Lettre des "Lundi de la cybersécurité n° 61

La Lutte Informatique d'Influence
L2I

La Lutte Informatique d'Influence

En octobre 2021, Florence Parly alors ministre des Armées, à l'occasion de l'actualisation stratégique de la Loi de Programmation Militaire (LPM) 2019-2025, présentait la doctrine militaire de la **L2I** (Lutte Informatique d'Influence). En mars 2023, à l'occasion de l'assemblée générale de l'ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information - dans l'amphithéâtre De Bourcet de l'École militaire, Paris, le général de brigade aérienne Thierry BAUER adjoint au commandant de la cyberdéfense, invité d'honneur de notre AG, clôturait cet évènement par une présentation du **COMCYBER**.

Le COMCYBER est l'entité de l'Armée française dont la mission est le commandement du cyberespace. Les crédits accordés au cyber, dans la loi de programmation militaire (LPM) pour les années 2024 à 2030 ont été multipliés par trois avec un investissement qui s'articule autour de quatre axes : le chiffre, la lutte informatique défensive (LID), la lutte informatique offensive (LIO) et la lutte informatique d'influence (L2I).

- **Le chiffre**, c'est bien sûr l'essence même et l'ADN des passionnés de l'ARCSI. Les systèmes d'information sont devenus très complexes. Ceux qui ne nous veulent pas que du bien, soit sur le plan de notre souveraineté, soit sur celui de notre économie ou de notre manière de vivre, sont devenus très agressifs et très inventifs. La cryptologie reste notre protection ultime dans l'espace numérique. C'est elle qui peut nous garantir une vraie souveraineté.
- **La LID** ou lutte informatique défensive, c'est la détection des cyber-attaques au plus tôt et une intervention rapide pour les caractériser et les contrer. Ce fut le sujet du Lundi de la cybersécurité de juin où Ivan Fontarensky, directeur technique de l'offre CTI – Cyber Trends Intelligence de Thalès nous a présenté ce que l'on sait, côté cyberattaques sur le déroulement du conflit russo-ukrainien.
- **La LIO** ou lutte informatique offensive, vous comprendrez que comme elle touche à des aspects « *très secrets* » nous n'en dirons pas plus ici, le général n'a pas abordé ce sujet.
- **La L2I** ou lutte informatique d'influence. j'ai pensé : « la L2I, quel beau sujet pour animer un Lundi de la cybersécurité ! ». Alors à la fin de l'intervention du général Bauer, je lui ai proposé d'animer un de nos Lundi de la cybersécurité sur le thème de la Lutte Informatique d'Influence. Il a été d'accord. Nous étions en mars et le premier Lundi encore libre, c'était celui de septembre, après la pause de juillet / août. Ce sera donc le lundi 11 septembre, 18h-20h. Remarquons que le 11 septembre 2001, le « nine eleven 9/11 » c'était aussi un lundi.

> *La lutte informatique d'influence désigne l'ensemble des opérations militaires conduites dans la couche informationnelle du cyberespace, pour détecter, caractériser et contrer les attaques, appuyer la communication stratégique, renseigner ou conduire une manœuvre de déception, de façon autonome ou en combinaison avec d'autres opérations.*

La lutte informatique d'influence, ce sont des opérations militaires sous le contrôle de l'officier général commandant de la cyberdéfense (COMCYBER).

L'Information, et en particulier celle véhiculée par les réseaux sociaux et autres sites web, est devenue une arme de guerre par destination. Les fake news (information erronée ou infox), les manipulations de l'Information, élaborées par des organisations mal intentionnées dans le but de nuire à nos armées ou à notre économie, influencent

l'opinion, qu'elles soient vérifiées ou pas. La déstabilisation des institutions par la manipulation des opinions, nous imposent leur perception de la réalité. Limiter la propagation de fausses informations à des fins hostiles, par des outils de veille est devenue un impératif.

Voici un exemple de fausse information parue sur Facebook, et dirigée contre l'opération Barkhane que la France a menée au Sahel : *« Les militaires français pillent les ressources* aurifères *du Mali* ». Il a été aussi question, en avril 2022, *de charniers* où l'armée française a été impliquée, mais des images-preuve filmées discrètement par nos drones ont révélé l'enterrement à la hâte de cadavres à proximité de la base de GOSSI, récemment rendue par la Force Barkhane. C'était la preuve que le coupable de ces massacres n'était pas l'armée française, nous n'y étions plus.

Ils sont forts les Russes et en particulier leur milice Wagner dans la désinformation !

Il parait même dans les Deep Fakes (hyper trucages) que nous soutenons des groupes terroristes d'Afrique de l'Ouest, alors qu'en vérité nous les combattons.

Ce n'est pas notre genre, et la France respecte la charte des Nations Unis et les règles du droit international humanitaire. Ces Informations sont fausses mais que pense l'opinion qui est émotionnellement réceptive ? Il est urgent de démentir car la couche sémantique » du cyberespace s'apparente de plus en plus à un champ de bataille.

Dans le cadre de la LPM 2024-2030, la L2I devrait *passer de l'artisanat à l'industrialisation* avec doublement de ses effectifs actuels à l'horizon 2030.

Le général de brigade aérienne Thierry BAUER étant appelé à d'autres fonctions, son remplaçant au COMCYBER, **le Contre-Amiral Vincent SEBASTIEN** animera notre Lundi de la cybersécurité du 11 septembre.

