (en équipe ou individuel) qui est à rendre dans les 15 jours qui suivent la session d'enseignement concernée par sa matière.

Règlement d'obtention des UE et du diplôme de DU :
Les différents enseignements se compensent pour l'obtention du module à laquelle ils se rattachent.
Les différents modules se compensent pour l'obtention d'une UE (note de 10/20).

Les différentes UE se compensent pour l'obtention du DU.
Pour plus de détails, voir Annexe 1 et la feuille correspondante du fichier Excel

Organisation de l'année
Pour plus de détails, voir Annexe 2 et la feuille correspondante du fichier Excel

Jury du DU:
Le jury de fin d'année peut se tenir à la mi-juin et les examens de rattrapage du S2 ont lieu en juillet.
Le jury de seconde session du S2 est en fin aout.
Pour plus de détails, voir Annexe 3 et la feuille correspondante du fichier Excel

Évaluation financière	• Frais de formation : 35'000€ (3'257€/stagiaire) 3'257€ +243€ de frais d'inscription • Coûts : 22'3534€ ○ Enseignements : 17'520€ (120 heures eq TD au taux horaire moyen chargé de 146€) ○ Responsabilité pédagogique de formation : 1'460€ (10 heures au taux horaire de 146€ de taux horaire moyen) ○ Tutorat : 3'504€ (2h par stagiaire soit 24h à 146€ de taux horaire moyen) ○ Frais (de déplacement des intervenants extérieurs et pauses café): 2'400€ ○ Prélèvement 23% pour frais administratifs : 8'989,32€ • Voir fichier budgétaire pour les détails
Procédure d'évaluation de la formation	Précisez les différentes formes d'évaluation (par exemple : indicateurs, évaluation par les étudiants, par les enseignants, par les professionnels…) ainsi que leur périodicité. Il est possible de renvoyer à une annexe. • Fiche d'évaluation standardisée à l'issue de chaque cours remplie par les étudiants via Moodle. • Conseil de perfectionnement avec les différents intervenants et organisations impliqués
Partenariats	Précisez les partenaires et leurs rôles respectifs • ~~CyberCom Rennes (sont à l'origine du besoin)~~ Ministère des armées
Observations particulières	**Possibles perspectives futures (à partir de la promotion 2022-2023) :** - **Possibilités de modularisation des blocs de compétences :** A l'éventuelle validation RNCP, le DU pourra être proposé en blocs de compétences. En effet, la formation du DU est conçue de manière à permettre à des professionnels en activité et/ou à des personnes en recherche d'emploi de

	pouvoir suivre l'un ou l'autre des 5 UE afin de valider l'acquisition de la compétence visée, indépendamment de la poursuite de l'ensemble du DU. - **Possibles évolutions après le suivi de la formation du DU :** Après avoir suivi le DU, les étudiants et professionnels formés peuvent envisager la poursuite de l'acquisition de blocs de compétences complémentaires de niveau M2 (à l'UBS ou dans d'autres universités et organismes de formation). Il est aussi envisageable que cette formation DU de niveau M1 soit l'objet d'un complément de montée en compétences vers un niveau de formation M2. Dès lors, deux spécialités seraient envisageables : l'une autour de la prévention (communication, sensibilisation et adhésion des employés et acteurs en interne) qui pourrait intéresser des publics de formations en sciences humaines et sociales, et l'autre autour du diagnostic de la vulnérabilité qui pourrait intéresser et offrir une double-compétence à des étudiants et professionnels issus des formations classiques en sciences de l'ingénieur et en informatique.
Date d'ouverture *(ou de modification)*	Lundi 11 octobre 2021
Ouverture demandée pour	1 an renouvelable

