n°1

contre MESURES

MASTER 2 MS
INGENIERIE SURETE SECURITE DEFENSE

Un Master atypique
de l'Université Toulouse III Paul Sabatier

DECEMBRE 2016 - N°1

DOSSIER CYBERCRIMINALITÉ

NOUVEAU ! Le magazine du MASTER 2 ISSD - Ingénierie Sûreté Sécurité Défense

EN BREF

Vous parcourez le n°1 de la revue du Master 2 “Ingénierie Sûreté Sécurité Défense”. Nous avons voulu lui donner une identité forte en créant un logo qui lui soit propre.

Ce logo représente une chouette, stylisée pour lui apporter agressivité et modernité,

Une chouette couleur de l’or : valeur et pérénité, sur un fond sombre : la lumière triomphe de l’obscurité.

Une chouette qui symbolise :
- l’intuition et l’intelligence clairvoyante (regard perçant),
- le savoir et la sagesse (immobilité silencieuse)
- une énergie redoutable et imprévisible (chasse du rapace).

Une chouette, visible partiellement pour dire le mystère, la discrétion, la clandestinité.

Un œil scrutateur, froid et technologique.
- Scrutateur : la curiosité, la capacité d’évaluation sont des qualités que nous cultivons dans ce Master.
- Froid : nous exigeons de nos stagiaires la neutralité, le sang froid, la capacité d’analyse objective.
- Technologique : référence au cyber, à l’ingénierie.

Le titre de cette revue est tout aussi évocateur : *contre*Mesures .

*contre*Mesures, non seulement pour s'opposer à une menace, à un effet, à un événement mais également pour les prévenir.

*contre*Mesures pour résumer un enseignement spécialisé en Sûreté, Sécurité et Défense.

*contre*Mesures pour représenter un Master 2 riche de ses enseignants et intervenants atypiques et de ses stagiaires capables de raisonnements disruptifs et innovants.

contre MESURES

SOMMAIRE

contre MESURES

UN MASTER 2 ATYPIQUE

3 LE MASTER 2 INGENIERIE SURETE SECURITE DEFENSE SE DEVOILE : ENSEIGNEMENTS, ACCESSIBILITE, MODALITES D'ORGANISATION, STAGES ET CONFERENCES. TOUR D'HORIZON.

FACE A FACE

6 PATRICK BLELLY - AERONAUTIQUE & TERRORISME
Survol du monde de la sécurité aérienne et cyberaérodéfense.

8 FREDERIC LENFANT -ANALYSE CRIMINELLE & RISQUES
Eduquer à l'analyse des risques et des menaces.

10 EMILY HANCOCK-MONNOT - ANGLAIS OPERATIONNEL
Say it in english, please !

11 INGRID VERSCHEURE - INGENIERIE
L'indispensable démarche d'ingénieur en formation.

12 JEAN-LOUIS LEMMET - INTELLIGENCE ECONOMIQUE & RENSEIGNEMENT
Les auditeurs de l'IHEDN s'impliquent dans le Master 2 ISSD.

DOSSIER CYBERCRIMINALITE

13 LE NUMERIQUE BOULEVERSE NOS VIES. LA CYBERCRIMINALITE NOUS PREND DE COURT. SAVOIR POUR FAIRE FACE.

14 ZOOM SUR LA CYBERCRIMINALITE
Cyberdéfense, cybersécurité, cybercriminalité : point de situation.

18 FABRICE CRASNIER - INTERVIEW
Défaçage, cryptolockers : un monde nouveau qui a une longueur d'avance.

20 PHILIPE TRUILLET - RENCONTRE
Fais-moi confiance ? Le bon sens comme règle de sécurité !

EN SAVOIR PLUS

22 RECHERCHE - 3 ANS DE MEMOIRES
Les mémoires traités en M2 ISSD et leur classement.

24 NOS PARTENAIRES
Ensemble pour plus d'efficacité.

Editorial

ESPRIT DE DEFENSE

L'intelligence stratégique s'impose au privé comme au public. Les questions d'intelligence économique, de renseignement et plus généralement les compétences relatives aux domaines de la sûreté, de la sécurité et de la défense sont incontournables.

Ces compétences ne sont plus éparses mais regroupées transversalement, répondant ainsi à l'émergence de fonctions et de métiers spécifiques.

Ces métiers sont essentiels aux entreprises et aux administrations : à côté du savoir-faire technique émerge désormais une véritable culture, un esprit de défense !

C'est pour cette raison que les enseignants, stagiaires et partenaires du Master 2 «Ingénierie Sûreté Sécurité Défense» (ISSD) ont souhaité bénéficier d'un support de présentation, d'analyse et de sensibilisation.

J'ai le plaisir de vous présenter le 1er numéro de notre magazine : *contre*Mesures

Vous y trouverez des informations sur le Master et nos réflexions sur ces questions de haute technicité. Ce numéro accueille d'ailleurs un dossier dédié à la cybercriminalité.

Notre magazine témoigne de la qualité des enseignements et des intervenants de ce Master atypique.

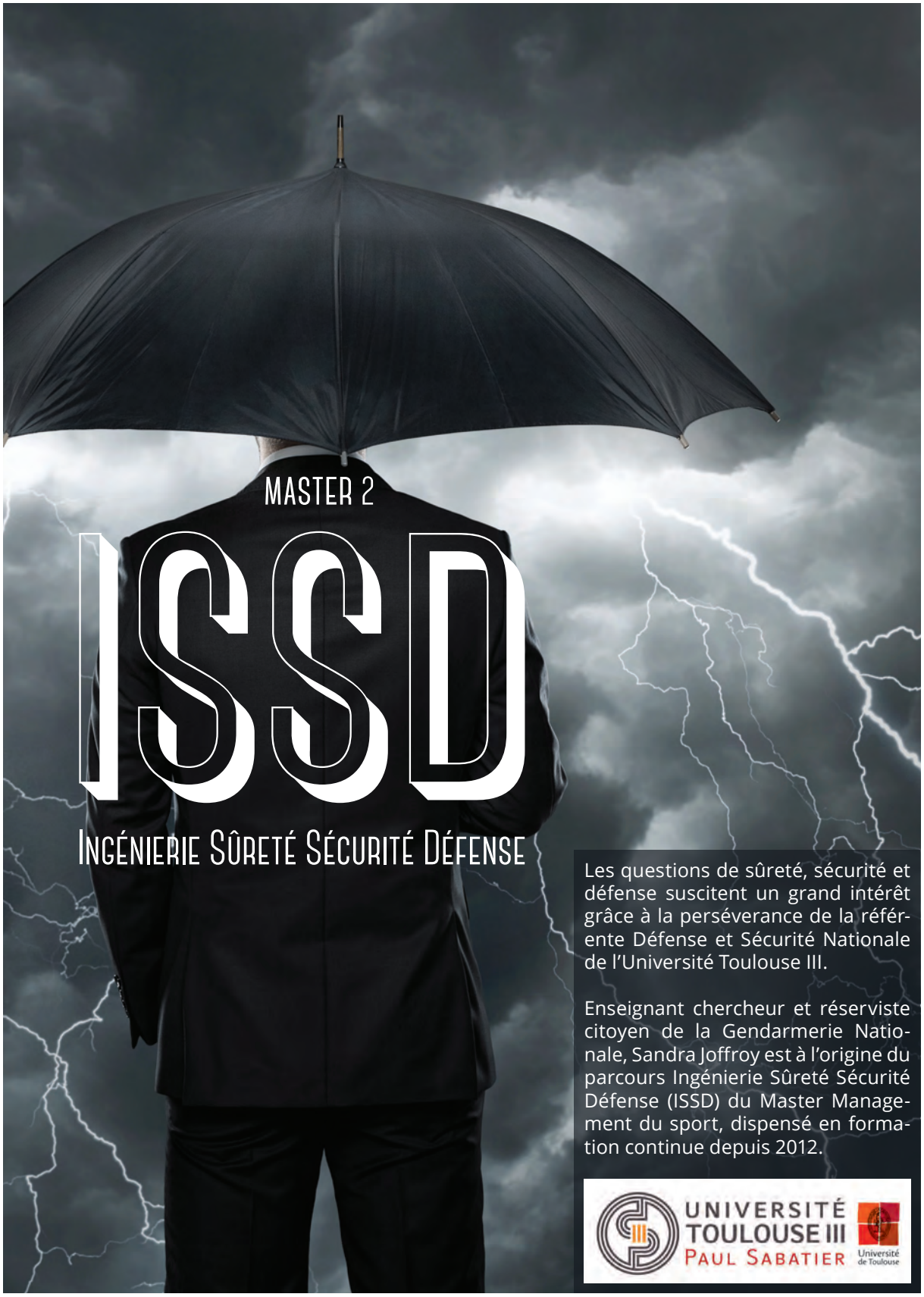
Les candidats qui nous rejoignent ont des parcours inédits, d'une grande diversité et souvent d'une valeur rare. Alors, pourquoi pas vous ?

Je remercie Serban Iclanzan, ancien légionnaire et auditeur de l'IHEDN, intervenant dans le Master 2 ISSD, directeur de presse économique, qui a particulièrement travaillé à la création de *contre*Mesures.

Bonne lecture !

Sandra Joffroy

Responsable du Master 2 ISSD
Référente défense et sécurité nationale
de l'Université Toulouse III-Paul Sabatier



MASTER 2

ISSD

Ingénierie Sûreté Sécurité Défense

Les questions de sûreté, sécurité et défense suscitent un grand intérêt grâce à la persévérance de la référente Défense et Sécurité Nationale de l'Université Toulouse III.