Le 08/03/2021,

Annexe 1 : UE et détails des enseignements

	Matières	Coef	CM	TD	h face à face étudiant	*nb gr*	h ETD
UE obligatoire 5 crédits ECTS	**UE1: Théories des comportements individuels, sociaux et organisationnels**	**1**	***8***	***12***	***20***	***1***	***24***
	Module 1 - Comportements individuels	**1**	***2,5***	***4***	***6,5***	***1***	***7,75***
	Théories du Comportement individuel	1	2	2	4	*1*	5
	Théories du Comportement du consommateur	1	2,5	4	6,5	*1*	7,75
	Module 2 - Comportements sociaux	**1**	1,5	3	4,5	2	5,25
	Théories des relations sociales	1	1,5	0	1,5	*1*	2,25
	Théories des mouvements sociaux	1	0	3	3	*1*	3
	Module 3 - Comportements organisationnels et incidences règlementaires	**1**	4	5	9	1	11
	Théories de la décision dans les organisations	1	2	0	2	*1*	3
	L'incidence de la loi et de la réglementation sur les comportements (Droits fondamentaux, Données personnelles, RDPD,...)	1	2	5	7	*1*	8

		Coef	CM	TD	h face à face étudiant	*nb gr*	h ETD
UE obligatoire 5 crédits ECTS	**UE2: Méthodologies de segmentation et de ciblage des groupes, auditoires et individus**	**1**	**6**	**15**	**21**	*1*	***24***
	Module 1- Segmentation et ciblage	**1**	***4***	***6***	***10***	***1***	***12***
	Les principes de la segmentation et de la caractérisation des segments types (groupes sociaux, communautés, auditoires, audiences et publics)	1	2		2	*1*	3
	Les stratégies de ciblage des groupes sociaux (simulitudes socioculturelles, communautés d'intérêt, mimétismes comportementaux)	1	1	2,5	3,5	*1*	4
	Les principes du ciblage individuel (microciblage et one-to-one)	1	1	3,5	4,5	*1*	5
	Module 2- Géolocalisation et traçage	**1**	1	4	5	1	5,5
	L'exploitation des données de géolocalisation des outils de traçage individuel	1	1	2	3	*1*	3,5
	Le profilage par l'exploitation combinée d'informations off-line et de traces numériques	1		2	2	*1*	2
	Module 3- Méthodes statistiques	**1**	1	5	6	1	6,5
	Les techniques statistiques de typologie (Classification Ascendantes et Descendantes)	1	1	2,5	3,5	*1*	4
	Les techniques statistiques de segmentation et de scoring (analyse discriminante, analyse neuronale, modélisation linéaire et non linéaire)	1		2,5	2,5	*1*	2,5

		Coef	CM	TD	h face à face étudiant	*nb gr*	h ETD
UE obligatoire 5 crédits ECTS	**UE3: Stratégies d'influence, techniques de captation de l'attention, verrouillage fonctionnel et émotionnel**	**1**	**6**	**15**	**21**	*1*	***24***
	Module 1- L'influence	**1**	***4***	***7,5***	***11,5***	***1***	***13,5***
	Les fondamentaux de la manipulation mentale et de l'influence	1	2		2	*1*	3
	La typologie et les principes des stratégies d'influence	1	0	3	3	*1*	3
	Les biais cognitifs individuels	1	2	1,5	3,5	*1*	4,5
	Les techniques d'altération de la prise de décision (nudge, ingénierie sociale)	1		1,5	1,5	*1*	1,5
	Les processus cognitifs de tromperie et de contre-déception d'acteurs stratégiques	1		1,5	1,5	*1*	1,5
	Module 2- La captologie	**1**	**2**	**3**	**5**	**1**	**6**
	Les principaux leviers de la captation de l'attention	1	2		2	*1*	3
	Les techniques de rhétorique et la PNL	1		1,5	1,5	*1*	1,5
	L'enfermement et les bulles informationnelles	1		1,5	1,5	*1*	1,5
	Module 3- Le verrouillage	**1**	**0**	**4,5**	**4,5**	**1**	**4,5**
	Les techniques de verrouillage fonctionnels, comportementaux et émotionnels et leur mesure	1		1,5	1,5	*1*	1,5
	Développement de la dépendance fonctionnelle et de l'addiction comportementale	1		1,5	1,5	*1*	1,5
	Développement de l'attachement et de la familiarité envers l'environnement et l'outil	1		1,5	1,5	*1*	1,5