Enseignant chercheur et réserviste citoyen de la Gendarmerie Nationale, Sandra Joffroy est à l'origine du parcours Ingénierie Sûreté Sécurité Défense (ISSD) du Master Management du sport, dispensé en formation continue depuis 2012.

UNIVERSITÉ TOULOUSE III PAUL SABATIER Université de Toulouse

UN MASTER ATYPIQUE

INGENIERIE SURETE, SECURITE, DEFENSE

Le manque de formation aux métiers de la sécurité et de la défense pour des publics qui peuvent être très divers est à l'origine de la création de ce Master 2.

Le parcours s'adresse à des militaires pour faire évoluer leur carrière ou pour accéder à de nouveaux métiers dans le secteur privé au moment de leur reconversion vers le milieu civil.

CONFIDENTIALITE

Les stagiaires signent une charte de confidentialité. Certains occupent ou ont occupé des postes dans des administrations sensibles; certaines visites sont réservées et confidentielles.

Il accueille également des étudiants de tous les cursus y compris en sciences et techniques des activités physiques et sportives (la condition physique étant un des critères de sélection des concours d'officiers ou de sous-officiers).

Enfin, il est ouvert aux publics des ministères de l'Intérieur, de la Défense et aux salariés des grandes entreprises et aux demandeurs d'emploi.

CONFERENCES - VISITES - STAGES

Chaque promotion doit suivre des conférences obligatoires dans le cadre de l'AOR-HG (Association des Officiers de Réserve de la Haute-Garonne). Les thèmes sont variés : "Transformation du journalisme et déviance des médias", "Drônes", "Les opérations extérieures de l'armée française"...

Conférences 2016-2017 :
- La justice à Toulouse
- L'artillerie
- La Brigade de prévention de la délinquance juvénile

Seminaires 2016-2017 :
- ENAP (Ecole Nationale de l'Administration Pénitentiaire) : 2 jours
- ETAP (Ecole des Troupes Aéroportées) : 2 jours
- CISIA (Centre d'Instruction en Sécurité Industrielle de l'Armement) : 2 jours
- GIGN : 1 jour
- Garde Républicaine : 1 jour

Visite 2016-2017
- LIEBHERR-AEROSPACE : ½ journée

MEMOIRE

Le 2ème semestre est consacré à la réalisation d'un travail de recherche portant sur un sujet théorique, la préparation et la soutenance d'un mémoire.

Le mémoire permet de démontrer l'acquisition de capacités techniques, intellectuelles et théoriques enseignées en combinant les apports des différentes disciplines de la formation ainsi que les références théoriques pertinentes et associées.

Le jury apprécie l'aptitude d'analyse de chaque stagiaire sur un sujet relevant du domaine de la sûreté, sécurité et défense.

RESSOURCES

Distribution 1 clé USB sécurisée (cryptage) aux stagiaires.

Enregistrement audio de tous les cours (MFCA)

Accès au cours en streaming.

Supports de cours fournis par les enseignants.

ACCESSIBILITE

Le master est accessible uniquement en formation continue (100%), il est organisé en alternance et, pour les plus jeunes, en contrat de professionnalisation. On peut y accéder sur dossier via une validation des acquis professionnels (VAP85).

La formation est dispensée sur 1 an. Dans le cadre de la politique de formation, la validation des unités d'enseignement peut être étalée tout au long de la vie.

ENSEIGNEMENTS

350 heures d'enseignement & stage
(de 3 à 6 mois maximum),
dont 70 heures séminaires et examens

Ingénierie des dispositifs de formations opérationnelles

Ingénierie des compétences de la sécurité et théorie de la sécurité – sécurité économique et gestion de crise

- *Relations internationales : de la fin de la Guerre froide à nos jours.*
- *Les opérations extérieures de l'armée française*
- *Lecture disruptive et permanente du Monde contemporain : l'enjeu du temps et de l'espace. Résiliences. Ruptures. La pression du temps et l'effacement des distances. La surprenante notion de « caporal stratégique ». Adaptation des stratégies. Prospective*
- *Analyse des conflits: tendances, facteurs structurants. Mise en concurrence et agrégation des experts. Méthode de Delphes (et autres méthodes). Les ONG*
- *Processus de prise de décision: La nature de l'analyse décisionnelle et sa place dans la théorie des relations internationales ; Paradigme bureaucratique (étude de cas). TD : cas pratique synthèse et application.*
- *Sécurité-sûreté et gestion globale des risques : référentiels, méthodologies et cas appliqués*
- *Culture de la sécurité et intelligence économique*
- *Organisation et fonctionnement du Renseignement en France* • • •

Sécurité, hygiène et santé au travail Sécurité des APS – Politique de sécurité

Droits et obligations en matière de sécurité

Sécurité et défense – Sécurité économique – Enjeux industriels géostratégiques

- *Organisation et fonctionnement de la sécurité économique au sein des services étatiques*
- *Organisation et fonctionnement de la sécurité économique au sein de l'entreprise privée Initiation à l'intelligence économique.*
- *Histoire, définitions, enjeux et acteurs. La veille stratégique et les différents types de veille, les moyens et outils de veille. La stratégie d'influence. Le cycle du renseignement, la cellule de veille. Sécurité de l'information. Les risques et menaces, la sécurité industrielle et la sécurité financière.*
- *De l'information au renseignement. Information. Evaluation. Exploitation. Collation. Analyse*
- *La Recherche humaine* • • •

Sécurité et Sûreté

- *Les détournements d'avions et le terrorisme aérien.*
- *Historique. Plans gouvernementaux actuels. Cas concrêts. Les actes terroristes et leurs séquences d'élaboration. Les menaces modernes et/ou nouvelles menaces : les cyber-attaques et le contrôle aérien, les drones et les armes NRBC* • • •

Sécurité des systèmes d'information (SSI) cybersécurité – Systèmes intelligents

Langue Vivante – Anglais scientifique et opérationnel

FACE A FACE

TERRORRISME & AERONAUTIQUE

Patrick BLELLY

intervient dans le cadre du Master 2 ISSD dans le cadre d'un module intitulé « Les détournements d'avions et le terrorisme aérien ». Pilote de ligne sur A330 et A340, B747, il a une double carrière – civile et militaire – et affiche 42 ans d'aviation dont 15 années passées dans l'Armée de l'Air sur Transall C-160, DC-8 et un appareil de guerre électronique à l'époque de la Guerre du Golfe. Réserviste de la Gendarmerie Nationale, il est Lieutenant-colonel (rc) à l'état-major de la Gendarmerie des Transports Aériens (GTA) à Paris où il apporte son expertise sur les questions relatives à la menace terroriste et aux détournements d'avions. Il fait aussi partie de plusieurs réseaux cyberdéfense nationaux près de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et à Toulouse où il s'investit sur les questions de cyberaérodéfense.

Patrick Blelly, pouvez-vous nous dévoiler les questions que vous abordez avec les stagiaires du Master 2 ISSD ?

Patrick Blelly : Dans le cadre de mon intervention sur le détournement d'avions et le terrorisme aérien je cherche à donner en premier lieu une culture globale de ces phénomènes aux étudiants. Nous abordons ensemble l'histoire, les différents type de terroristes, les profils psychologiques, les méthodes : les bombes à bord, les tirs de missiles, les attaques par les drônes, les clandestins dans les trains d'atterissage...

Est-ce un enseignement que vous axez surtout sur l'expérience ou vous vous inscrivez aussi dans la prospective ?

PB : Cet enseignement n'aurait pas de sens si on se cantonnait à un simple passage en revue des expériences. En réalité nous accordons beaucoup de temps à l'étude des menaces futures, à la veille Internet sur les menaces terroristes. Ce sont des questions préoccupantes. Aujourd'hui nous intervenons avec la RCC Toulouse auprès de l'*Aerospace Valley* dans une œuvre d'expertise et sensibilisation. Nous n'avons pas le droit de faire des audits, alors nous faisons des analyses de maturité des sociétés sur les questions de risques cybertechnologiques. Cette pratique et mes actions au profit de OIV (opérateurs d'importance vitale) auprès de l'ANSSI me permettent d'accrocher les stagiaires du Master à un monde en perpetuel mouvement, à les sensibiliser à des risques qui sont en mutation permanente. Je dois reconnaître qu'ils sont particulièrement réceptifs.

Quel est pour vous l'intérêt d'un Master 2 Ingénierie Sécurite Surêté Défense, tel qu'il a été défini à l'Université Toulouse III Paul Sabatier ?

PB : Ce Master est essentiel et il est très bien. La surêté et la sécurité ne sont plus des sous-matières ou des sous-compétences. Avant quand nous voulions traiter en entreprise de ces questions, nous cherchions des compétences parmi les sachants... Ce temps est révolu. Aujourd'hui ce sont des métiers à part entière, avec des postes pourvus de moyens et d'un classement adéquat dans la hiérarchie d'une entreprise.

L'ensemble des enseignements du Master vous semble suffisant pour armer les candidats d'une compétence en la matière ?

PB : Pour moi ce Master est triplement riche pour ceux qui le choisissent. Il y a d'abord le savant mélange entre la qualité des universitaires qui interviennent et les cours donnés par des opérationnels avec un *background* impressionant : des gens en activité

FACE A FACE

et des anciens militaires des unités d'élites, des gendarmes spécailisés dans des domaines rares, des anciens des services spéciaux, des opérationnels du monde de l'entreprise en intelligence économique, en communication et influence… Le fait d'avoir des entités du niveau de l'IHEDN, de la DGA, du GIGN comme partenaires est une marque de reconnaissance et de sérieux.

La deuxième richesse consiste dans la diversité des thématiques abordées : je vois l'ingénierie, le droit, le renseignement, la cybersécurité, l'analyse décisionnelle, la gestion des risques, la sécurité économique, la géopolitique, la culture de défense et je suis loin de tout évoquer.

Enfin, la troisième chose que je souhaite évoquer est le fait que ce Master 2 est une sorte d'auberge espagnole. C'est incontestablement un atout. L'étudiant issu d'une Licence Gestion de la condition physique des intervenants en situation hostiles, va cotoyer celui venant de Sciences-Po ou de Psycho et tout ce monde va avoir dans la même promo des anciens des services spéciaux, d'unités ou d'administrations particulières et confidentielles, d'entreprises de pointe qui sont là parce qu'ils se trouvent en reconversion ou en acquisition de compétences. Ces opérationnels apportent un regard d'une qualité exceptionnelle aux très jeunes. A l'inverse ces derniers ouvrent à leur ainés les cartes mentales d'une nouvelle génération pleine de ressources et avec une capacité nouvelle de lecture et d'intégration des risques.

Pour quelles raisons orienterez-vous quelqu'un vers le Master 2 ISSD ?

PB : A l'échelle nationale c'est un des Masters les plus en pointe aujourd'hui. Il suffit de voir la renomée acquise en si peu de temps, les candidatures qui affluent…De plus il s'agit d'une matière appelée à se développer, car nous allons avoir besoin de spécialistes de la sécurité, de la sûreté, de la cybersécurité. Nous devons préparer des cadres à la pointe de la protection des futures sociétés avec lesquelles ou au sein desquelles ils seront amenés à travailler. Aujourd'hui la sûreté est un métier complet et à part entiere.
Pourquoi ce Master en particulier ? Pour la réputation acquise après seulement 4 promotions. Aujourd'hui il est *« combat proven »*.

RCC: Réserve Citoyenne
RCC : Réserve Citoyenne Cyberdéfense

PARCOURS - ATTENTES - OBJECTIFS

Maxime R. est déjà titulaire d'un Master en sécurité et gestion du risque. Voulant mettre toutes les chances de son côté il a choisi de suivre le Master 2 ISSD pour être polyvalent en entreprise dans le domaine de la sécurité et de la sûreté. Maxime trouve ce Master « très bien » et il apprécie particulièrement la qualité des intervenants, les enseignements dans le domaine du renseignement, l'ouverture sur la géopolitique et les relations internationales. Il trouve que sa promo est très hétérogène, à taille humaine ce qui a facilité la constitution d'un groupe. Questionné sur la rencontre avec des stagiaires forts d'expériences professionnelles conséquentes et dans des domaines rares, il apprécie leur humilité, les explications et ce qu'il apprend à leurs côtés.

Jean E. est ancien militaire. Il a fait une carrière complète dans une unité relevant de la Direction du Renseignement Militaire (13°RDP) et des unités d'action d'influence avec de nombreuses projections sur des théâtres d'opérations. Jean a déjà une expérience dans le domaine de la sûreté et souhaite acquérir un cadre théorique en plus de la pratique. Sa reconversion au milieu civil l'ayant amené à travailler pour le ministère des Finances, il prépare aujourd'hui une réorientation vers le ministère de l'Intérieur. Il aime dire du Master « il y a des choses que l'on croyait savoir, mais ce qui est certain c'est que cela me remet dans le bain » ! Jean adore échanger avec une jeune génération dont la façon de voir les choses est très différente et qui est naturellement habituée à un monde où le numérique est omniprésent.

FACE A FACE

ANALYSE CRIMINELLE & RISQUES

Frédéric LENFANT

travaille actuellement pour la société SOGETI en tant qu'analyste en cybermenace (en anglais : *threat intelligence*) dans le cadre du CERT (*Computer Emergency Response Team*). Il a fait toute sa carrière dans la Gendarmerie essentiellement dans le domaine judiciaire (homicides, stupéfiants, criminalité organisée) au sein d'unité territoriales, mais aussi dans des cellules relevant des brigades de recherche pour finir à la Section de Recherches en qualité d'analyste criminel. Il a créé et a été le chef du Groupe d'appui renseignement de la Section de Recherches de la Région de Gendarmerie Midi-Pyrénnées et dans ses qualifications d'analyste criminel il s'est occupé entre autres du traitement de la téléphonie, la data analyse, des recoupements en la matière... Frédéric LENFANT est titulaire d'un Master 2 spécialisé en "Ingénierie et Management en Sécurité globale apliquée". Aujourd'hui il est aussi réserviste de la Gendarmerie Nationale dans les nouvelles structures de cyberdéfense.

Quels sont vos domaines d'intervention dans le cadre du Master 2 ISSD ?

Frédéric LENFANT : J'interviens d'abord pour présenter l'analyse criminelle, comment faire des recoupements dans l'information pour orienter tous cela par la suite avec une méthodologie d'analyse de risque et par le biais des différentes méthodes d'analyse des risques que j'ai moi-même assimilées pendant mon Master. Tout ceci a pour objectif de donner une approche globale au lieu de focaliser sur un seul élément. Cela va très bien avec l'analyse criminelle car il s'agit d'etre capable de faire le lien entre différents événements et différents éléments. Bien entendu, tout cela appliqué à la sécurité. Il s'agit au final d'un eseignement sur la méthodologie d'analyse globale et de l'analyse systémique appliquée à la sécurité.

Quand vous parlez de recoupement, vous pensez aux processus habituels d'évaluation, collation...

FL : Non c'est plutôt l'application dans une enquête judiciaire. Au final j'oriente beaucoup sur l'analyse globale de l'information dans la gestion des risques. Par exemple un incident « sécurité » dans une entreprise. Je fais parfois un cas concret pour voir comment on va pouvoir analyser les différents événements qu'il peut y avoir lors d'une situation et faire du lien entre ces événements.

Comment analysez-vous la manière dont se construit l'enseignement au sein de ce Master ?

FL : Dans le Master que j'avais fait j'avais beaucoup apprécié l'approche systémique. C'est aujourd'hui ce que je cherche à apporter dans les M2 ISSD de Toulouse, car je considère que dans la sécurité il faut avoir une approche globale. Je sais que nous sommes plusieurs intervenants et qu'il nous arrive de traiter parfois de questions similaires ou fortement complémentaires. Ceci n'est pas rédhibitoire. Par exemple j'évoque l'intelligence économique, alors que je sais qu'il y a un module qui est dédié à cet aspect. Il y a une réflexion à faire sur le fil conducteur, sur la chronologie des cours. Cela nous permettrait de gagner en efficacité ou insister sur certaines compétences de manière coordonnée. J'accorde aussi une grande importance à une partie qui peut paraître rébarbative et qui est cependant essentielle : il s'agit de la sémantique, de la définition des notions de sécurité, sûreté, risque, menace. Ceci pour éviter les moments de flou et de doute à nos stagiaires.

Vous accordez donc une grande importance à la justesse des notions, aux cadres théoriques...

LF : Attention, je reste très attaché au pragmatisme, à la réalité du terrain... Je travaille en complémentarité avec Fabrice Crasnier qui intervient sur la cybersécurité. Lui, il est très technique et dans une démarche façon gendarmerie, de mon côté j'apporte une démarche type entreprise. Aujourd'hui je vois les deux domaines et souhaite privilégier une vision globale. Je prends pour exemple la partie *threat intelligence*, les indicateurs de compromission et tous ces éléments qui sont typiquement dans la culture « entreprise ». J'intégre aussi des notions de sensibilisation dans mes cours, tel que cela est fait aux entreprises par les services spécialisés de l'Etat. Je crois aussi que de nos jours il y a un énorme rapprochement à faire entre la sûreté et la cyber. L'une ne peut plus être indépendante de l'autre, mais nous restons encore très segmentés par une logique de pôles de spécialité différents. Il faut se situer à un niveau supérieur qui prendrait en compte les contraintes des uns et des autres pour mieux faire face aux menaces

FACE A FACE

et aux risques. Voici typiquement un retour d'expérience de terrain...

Vous avez devant vous des stagiaires qui ont un parcours professionnel très riche, qui ont parfois servi dans des unités assez confidentielles et des stagiaires qui achèvent un premier cycle complet de formation universitaire. Comment appréciez-vous cette rencontre ?

FL : C'est très riche et très fort. Quelqu'un qui a de l'expérience met rapidement du concret dans la théorie et il saura par expérience pourquoi telle ou telle chose fonctionne d'une certaine façon. Il finira par mettre un socle théorique sur quelque chose qu'il maîtrise en pratique. En face, les stagiaires qui sont toujours dans le circuit académique classique auront un socle plus construit - par exemple sur des procédures de qualité - , un raisonnement déjà formaté et parfois plus organisé. Pourtant tout prend corps pour eux aussi dans les témoignages de ceux qui ont l'expérience. La rencontre de ces deux profils crée un cercle vertueux.

Pourquoi choisir le M2 ISSD ?