		Coef	CM	TD	h face à face étudiant	*nb gr*	h ETD
UE obligatoire 5 crédits ECTS	**UE4: Analyser les failles et vulnérabilités des utilisateurs d'outils et solutions numériques**	**1**	**6**	**19,5**	**23**	*1*	***24***
	Module 1- Identifier et catégoriser des vulnérabilités numériques humaines	**1**	***0***	***13,5***	***14***	***5***	***13,5***
	Connaître et identifier les principales sources de vulnérabilités humaines et techniques	1		3,5	4	*1*	3,5
	Les vulnérabilités au renseignement obtenu par manipulation humaine (sources humaines, ingénierie sociale, élicitation)	1		2	2	*1*	2
	Les vulnérabilités au renseignement de sources techniques et opérationnelles (Interception et intrusion, piégeages, risques IoT)	1		2	2	*1*	2
	Les vulnérabilités au renseignement de sources ouvertes et au contrôle de son exposition médiatique et numérique	1		2	2	*1*	2
	Les vulnérabilités induit par la sensibilité individuelle et culturelle aux groupes d'influence politiques et idéologiques	1		4	4	*1*	4
	Module 2- Analyser les vulnérabilités numériques d'usage et d'appropriation	**1**	***3***	***6***	***9***	***4***	***10,5***
	Etudier les risques induits par l'usage quotidien, détourné et simplifié, des outils et applications de l'organisation	1	0	3	3	*1*	3
	Etudier les risque induits par les pratiques des développeurs (absence de privacy by design, utilisation de codes libres, etc.)	1	2	0	2	*1*	3
	Relever les déterminants de l'acceptation à l'agir au sein d'une population cible et l'influence de la pression temporelle et des conditions de stress	1		3	3	*1*	3
	Repérer les pattern de facteurs à risque à partir des usages humains (cas des historiques de navigation Google et Facebook)	1	1	0	1	*1*	1,5

		Coef	CM	TD	h face à face étudiant	*nb gr*	h ETD
UE obligatoire 5 crédits ECTS	**UE5: Anticipation, prévention et résilience face aux menaces économiques et réputationnelles**	**1**	***4***	***18***	***22***	***1***	***24***
	Module 1- Anticiper les menaces d'origine humaine sur les intérêts de l'organisation	**1**	***2***	***6***	8	***1***	***9***
	Identifier les faiblesses de protection d'une organisation selon l'objet des menaces (attaques réputationnelles vs économiques)	1	2	1,5	3,5	*1*	4,5
	Mesurer la criticité et la probabilité d'occurrence des différentes menaces pour l'organisation	1		1,5	1,5	*1*	1,5
	Etablir une priorisation des intérêts à protéger compte tenu de la stratégie et de la mission de l'organisation	1		1,5	1,5	*1*	1,5
	Formaliser la participation du facteur humain en situation de gestion de la crise	1		1,5	1,5	*1*	1,5
	Module 2- Réagir et se préparer aux attaques économiques et réputationnelles	**1**	***0***	***9***	***9***	***3***	***9***
	Savoir reconnaitre une attaque d'influence	1		1,5	1,5	*1*	1,5
	Lancer et organiser les procédures de gestion des crises économiques et réputationnelles	1		1,5	1,5	*1*	1,5
	Sensibiliser et accroitre la résistance des personnels et partenaires aux attaques par l'entraînement et l'expérimentation fictionnelle	1		6	6	*1*	6
	Module 3- Réduire le risque en animant la politique de prévention et en augmentant la résistance des personnels	**1**	***2***	***3***	***5***	***3***	***6***
	Proposer un plan de prévention des failles humaines dans une organisation privée, une structure étatique, une collectivité territoriale ou une association	1	2	0	2	*1*	3
	Concevoir des documents informationnels encadrant les usages numériques dans l'organisation (codes de bonnes pratiques, charte éditoriale des réseaux sociaux numériques)	1		1,5	1,5	*1*	1,5
	Faire adhérer et animer à la gestion de l'hygiène numérique au sein de l'organisation	1		1,5	1,5	*1*	1,5