FL : Il faut s'adapter à la situation actuelle qui a beaucoup changé dans notre pays. Les anciennes façons de faire en matière de sécurité en faisant appel soit à des anciens policiers, soit à des anciens militaires ne suffisent plus. Il faut mettre en place un volet professionnel, un raisonnement par rapport à des exigences de politique de sécurité. Il faut à tout prix s'orienter davantage sur un formalisme des politiques de sécurité et une empreinte de ce qui se fait en entreprise. Nous sommes dans une permanente adaptation aux besoins. Ce Master offre ce cadre et permet aussi la rencontre d'un grand nombre de professionnels.

PARCOURS - ATTENTES - OBJECTIFS

Youna CONNAN-ANDRE est titulaire d'un Master 1 en Psychologie clinique et pathologique, spécialité déviances et exclusions. Elle a suivi aussi une formation d'assistante sociale qui l'a amené à travailler avec la PJJ (Protection Judiciaire de la Jeunesse) sur les questions de radicalisation. L'intérêt de ce Master réside pour elle dans la possibilité d'acquérir des compétences dans un domaine différent. Elle vise le ministère de la Justice, l'Administration pénitentiaire ou la défense. Youna trouve qu'elle a trouvé dans les enseignements des choses qu'elle voulait confirmer, mais aussi des choses auxquelles elle s'attendait moins, mais qui sont passionnantes. La rencontre avec les autres profils et parcours des stagiaires du Master est le secret d'une « ouverture d'esprit » qui met très vite son empreinte sur le groupe, contrairement à des formations classiques visant des étudiants sortis des mêmes parcours.

Pierre MATA est titulaire d'une Licence profesionnelle GCPSH (Gestion de la condition physique des intervenants en situations hostiles). Il est sapeur-pompier volontaire et titulaire du SSIAP3. Il veut donc se spécialiser dans le secteur de la sécurité et de la sûreté. Pierre trouve que ce Master correspond à toutes ses attentes et est enthousiasmé par les cours en relations internationales et géopolitique qu'il voudrait encore plus riches. Il ajoute que les contacts avec ceux qui ont déjà un *background* professionnel ou viennent d'autres cursus universitaires complètent et enrichissent les cours de manière naturelle.

FACE A FACE

ANGLAIS OPERATIONNEL

EMILY HANCOCK-MONNOT
professeur d'anglais au sein du Département Langues Vivantes et Gestion de l'Université Toulouse III Paul Sabatier

Vous enseignez un cours d'anglais que vous avez spécifiquement adapté au Master 2 Ingénierie Sécurité Sureté Défense. Pouvez-vous nous en dire davantage ?

Emily Hancock-Monnot : Une langue est un instrument de communication, mais aussi d'ouverture, de connaissance. Aujourd'hui la maîtrise de l'anglais est un atout incontestable dans le monde professionnel. Le Master 2 ISSD dans lequel j'interviens est un Master professionnalisant au sein duquel on traite de questions d'intelligence, de renseignement, de défense, de sûreté, de cybersécurité... Les intervenants dans les différentes disciplines utilisent parfois des documents libellés en anglais et les recherches dans ces domaines sont souvent le produit d'universités anglo-saxonnes. Les débouchés imposent aux stagiaires du Master une maitrise générale, mais aussi spécifique de la langue anglaise. Nous avons en conséquence deux objectifs: développer l'aisance à l'oral et donner les clés d'un langage professionnel spécifique au milieu de la sécurité, de la surêté et de la défense.

Quel est le niveau d'anglais des étudians à l'entrée du Master ?

EHM : Les niveaux sont trés variés. Le parfaitement bilingue côtoie l'étudiant moyen qui a toujours galéré à l'oral. En réalité c'est la richesse des profils de ceux qui rejoignent ce Master qui nous permet de tirer tout le monde vers le haut. Entre ceux qui viennent du monde professionnel, parfois après des carrières internationales et ceux qui se préparent pour le marché du travail, il existe un fort intérêt pour la maîtrise de l'anglais. C'est très hétérogène en terme de parcours et d'apprentissage de la langue. J'ai de très bons retours des stagiaires.

Que diriez-vous à quelqu'un pour recommander le Master 2 ISSD ?

EMG : Il faut venir à Toulouse rien que pour ça ! Je suis très enthousiaste. La diversité des profils, l'impressionnant CV des intervenants... C'est une formation qui est géniale et Sandra Joffroy à bâti ce Master un peu à son image. C'est quelqu'un qui entreprend, qui est très professionnel, qui aime innover, qui est à l'affût et qui cherche toujours à avancer. Avec elle il faut tenir le rythme, ce n'est pas tellement du *keep calm*, mais plutôt du *straight on, right now* !

PARCOURS - ATTENTES - OBJECTIFS

Geoffroy TRUBERT est déjà titulaire d'un Master 1 en Sciences Politiques à Bordeaux et d'un Master 2 en anglais de Relations internationales et Pratiques culturelles qu'il a parfait en Asie. Il est aussi réserviste de l'armée de terre au 126 RI de Brive. Il serait tenté par un engagement en tant qu'officier sous contrat. En attendant il a choisi le M2 ISSD « *pour descendre d'un niveau trop théorique vers un niveau plus pratique d'un Master profesionnalisant* ». Geoffroy dit savourer la qualité des intervenants, le côté pratique et ces premiers mois passés à découvrir une certaine culture en matière de renseignement. Il considère que compter parmi ses camarades de promo des anciens « opérationnels » est une sorte de bonus, un apprentissage supplémentaire : « *c'est comme si on me racontait des histoires et je m'en nourris volontiers* » !

FACE A FACE

INGENIERIE

INGRID VERSCHEURE
maître de conférence à l'Université Toulouse Jean-Jaurès au sein du « Laboratoire Education, Foramtion, Travail, Savoirs » et co-responsable du Master 1 sciences de l'éducation. Référente pour les Sportifs de Haut-Niveau de sciences de l'éducation.

Sur quelle partie de l'enseignement intervenez-vous au sein du Master 2 ISSD ?

Ingrid Versheure : J'interviens sur le cadre théorique essentiel pour ce Master : qu'est-ce que l'ingénierie de la formation, comment peut-on la construire ? J'ai intitulé ce cours « Démarche d'ingénieur de formation ». Les stagiaires voient beaucoup de choses très différentes et très concrètes tout au long de l'année. Mon rôle est de leur apprendre à systématiser et donner une logique scientifique à leur compétence. Ce n'est pas un hasard si on parle d'ingénierie dans l'intitulé du Master...

Que pensez-vous de ce Master et du profil de sesstagiaires ?

IV : Je ne suis pas une spécialiste de la sécurité ou de la défense, mais je trouve cet enseignement particulièrement pertinent dans le contexte actuel. Nous avons un moyen de former des ingénieurs, des spécialistes e itifs de formation dans ce domaine. Je suis agréablement surprise par la diversité des intervenants et la richesse en connaissance et en expérience qu'ils apportent. J'apprécie cette adaptation permanente aux besoins qui remontent du terrain et je me surprends parfois à me dire que je voudrais moi-même assister à l'intégralités des cours du Master. En ce qui concerne les étudiants et leur profil, il y a parfois une difficulté liée à la différence des parcours. Cette différence est également source de richesse : les débats et les discussions qu'ils y engagent en témoignent. Cela nécessite une préparation des cours assez complexe. Finalement cela se passe très bien, parce qu'ils osent questionner beaucoup ce qui fait avancer le groupe.

Avec Sandra Joffroy nous travaillons aussi sur les mémoires en aidant les stagiaires en leur apprenant à rédiger un véritable mémoire de Master 2 dans lequel ils doivent être capables d'abstraction, de recul, de définition d'une grille d'analyse de portée générale affranchie du simple cas d'espèce qui justifie leur recherche.

Qu'est-ce qui explique la réussite et la reconnaisance dont jouit le Master 2 ISSD ?

IV : Ce qui caractérise le M2 ISSD c'est l'adéquation et l'adaptation aux besoins réels du terrain. Il s'agit d'un parcours qui apporte des compétences au-delà du diplôme. A mon niveau je vois bien que les stagiaires partent tous à même de mettre en place un plan de formation et analyser un besoin.

STAGIAIRES ATYPIQUES

Les promotions du Master 2 ISSD accueillent des stagiaires atypiques : officiers ou sous-officiers de Services Spéciaux, de la Gendarmerie, de l'Armée de Terre et de la Marine, mais aussi de la DGA, de la répression des fraudes, etc. Ainsi dans la dernière promotion, se cotoyaient un cadre de la Légion Etrangère, un spécialiste italien de l'intelligence économique et un officier d'état-major de l'armée algérienne ...

METHODE SPECIFIQUE

Des sources transversales pour un enseignement cohérent et convergent. Pour aborder la question du renseignement et de la prise de décision, le stagiaire bénéficie de l'intervention de spécialistes complémentaires : une vision de type sciences politiques en matière de processus décisionnels, une synthèse du cycle du renseignement et de sa production par des anciens officiers qualifiés, un parallèle avec l'intelligence économique par des opérationnels et le témoignage concret d'un ancien officier de terrain du 13ème RDP spécialisé dans la recherche humaine.

FACE A FACE

INTELLIGENCE ECONOMIQUE & RENSEIGNEMENT

JEAN-LOUIS LEMMET

lieutenant-colonel (er), actuellement président de l'association régionale des auditeurs de l'IHEDN (AR19).
Ancien officier d'active au sein de la Légion étrangère où il a été le commandat en second du 4ème Régiment Etranger (l'école de la Légion), il a quitté l'armée d'active en 2010. Il a notament commandé le Centre d'entrainement commando de Givet et a servi à l'Etat-Major de la 11ème Brigade Parachutiste en qualité du chef de bureau renseignement. Il est également directeur adjoint du cours supérieur des ORSEM (Officiers de réserve spécialistes d'état-major).

Vous êtes le président de l'association régionale des auditeurs de l'IHEDN (Institut des hautes études de défense nationale) qui est un des partenaires majeurs du Master 2 ISSD. Quelle est la nature de ce partenariat ?

Jean-Louis LEMMET : L'association régionale des auditeurs IHEDN (AR-19 Midi-Pyrénées) intervient dans le master que dirige Sandra Joffroy au titre de l'expertise qu'elle détient en termes de réflexion sur les questions de sécurité et de défense. En effet, plus de la moitié des intervenants, ainsi que la responsable du master, sont des auditeurs de l'IHEDN, ou des membres associés de l'AR19.

L'IHEDN a pour but de développer l'esprit de défense et de sensibiliser aux questions internationales. Grace aux différentes sessions qu'il organise : sessions nationales "politique de défense", sessions nationales "Armement et Economie de Défense", sessions en région, et sessions intelligence économique en particulier, il recrute des auditeurs au bon niveau pour relayer son message dans différents domaines de la société et en particulier dans le monde de l'enseignement.

C'est dans ce cadre que nous intervenons dans ce Master depuis sa création, dans les enseignements spécifiques dédiées aux relations internationales, à la politique de défense de la France, au travers de la présentation du Livre blanc sur la défense et la sécurité 2013, sur l'organisation et les missions de nos armées, de notre gendarmerie et de notre police, ainsi que sur l'intelligence économique et enfin sur la cyberdéfense ; autant de domaines ou de par le recrutement de ses auditeurs, l'AR19 détient une réelle expertise.

Vous enseignez personnellement au sein du Master 2 IISD.

JLL : Je propose une initiation à l'intelligence économique, l'objectif de la formation dispensée étant la sensibilisation et l'information générale sur les différents sujets que recouvre l'intelligence économique par l'acquisition d'un minimum de connaissances nécessaires pour aborder un sujet touchant à la veille et à la sécurité, dans le monde de l'entreprise en particulier.

Je fais d'abord une présentation de la veille stratégique et des différents types de veille, des moyens et des outils de veille. Ensuite je traite de la stratégie d'influence, pour finir par aborder des notions précises comme le cycle du renseignement, la cellule de veille, la sûreté et sécurité, sécurité de l'information, la sécurité industrielle et la sécurité financière.

La vocation de l'IHEDN (Institut des Hautes Etudes de Défense Nationale) est de former des responsables de haut niveau de la fonction publique civile et militaire ainsi que des différents secteurs d'activité de la Nation. L'Institut contribue à promouvoir et à diffuser toutes connaissances utiles sur des questions de défense, de politique étrangère, d'armement et d'économie de défense.

Les associations régionales de l'IHEDN-AR, regroupent les auditeurs des sessions régionales de l'IHEDN ainsi que des auditeurs des sessions nationales et des cadres résidant en province. L'engagement des auditeurs se poursuit au delà des sessions régionales et affiche trois objectifs :

- *maintenir et renforcer les liens entre les auditeurs de l'IHEDN*
- *développer l'esprit de défense dans la Nation;*
- *contribuer à la réflexion sur la Défense Nationale et apporter son concours à l'Institut.*

CYBER

Securite - Surete - Defense

Les relations entre les Nations, les puissances, les organisations, sont profondémment influencées par la numérisation de notre espace d'action. Certains parlent même de "cyber guerre". A l'échelle des entreprises ou des particuliers, nous parlons de "cybersécurité".

Les technologies modernes appuient aujourd'hui une criminalité ordinaire mais elles pourraient être dès demain au service de nouvelles formes d'extorsion et de terrorisme, par des attaques menées contre nos systèmes d'information.

La cybersécurité est réellement une composante essentielle de la sécurité des Nations, des Entreprises et des Personnes.

Nous avons donc décidé de dédier ce dossier à la cybercriminalité, premier niveau de menaces à mieux appréhender pour construire une cybersécurité efficiente.

DOSSIER

CYBERCRIMINALITE

DOSSIER CYBERCRIMINALITÉ

ALBERT EINSTEIN « L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique. »

ZOOM

CYBERCRIMINALITE - CYBERSECURITE - CYBERDEFENSE

INTERNET EST DEVENU EN QUELQUES ANNÉES UN VECTEUR D'INFORMATIONS INCONTOURNABLES TANT DANS NOTRE VIE PRIVÉE QUE DANS NOTRE SPHÈRE PROFESSIONNELLE.

Cette boulimie d'informations attise également toutes les convoitises, pour nous nuire directement ou bien atteindre à travers nous, notre entreprise. La Gendarmerie Nationale, à l'aide de son réseau CYBERGEND, lutte depuis déjà plus de 15 ans contre les comportements cybercriminels. Toutefois, force est de constater que la mission est difficile à remplir. En effet, la cybercriminalité est l'une des formes de criminalité qui connaît actuellement la plus forte croissance. Outre les failles de nos outils informatiques, les malfaiteurs exploitent également celles de notre système législatif du fait des fonctionnalités des technologies modernes en perpétuelle évolution (formation des personnels de la chaine judiciaire de l'enquêteur au magistrat), des « lenteurs » administratives (temps judiciaire), des conflits et des règles internationales (ratification des conventions, diplomaties), de la rapidité du réseau (temps numérique) ou bien de l'anonymat pour commettre les infractions les plus diverses.

Gendarmerie nationale
Une force humaine

Les technologies de l'information, et Internet en particulier, sont devenues des armes de destruction, de compromission et de délinquance en tout genre. Ainsi, les États, les entreprises, les forces armées, les activistes et même les particuliers puisent désormais dans cet arsenal pour capter des informations ou de l'argent, diffuser des rumeurs ou provoquer des dysfonctionnements chez leurs adversaires.

Comme les systèmes d'information irriguent désormais toutes les organisations modernes, nos vies personnelles et professionnelles se trouvent dépendantes de la cybersécurité. Comme l'indique Nicolas Arpagian (*in* La Cybersécurité) : «*Chacun, dorénavant, a le devoir de s'informer sur les enjeux de la sécurité numérique* ».

La cybersécurité peut être définie comme l'ensemble des processus à mettre en place pour garantir l'intégrité du système d'informations dans sa globalité.

Alors que l'informatique touche désormais la plupart de nos activités, la grande délinquance s'est tout naturellement attaquée aux faiblesses du système. Ainsi est née la cybersécurité, destinée à prévenir les actes cybercriminels.

260

LE NOMBRE D'ENQUÊTEURS EN NOUVELLES TECHNOLOGIES AU SEIN DU RÉSEAU CYBERGEND

3,3

(MILLIARDS D'EUROS) C'EST LE MONTANT EN 2015 DE LA PERTE DE DONNÉES SENSIBLES POUR LES ENTREPRISES FRANÇAISES

La cybercriminalité, quant à elle, est définie comme étant l'ensemble des infractions pénales qui se commettent via les réseaux informatiques, notamment sur le réseau Internet.

Elle est caractérisée par les atteintes aux biens (fraude à la carte bleue sur Internet, vente d'objets volés ou contrefaits, piratage d'ordinateur, vente de médicaments sans ordonnance, vente de stupéfiants…) et les atteintes aux personnes (diffusion d'images pédophiles, injures à caractère racial, atteintes à la vie privée…). Les exemples de cybercriminalité sont légion à l'encontre des sociétés à l'aide de *ransomwares* tels CTB-Locker, Dridex, TeslaCrypt, KeRanger (Mac OS) ou Locky. Les actes de piratage du site TV5 Monde ou de sites administratifs en ont été des exemples marquants en 2015.

Pourtant, la prévention des incidents contre les attaques informatiques relève souvent de réflexes simples de prudence dans l'utilisation de sa messagerie de son smartphone ou tablette, lors de paiement sur Internet, de consultation d'un compte Facebook, de sécurisation par mot de passe ou lors du téléchargement d'applications de tiers inconnus.

LE RÉSEAU CYBERGEND

Pour prévenir les débordements pouvant survenir sur la toile, la gendarmerie forme depuis plus de 15 ans des personnels chargés de surveiller et de relever l'ensemble des infractions à la loi pénale commis dans et au travers du cyberespace.

Le réseau Cybergend est actuellement constitué de 260 enquêteurs en nouvelles technologies (N'tech) secondés par 1 700 correspondants N'tech répartis dans les unités territoriales.

Ce réseau s'appuie sur le haut niveau d'expertise du Centre de lutte contre les criminalités numériques (C3N).

Dans 76% des cas, les intrusions dans les réseaux informatiques se commettent par vol ou déduction de code d'accès, il faut dire que les 3/4 des internautes utilisent le même mot de passe pour l'ensemble de leurs connexions.

A cet effet, l'ANSSI publie de nombreux guides sur la thématique de la cybersécurité dont celui des bonnes pratiques de l'informatique destinées à tout public (www.ssi.gouv.fr/).

Malgré les efforts des sociétés en IT et les acteurs de la Cybersécurité, la cybercriminalité est toujours la forme de criminalité qui connaît la plus forte croissance depuis ces quinze dernières années.

Le nombre d'entreprise exposées à la perte de données sensibles aurai doublé en 7 ans, elle serait estimée à 3,3 milliards d'euros en France l'an dernier.