Annexe 2 : Organisation de l'année

Organisation logistique des enseignements

1 session mensuelle = 7h /jour *2jours
soit 14h de face à face étudiant
Jours privilégiés : Jeudi et Vendredi

2 UE en Semestre 1 =		Octobre - Novembre - Décembre
	6 jours de cours	
	sur 3 mois	
en face à face	41h pour UE1 et UE2	
pour 6 jours de cours		
sur le S1	**7 h de cours en face à face étudiant par jour**	

3 UE en Semestre 2 =		Janvier-Février-Mars-Avril-Mai
	10 jours de cours	
	sur 5 mois	
en face à face	66h pour UE3 et UE4 et UE5	
pour 10 jours de cours		
sur le S2	**7 h de cours en face à face étudiant par jour**	

Les périodes d'examens de rattrapage et Jury

Périodes des Jurys et de la session de rattrapage:

Jury de session 1 :	semaine 21
Session de rattrapage :	semaine 25
Jury de session 2 (rattrappage) :	semaine 27

Remise des diplômes :

Remise des diplômes : Lors de la European cyberweek pour l'année 2021 (Novembre)

PUIS / et- ou

A la fin de la première journée de la session d'octobre de la promotion de l'année suivante

Annexe 3 : Modalités de contrôles de connaissances

	Matières	Coef		
UE obligatoire 5 crédits ECTS	**UE1: Théories des comportements individuels, sociaux et organisationnels**	**1**	**MCC 1ière session**	**Modalités (MCC) Rattrapage**
	Module 1 - Comportements individuels	**1**		
	Théories du Comportement individuel	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Théories du Comportement du consommateur	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 2 - Comportements sociaux	**1**		
	Théories des relations sociales	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Théories des mouvements sociaux	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 3 - Comportements organisationnels et incidences règlementaires	**1**		
	Théories de la décision dans les organisations	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	L'incidence de la loi et de la réglementation sur les comportements (Droits fondamentaux, Données personnelles, RDPD,...)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve

		Coef		
UE obligatoire 5 crédits ECTS	**UE2: Méthodologies de segmentation et de ciblage des groupes, auditoires et individus**	**1**	**MCC 1ière session**	**Modalités (MCC) Rattrapage**
	Module 1- Segmentation et ciblage	**1**		
	Les principes de la segmentation et de la caractérisation des segments types (groupes sociaux, communautés, auditoires, audiences et publics)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les stratégies de ciblage des groupes sociaux (simulitudes socioculturelles, communautés d'intérêt, mimétismes comportementaux)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les principes du ciblage individuel (microciblage et one-to-one)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 2- Géolocalisation et tra9age	**1**		
	L'exploitation des données de géolocalisation des outils de traçage individuel	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Le profilage par l'exploitation combinée d'informations off-line et de traces numériques	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 3- Méthodes statistiques	**1**		
	Les techniques statistiques de typologie (Classification Ascendantes et Descendantes)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les techniques statistiques de segmentation et de scoring (analyse discriminante, analyse neuronale, modélisation linéaire et non linéaire)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve

		Coef		
UE obligatoire 5 crédits ECTS	**UE3: Stratégies d'influence, techniques de captation de l'attention, verrouillage fonctionnel et émotionnel**	**1**	**MCC 1ière session**	**Modalités Rattrapage (MCC 2ième session)**
	Module 1- L'influence	**1**		
	Les fondamentaux de la manipulation mentale et de l'influence	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	La typologie et les principes des stratégies d'influence	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les biais cognitifs individuels	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les techniques d'altération de la prise de décision (nudge, ingénierie sociale)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les processus cognitifs de tromperie et de contre-déception d'acteurs stratégiques	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 2- La captologie	**1**		
	Les principaux leviers de la captation de l'attention	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les techniques de rhétorique et la PNL	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	L'enfermement et les bulles informationnelles	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 3- Le verrouillage	**1**		
	Les techniques de verrouillage fonctionnels, comportementaux et émotionnels et leur mesure	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Développement de la dépendance fonctionnelle et de l'addiction comportementale	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Développement de l'attachement et de la familiarité envers l'environnement et l'outil	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve

		Coef		
UE obligatoire 5 crédits ECTS	**UE4: Analyser les failles et vulnérabilités des utilisateurs d'outils et solutions numériques**	**1**	**MCC 1ière session**	**Modalités (MCC) Rattrapage**
	Module 1- Identifier et catégoriser des vulnérabilités numériqueshumaines	**1**		
	Connaître et identifier les principales sources de vulnérabilités humaines et techniques	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les vulnérabilités au renseignement obtenu par manipulation humaine (sources humaines, ingénierie sociale, élicitation)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les vulnérabilités au renseignement de sources techniques et opérationnelles (Interception et intrusion, piégeages, risques IoT)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les vulnérabilités au renseignement de sources ouvertes et au contrôle de son exposition médiatique et numérique	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Les vulnérabilités induit par la sensibilité individuelle et culturelle aux groupes d'influence politiques et idéologiques	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 2- Analyser les vulnérabilités numériques d'usage et d'appropriation	**1**		
	Etudier les risques induits par l'usage quotidien, détourné et simplifié, des outils et applications de l'organisation	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Etudier les risque induits par les pratiques des développeurs (absence de privacy by design, utilisation de codes libres, etc.)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Relever les déterminants de l'acceptation à l'agir au sein d'une population cible et l'influence de la pression temporelle et des conditions de stress	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Repérer les pattern de facteurs à risque à partir des usages humains (cas des historiques de navigation Google et Facebook)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve

		Coef		
UE obligatoire 5 crédits ECTS	**UE5: Anticipation, prévention et résilience face aux menaces économiques et réputationnelles**	**1**	**MCC 1ière session**	**Modalités (MCC) Rattrapage**
	Module 1- Anticiper les risques humains de menaces sur les intérêts de l'organisation	**1**		
	Identifier les faiblesses de protection d'une organisation selon l'objet des menaces (attaques réputationnelles vs économiques)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Mesurer la criticité et la probabilité d'occurrence des différentes menaces pour l'organisation	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Etablir une priorisation des intérêts à protéger compte tenu de la stratégie et de la mission de l'organisation	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Formaliser la participation du facteur humain en situation de gestion de la crise	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 2- Réagir et se préparer aux attaques économiques et réputationnelles	**1**		
	Savoir reconnaitre une attaque d'influence pour lancer les process de protection	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Lancer les procédures de gestion des crises économiques et réputationnelles	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Sensibiliser et accroitre la résistance des personnels et partenaires aux attaques par l'entraînement et l'expérimentation fictionnelle	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Module 3- Réduire le risque en animant la politique de prévention et en augmentant la résistance des personnels	**1**		
	Proposer un plan de prévention des failles humaines dans une organisation privée, une structure étatique, une collectivité territoriale ou une association	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Concevoir des documents informationnels encadrant les usages numériques dans l'organisation (codes de bonnes pratiques, charte éditoriale des réseaux sociaux numériques)	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve
	Faire adhérer et animer à la gestion de l'hygiène numérique au sein de l'organisation	1	CC ou écrit ou oral selon la nature de l'épreuve	écrit ou oral selon la nature de l'épreuve