La cyberdéfense représente l'avenir de la Défense dans un milieu virtuel et sans frontière.

Afin d'ajouter une nouvelle force dans la lutte contre cette criminalité organisée, l'Etat-major des armées et la Gendarmerie Nationale porte une nouvelle priorité stratégique pour la souveraineté nationale : la cyberdéfense. Par le biais de nombreux acteurs, le ministère de la Défense participe activement à la protection et à la défense des systèmes d'information dans le cyberespace.

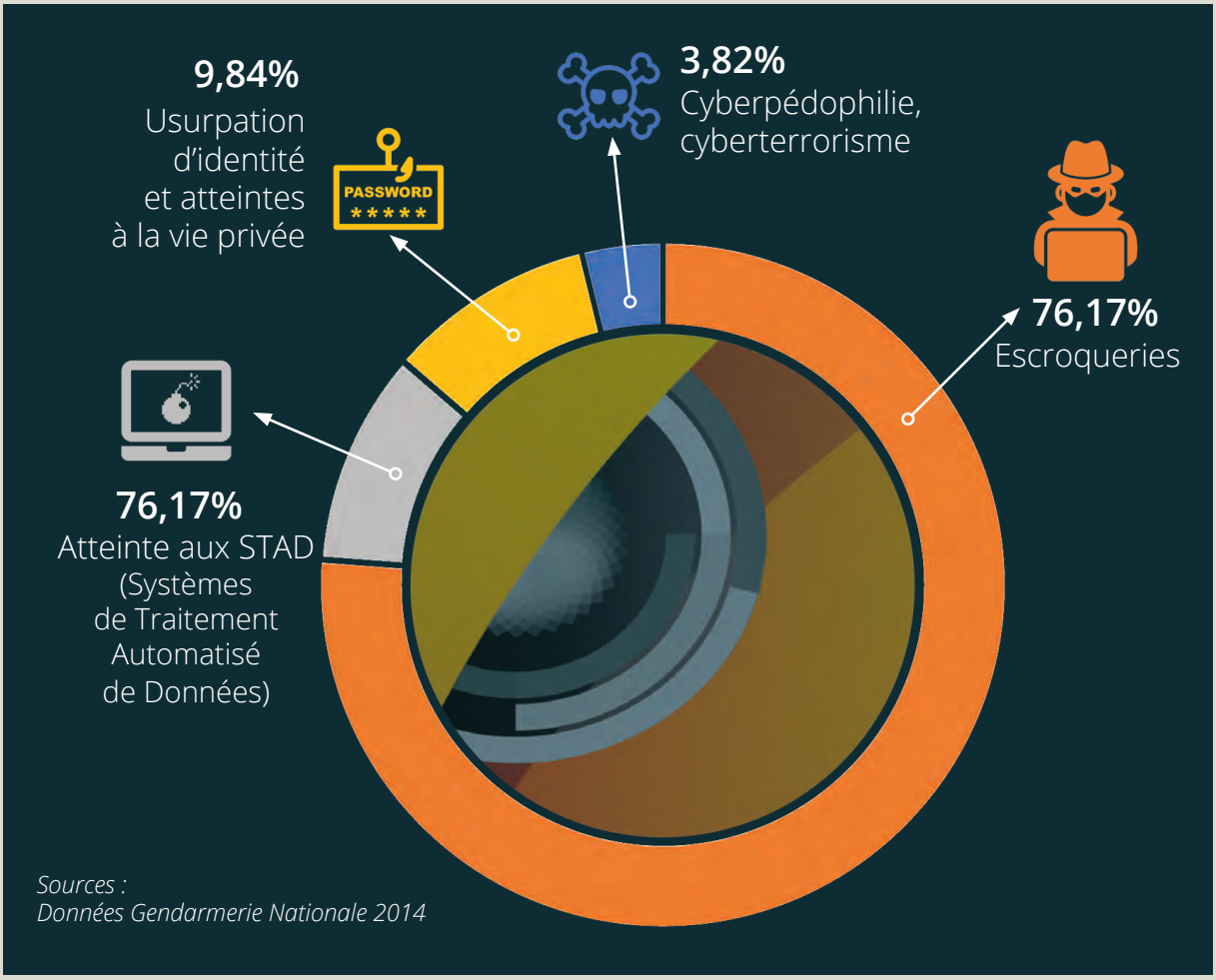
Le réseau de la Réserve citoyenne cyberdéfense (RCC) se compose de 150 membres répartis en 7 groupes de travail et 8 équipes régionales.

Le réseau entreprend un large éventail d'actions allant de l'organisation d'événements, tels que le premier Symposium académique de recherche en cyberdéfense de septembre 2013, à des travaux de réflexion ou de sensibilisation aux enjeux liés à la cyberdéfense. Il étend progressivement son activité en région en se concentrant sur les opérations de sensibilisation à destination des PME-PMI. Les travaux du réseau se font en lien avec la Direction générale de la gendarmerie nationale (DGGN), l'Agence nationale de sécurité des systèmes d'information (ANSSI) et la Direction générale de l'armement (DGA).

Les réservistes citoyens, collaborateurs bénévoles du service public, sont tous liés à la cyberdéfense dans leur vie professionnelle et se sont engagés pour mettre leur expertise au profit de la protection du pays. Ils ont des profils variés offrant à la réserve un large panel de compétences aussi bien en recherche et ingénierie, qu'en droit, management, R&D...

Major Fabrice Crasnier

CYBERCRIMINALITE EN CHIFFRES



INTERVIEW

LA CYBERCRIMINALITÉ : UNE MENACE REELLE

MAJOR FABRICE CRASNIER,
Intervenant majeur au sein du Master 2 ISSD, commandant de la division analyse criminelle et investigations spécialisées de la section d'appui judiciaire (SAJ) de la région de Gendarmerie Midi-Pyrénées. Ingénieur en informatique en conception et développement, doctorant en informatique et à l'IRIT, Fabrice Crasnier est aussi directeur d'enquête judiciaire spécialisé en technologie numérique et délinquance financière.

Sommes-nous tous concernés par la cybercriminalité ?

Même dans les territoires reculés, la cybercriminalité est omniprésente. À partir du moment où il y a des sociétés et des personnes connectées, vous pouvez être confrontés à une faille de sécurité et, de fait, à un phénomène cybercriminel. Dans le cyberespace, il n'y a pas de règles de territorialité, nous sommes tous égaux face aux menaces. Enormément de nos grosses affaires de cyber escroqueries ont pris naissance dans les campagnes de l'Aveyron, de l'Ariège, du Gers et du Lot. Les plus grosses attaques n'arrivent pas forcément dans les grands centres.

De quel type sont ces attaques ?

Je peux vous donner l'exemple de deux enquêtes dont la portée fut internationale et qui sont parties pour la première du Lot, et a conduit à 22 arrestations sur le territoire pour des fraudes à la carte bancaire, avec ouverture d'une enquête internationale; et pour la seconde de l'Ariège, pour un exercice illégal de la profession de banquier à l'aide de crypto-monnaies (bitcoin). Par ailleurs, une des plus impressionnantes attaques de société que j'ai eue à traiter avait concerné une entreprise gersoise, avec arrêt des machines-outils pendant tout un week-end.

Ces attaques sont nombreuses ?

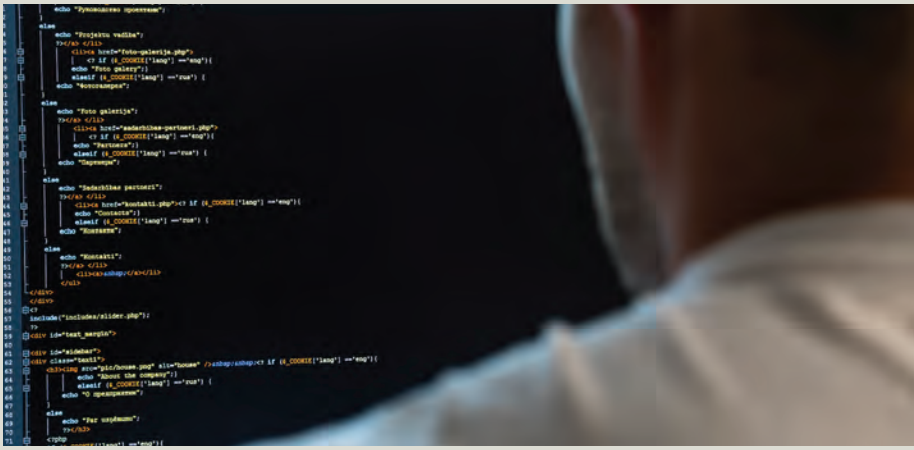
Elles sont en progression constante depuis 15 ans. La cybercriminalité est l'une des formes de criminalité qui connaît actuellement la plus forte croissance. Les malfaiteurs exploitent la rapidité du réseau, les fonctionnalités des technologies modernes et l'anonymat qui leur permettent de commettre les infractions les plus diverses. Pour les escroqueries par faux ordre de virement international (FOVI) par exemple, qui totalisent 30 M€ de préjudice au niveau national en 2013-2014 (contre 3,9 M€ en 2012-2013), seulement sur des faits avérés, cinq affaires ont eu lieu dans un petit département comme le Gers en 2013-2014 alors que nous n'en avions recensé aucune sur la période précédente. Deux escroqueries sont arrivées à leur terme, les auteurs ont pu ainsi s'emparer de 340 000 € au préjudice des sociétés visées.

Que traquez-vous le plus ?

Il y a deux ans, 80 % de notre activité était concentrée sur les défaçages de sites, en réaction à la campagne de communication menée contre Charlie Hebdo ; nous avons ensuite été confrontés à une vague de cryptolockers ; et en mars, nous avons retrouvé l'implantation de nombreux shellcode.

De quoi s'agit-il ?

Le défaçage consiste à remplacer la page de garde d'un site internet par une autre pour faire passer un message de propagande. Nous



MAJOR FABRICE CRASNIER

Commandant de la division analyse criminelle et investigations spécialisées de la section d'appui judiciaire de la région de gendarmerie Midi-Pyrénées,

Pilote du relais de la réserve Citoyenne Cyberaérodéfense (R.C.C.) de la région Languedoc Roussillon Midi-Pyrénées.

avions recensé à l'époque une vingtaine de cas en région, rien que sur des sites de collectivités. Ces dernières ont l'obligation de communiquer à ce sujet, alors que souvent les entreprises victimes n'osent pas le dire et appliquent simplement un correctif en interne. Or, cette politique de l'autruche détruit la preuve matérielle dont nous avons besoin pour poursuivre notre enquête alors que celle-ci revêt un caractère essentiel lors de la présentation du dossier aux magistrats du parquet. Il est nécessaire également de rappeler que la suite donnée à la procédure sera conditionnée à la présentation de cet élément de peuve.

Concernant le cryptolocker, l'escroquerie est lancée par mail avec une pièce jointe compromise. Le destinataire malheureux du courriel cherchant à ouvrir le fichier joint active ainsi le cryptolocker qui a pour mission de crypter l'ensemble des fichiers de la machine du destinataire . Le déverrouillage est ensuite proposé contre une somme d'argent. Il y en a beaucoup car un outil de cryptolockage a été mis en vente sur des black market (marché noir) du darknet (NDLR : un web profond). Partout en Franc ement pas l'ensemble du spectre infractionnel du cyberespace prévu dans la loi française.

Concernant ce dernier point justement, vous disposez d'un nouvel outil : la cyberinfiltration ?

La pédophile est en effet toujours présente. Le cyberespace français avait été « nettoyé » mais les cyberpédophiles utilisent désormais des serveurs étrangers ou passent par des anonymiseurs. Nous avons été formés à la cyberinfiltration. Elle concerne la pédophilie, mais aussi le terrorisme, les faux médicaments et le trafic de stupéfiant. Une loi est intervenue en octobre 2015 ainsi qu'un arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme. A compter de cette date nous avons mené plusieurs actes qui ont conduit à l'arrestation de plusieurs toulousains qui ont été conduits devant le tribunal correctionnel pour des faits de corruption de mineur, propositions sexuelles à mineur de 15 ans avec et sans rencontre (art. 227-22 et 227-22-1 CP), de pédopornographie par production pour diffusion, mise à disposition, importation, exportation, diffusion, détention, consultation habituelle (art. 227-23 CP).

Quid des objets connectés ?

C'est le nouveau marché des cyberdélinquants, sachant qu'à horizon 2020 il y en aura dix milliards sur la planète. Détournés de leur emploi, ils peuvent devenir un vecteur de compromission encore plus menaçant car ils vont se nicher au cœur de nos foyers, collecter encore plus d'information, et agir en toute transparence. Qui se méfierait de son réfrigérateur ? Personne. Ils vont également requérir un haut niveau de technicité pour comprendre leur comportement déviant. Un microcontrôleur allie par exemple l'électronique et l'informatique, et contient tous les outils pour contourner des règles de sécurité. Il n'existe pas encore d'arsenal de détection contre cela. La législation évolue et essaie de s'adapter mais les cybercriminels avancent vite, ils ont toujours un train d'avance car la technologie est en perpétuelle évolution. L'objectif est de les suivre de près, tant dans la technologie que dans la réponse pénale, c'est l'histoire du gendarme et du voleur dans le cyberespace.

Avec la courtoisie de la Gazette du Midi

RENCONTRE

LA CONFIANCE : LE MOTEUR DU PIRATAGE !

Philippe Truillet
Maître de conférences à l'Université Toulouse III Paul-Sabatier, passionné des questions de cybersécurité, chercheur et informaticien de l'Irit (Institut de Recherche en Informatique de Toulouse), officier de la réserve opérationnelle de la Gendarmerie nationale.

Philippe Truillet a beau sourire, le constat qu'il livre sur les réseaux informatiques a de quoi glacer le sang :

> *« On n'est en sécurité nulle part! Aujourd'hui, quand on consulte internet, l'important est d'obtenir le service que l'on recherche, comme accéder à ses mails ou à ses comptes bancaires, mais vous ne voyez jamais par où transitent vos informations, et de quelle manière : autant dire que vous ne pouvez pas savoir si vos transferts de données sont bien sécurisés ! »*

Pour prouver ses dires, l'enseignant-chercheur du Laboratoire de recherche en informatique de Toulouse (IRIT, au sein de l'université Toulouse III Paul-Sabatier, a réalisé il y a 2 ans une petite expérience sur la confiance que nous accordons aux réseaux publics.

En installant une fausse borne wi-fi au sein de l'université Toulouse I Capitole, qui fonctionnait comme un routeur, il a pu ainsi récupérer les mots de passe des étudiants qui s'y étaient connectés !

Comment ? La réponse ne tarde pas : Philippe Truillet allume son ordinateur et lance un simple logiciel, baptisé *Wireshark*. En quelques secondes, cet outil d'analyse des protocoles des réseaux affiche toutes les connexions informatiques qui transitent par le routeur du laboratoire, révélant, en temps réel, quelles sont les machines connectées, les adresses internet et les fichiers qu'elles consultent, et même les identifiants et les mots de passe qui ont été enregistrés !

> *« Wireshark est un outil gratuit, facile à trouver et à utiliser quand on s'y connaît un peu, mais de manière générale, il n'y a pas besoin d'être informaticien pour faire tomber un système ou récupérer des informations »*, souligne Philippe Truillet.

Alors, comment se protéger ?

> *« Il faut utiliser des protocoles sécurisés, symbolisés par le "s" : https, ftps, SSH… Ils permettent de crypter les communications entre celui qui demande un accès et celui qui le donne, dont les logins qui sinon seraient en clair.*
>
> *Mais bien sûr le système n'est pas parfait, les attaques sont toujours possibles ! »*

Pour ne rien arranger,

> *« rien ne dit que la personne ou la machine avec laquelle je communique soient sécurisées ! Car elle héberge peut-être des virus qui récupèrent l'information directement chez elle… »*

PHILIPPE TRUILLET

Auditeur de la 191ème SR de l'IHEDN (Institut des hautes études de défense nationale), Philippe Truillet enseigne au sein du Master 2 ISSD

IRIT
CNRS - INPT - UPS - UT1 - UT2J

LIMITER LA DIFFUSION DES INFORMATIONS SUR INTERNET

Autre risque auquel s'exposent les entreprises, celui qui consiste à

> *« proposer des services ou des documents sur internet au prétexte que leur accès est restreint et bien protégé. Mais la confiance, c'est le moteur du piratage !*
>
> *Il y a clairement des informations qui n'ont rien à faire sur internet; et même si on ne connaît pas l'adresse URL qui amène à ces documents, les moteurs de recherche feront très bien ce travail à votre place. »*

Ne reste plus qu'à s'introduire par effraction, ce qui, du fait de la profusion de logiciels de piratage sur internet, ne présente plus une grande difficulté, même pour des hackers amateurs. Un autre bon moyen de récupérer des codes informatiques est de créer une copie du site informatique visé, et d'y amener les usagers qui, en toute bonne foi, vont enregistrer leurs logins et mots de passe.

Aussi Philippe Truillet défend-il l'idée qu'une entreprise, au lieu de proposer des informations à partir d'un site internet,

> *« devrait plutôt permettre à l'utilisateur de rentrer dans le système informatique interne de l'entreprise, à condition qu'il soit protégé, de part et d'autre, par un réseau privé virtuel (virtual private network, VPN) ».*

Un système qui, chez l'utilisateur et son destinataire, crypte toutes les informations entrantes et sortantes, rendant presque impossible toute interception.

LE BON SENS COMME RÈGLE DE SÉCURITÉ

> *« En fait, pour éviter la plupart des risques informatiques, il suffit parfois juste d'un peu de bon sens, et se demander : est-ce que je livrerais sans contrôle ces mêmes informations dans la vie réelle ? »*, souligne Philippe Truillet.

Ce qui suppose, par exemple, de se méfier des réseaux publics gratuits, comme on en trouve dans les fast-foods et certains espaces publics.

Attention également aux objets électroniques, comme les clés USB, les tablettes et les smartphones que l'on utilise désormais sans discernement, par simple commodité : encore en vogue récemment dans les entreprises, la mode du bring your own device (*BYOD*, « amenez vos propres outils ») qui poussait les employés à utiliser leurs propres objets communicants se voit de plus en plus encadrée,

> *« car cela pose la question de la limite entre information publique et privée et de leur sécurisation ».*

Même un outil apparemment aussi innocent qu'une souris informatique peut représenter un risque de sécurité ! En témoigne une société américaine qui s'était vantée d'être parfaitement impénétrable. Son sous-traitant en sécurité informatique, Netragard, l'a pris au mot : mais au lieu de l'attaquer par le réseau, comme l'aurait fait n'importe quel hacker, les faux pirates choisirent d'envoyer de faux cadeaux promotionnels aux employés de l'entreprise-cible, en l'occurrence des souris de la marque Logitech. Caché à l'intérieur, se trouvait un microcontrôleur relié à une mémoire flash qui, au bout d'une minute d'inactivité de la souris, déclencha l'envoi d'un logiciel malveillant qui permit de prendre le contrôle de l'ordinateur !

Moralité - Ne jamais faire trop confiance : même les meilleurs s'y feront prendre un jour !

RECHERCHE

3 ANS DE MEMOIRES - 2013-2016

- Sauvetage en mer : dispositifs des postes de secours et condition physique
- Protection Rapprochée aux Nations Unies : développer un concept adapté aux nouvelles menaces.
- Préparation physique et sportive au sein du GIGN : Vecteur essentiel dans la réussite leur mission
- Adaptation au stress et préparation mentale des policiers américains versus lutte du suicide de ces fonctionnaires
- Ingénierie de formation en milieu hostile
- Sécurité au travail
- La reconversion des militaires en particulier à la Légion Etrangère
- La création d'une formation pour une préparation technique et tactique en zone dangereuse
- Cyberprotection : sécurisation des flux des moyens de chiffrement dans le monde industriel de la Défense
- Stagiaires volontaires ou désignés: stratégie de l'ingénierie de formation pour adultes
- Sécurité sûreté
- Le "Chiffre" dans la Cyberdéfense, l'importance de sa prise en compte.
- La prévention des risques professionnels en lien avec l'activité des opérateurs lutte antivectorielle dans les armées
- Ingénierie de formation des relais de sûreté dans les différents établissements de la SNCF
- La simulation opérationnelle comme aide à la formation des futurs officiers
- Enquête de l'insécurité au sein d'un établissement scolaire
- Formations spécifiques des équipiers du Centre Parachutiste d'Instruction Spécialisée CPIS
- Préparation physique des intervenants en milieu hostile
- Formation des intervenants en milieu sécurité sûreté défense
- La formation dans l'armée française : le problème de l'adaptation aux conflits actuels et à l'évolution de la menace
- Ingénierie de formation des officiers de la Gendarmerie
- Application des mesures VIGIPIRATES dans les différents établissements de la SNCF
- Simplification de la gestion des droits d'accès
- Etude des carrières des consultants en sécurité
- Mise en condition physique opérationnelle
- Plan d'Organisation des Secours : refonte d'un plan d'urgence
- Création et mise en place des fiches réflexes pour les officiers de permanence et pour la cellule de crise
- Création du dossier sécurité de la station ski TVGD
- Traitement des infractions pénales commises dans le Cyber espace par les Gendarmes Départementaux non spécialisés.
- L 'armement et l'industrie de l'armement espagnol : quelle place dans la défense nationale et internationale ?
- Sport de combat et formation

- ✖ • L'application du tir réglementaire militaire à la pratique du tir sportif norme FFT présente-t-elle un intérêt ?
- • La prévention et le développement de la culture du risque auprès de la population
- ✖ • Les ESSD instrument au service des entreprises (Airbus)
- 🔒 • Intelligence et sécurité économique en industrie spatiale - Analyse d'une organisation de travail dans les activités de veille stratégique et d'analyse de marché
- • Gestion des crises et procédures d'intervention : place de l'entrainement virtuel dans la formation, le maintien et le perfectionnement des acquis
- 🔒 • Gestion de crises / Une documentation sécurisée sans délai
- 🔒 • La Sûreté dans une grande entreprise
- • La mise en place de dispositifs de formations internes au sein d'un centre de secours.
- ✖ • Cyber Sécurité - Intégration d'une solution Cyber Sécurtité dans les TPE et PME
- 🔒 • Les forces publiques et les nouvelles menaces
- 🔒 • Enjeux de la gestion de crise au sein d'une ETI. Comment appréhender l'intégration du processus de getion de crise au sein d'une ETI ?
- ✖ • La police municipale est-elle capable de répondre, en terme de sûreté, aux attentes et enjeux actuels de notre société
- • Les interférences/oppositions entre les règlementations de sûreté et de sécurité au travail
- ✖ • L'intégration du chiffre dans la cybersécurité et étude de sa vulnérabilité.
- • L'évaluation en formation, approches, pratiques et outils
- • Ingénierie d'une Certification de Spécialisation Entraînement et Encadrement des Sportifs Blessés de la Défense
- ✖ • Quelle est la place de l'ingénierie de formation dans la préparation d'un DLAO (détachement de liaison et d'appui opérationnel) en vu de sa certification et de sa projection ?
- 🔒 • Quelle réponse la Force Formation du GIGN peut apporter aux demandes des unités d'intervention étrangères qui sont confrontées aux évolutions du terrorisme
- • Radicalisation dans le monde associatif
- • L'action de la Gendarmerie en matière de sûreté du transport aérien.
- 🔒 • Sûreté et entreprises à l'étranger
- • Etude d'un marché dans l'environnement de l'intelligence économique et développement d'une offre de service : audit, conseils et formation sur la sécurité des systèmes d'information à destination des PME/PMI.
- ✖ • L'interopérabilité entre la SNCF et les services de l'État dans l'organisation et la gestion de la sécurité de l'Euro 2016 face à la menace terroriste
- 🔒 • Comment une entreprise de transport de voyageurs lutte face au terrorisme ?
- • Rédaction des procédures du bureau planification et formation aux agents prévisionnistes et officiers adjoints au CTA
- • Le Sauvetage Aquatique sur le Bassin d'Arcachon
- 🔒 • Risques psychosociaux inhérents aux nouvelles techniques de management (santé/sécurité)
- 🔒 • Organisation des connaissances et des compétences en matière de sûreté protection
- 🔒 • Nageurs de combats. Comment diminuer de taux d'attrition.
- • Etat des lieux du sauvetage aquatique en France et à l'étranger
- • Formation des officiers de gendarmerie
- 🔒 • Le maintien de la condition physique en OPEX
- 🔒 • Assistance Militaire Opérationnelle
- • Les entorses de chevilles chez les sapeurs-pompiers : analyse, prévention et suivi des agents par la filière EPS
- 🔒 • Optimisation de la formation opérationnelle des journalistes reporters de guerre
- • Ingénierie des formations pour l'efficience et le confort des forces de l'ordre en opération.Plus particulièrement en situations de tir par la gestion du stress opérationnel.
- • La mise à niveau de la Sécurité des Systèmes d'Informations

CLASSEMENT

🔒 Confidentiel

✖ Diffusion Restreinte

contre MESURES

Publication
Sandra Joffroy

UNIVERSITÉ TOULOUSE III PAUL SABATIER

Rédaction
Serban Iclanzan

iclanzan & ASSOCIÉS

Création & réalisation
Elisabeth Dupont

ADN advanced data network

Impression
GROUPE reprint parchemins du midi

PARTENARIAT

PARTENAIRES SOUS CONVENTION

Région de Gendarmerie Midi-Pyrénées

Groupe d'Intervention de la Gendarmerie

Ecole Nationale Supérieure d'Application de la Police

Ecole Nationale d'Administration Pénitentiaire

Centre d'Instruction en Sécurité Industrielle de l'Armement

Association régionale AR19 de l'IHEDN

Délégation Générale de l'Armement

11ème Brigade Parachutiste

LABORATOIRES DE RECHERCHE

Institut de Recherche en Informatique de Toulouse

Laboratoire Education Formation Travail Savoirs de l"Université Toulouse II – Jean-Jaurès

SOUTIENS PEDAGOGIQUES

Ecole Nationale de l'Aviation Civile

Ecole Nationale Supérieure des Officiers Sapeurs-Pompiers

ILS NOUS FONT CONFIANCE

MASTER 2
INGENIERIE SURETE SECURITE DEFENSE

MELIORA PARAMUS

RESPONSABLE DU MASTER

Sandra Joffroy
Tél : 05.61.55.88.89
Mail : sandra.joffroy@univ-tlse3.fr

SECRETARIAT PEDAGOGIQUE

(scolarité, emploi du temps, relevé de notes et diplôme)

Myriam CLERMONT
Tél : 05.61.55.88.89
Mail caminade@adm.ups-tlse.fr
Fax : 05.61.55.82.17
Web: http://www.f2smhstaps.ups-tlse.fr/

Université Paul Sabatier
Faculté des Sciences du Sport et du Mouvement Humain
Secrétariat du Master 2 ISSD
118 route de Narbonne
31062 TOULOUSE Cedex 9

SECRETARIAT ADMINISTRATIF

(inscription Formation Continue et Contrat de Professionnalisation)

Formation Continue

Marie-Pierre PINQUIE
Tél : 05.61.55.87.13
Mail : marie-pierre.pinquie@univ-tlse3.fr
Fax : 05.61.55.87.01

Contrat de Professionnalisation

Bachir ATROUS
Tél : 07.63.03.93.38
Mail : bachir.atrous@univ-tlse3.fr
Fax : 05.61.55.87.01

Mission Formation Continue et Apprentissage de l'Université Paul Sabatier
1, rue Latécoère
31062 TOULOUSE Cedex9

MELIORA PARAMUS

Master 2 MS

Ingénierie Sûreté Sécurité Défense

Université Toulouse III - Paul Sabatier

Secrétariat du Master 2 ISSD
118 route de Narbonne
31062 TOULOUSE Cedex 9

Myriam CLERMONT
Tél : 05.61.55.88.89
Mail : caminade@adm.ups-tlse.fr