Je donne la plume au Contre-Amiral Vincent SEBASTIEN

La guerre de l'information n'est pas nouvelle. Elle est partie intégrante de toute stratégie militaire : sans capacité à convaincre et à contrer l'influence adverse, tout engagement militaire est voué à l'échec.

La compétition entre grandes puissances stratégiques ou l'émergence de puissances régionales a considérablement renforcé cette conflictualité informationnelle qui s'exprime au-delà des traditionnelles notions de temps de paix, de crise ou de guerre. Le Cyberespace, nouveau milieu en croissance exponentielle, offre de plus un terrain d'expression, via en particulier les réseaux sociaux, qui accélère la circulation d'informations vraies ou fausses et en renforce considérablement la portée et la résonnance.

Les attaques informationnelles visent depuis quelques années déjà nos armées sur leurs théâtres d'opération. Elles peuvent être lourdes de conséquences en contribuant par exemple à soulever l'hostilité des populations, la méfiance des autorités locales voire occasionner une altération durable de légitimité à l'échelle internationale.

La volonté d'obtenir la supériorité opérationnelle dans le champ informationnel s'est traduite par la structuration et la montée en puissance, sous les ordres du COMCYBER de la Lutte Informatique d'Influence (L2I) accompagnées par la publication d'une doctrine dédiée en 2021. Plus récemment, la Revue Nationale Stratégique 2022 consacre la création d'une nouvelle fonction stratégique *Influence* visant à promouvoir et à défendre les intérêts et les valeurs de la France. Cette dimension nouvelle accordée à l'influence prend acte de l'accélération et du durcissement de la compétition menant à un phénomène de guerre hybride mondialisée.

Les opérations de Lutte Informatique d'Influence conduites par le COMCYBER avec des unités spécialisées s'inscrivent dans ce cadre stratégique, en parfaite intégration avec les actions interarmées menées dans les autres milieux et champs. Elles respectent le cadre juridique international comme français.

Domaine jeune, la L2I connait une montée en puissance rapide que la récente LPM 2024/2030 appuie. Les défis sont nombreux. Le premier est celui des ressources humaines qui doivent disposer de compétences étoffées et extrêmement variées, le deuxième est celui des outils dédiés qui doivent bénéficier des dernières innovations technologiques (traitement Big Data, IA notamment) et enfin celui des partenariats nationaux comme internationaux qui représentent un levier majeur d'efficacité opérationnelle.

Je reprends la plume

Qui est le contre-amiral Vincent Sébastien ?

Le contre-amiral Vincent Sébastien a pris en août 2023 ses nouvelles fonctions en tant qu'Adjoint au commandant de la cyberdéfense (le COMCYBER). Il a commandé plusieurs navires de la Marine Nationale dont le Porte-Hélicoptères Amphibie « Mistral ». Il est spécialisé dans le domaine numérique et Cyber.

Il a notamment été Chef du bureau Numérique et Systèmes d'Information et de Communication de l'état-major de la Marine, puis Chef d'Etat Major du COMCYBER avant de rejoindre son poste actuel.

Demande d'inscription pour le Lundi de la cybersécurité du mois de septembre

Lundi 11 septembre à partir de 18 h 00, en présentiel à l'université Paris Cité, 45 rue des Saints-Pères Paris 6e, si le nombre des inscrits en présentiel le justifie, et toujours en parallèle en ligne par visio-conférence Zoom.

Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, les coordonnées de l'amphi de l'université Paris Cité, si vous avez demandé le présentiel, ou un hyperlien personnel vers la visioconférence.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Dans votre message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements. **Et bien entendu, précisez si vous choisissez le présentiel ou le distanciel.**

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants.

Si vous souhaitez ne plus recevoir les lettres des « Lundi de la cybersécurité » mensuels, une simple demande par mail suffit. Si vous voulez être ajouté à la liste de distribution, demandez-le nous.

Quelques minutes avec l’Agence Nationale des Fréquences (ANFR)

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une dizaine de minutes la parole à une organisation, qui opère dans l 'écosystème du numérique et dans la sécurité de l'information.

Catherine Gabay **est Directrice Adjointe du Contrôle du Spectre à l’Agence Nationale des Fréquences (ANFR).**

A ce titre, Catherine Gabay participe à la définition et au suivi de la stratégie de l'ANFR pour protéger le spectre des radiofréquences face à l'évolution du nombre, de la complexité et de la criticité des cas de brouillage.

Dans le cadre de sa mission de Contrôle du Spectre, l’ANFR participe à la sécurité numérique et à la cybersécurité en luttant contre les brouillages qui peuvent engendrer le déni de service de tous types d’applications utilisant des connexions hertziennes pour transmettre et recevoir des informations.

.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements sur le web de l'ARCSI, en **https://www.arcsi.fr/.** pour les plus récents. Les événements plus anciens sont en **https://www.arcsi.fr/evt_passes.php.** Les enregistrements des organisations qui sont intervenues durant les « quelques minutes » se trouvent en première page du site de l'ARCSI, là où sont les logos des organisations qui sont déjà intervenues dans nos « Lundi de la cybersécurité ». Cliquez sur un logo, vous obtenez l'enregistrement.

Nous remercions Francis Bruckmann, webmestre et membre du Conseil

d'Administration de l'ARCSI pour son travail qui constitue la mémoire de nos événements.

Le coin coin de l'IA générative

Question posée au module d'Intelligence Artificielle générative inclus dans le moteur de recherche Bing, et sans livrer, bien sûr, de données confidentielles qui pourraient être exploitées :

La lutte informatique d'influence est-elle légale ?

Réponse reçue :

La lutte informatique d’influence (L2I) est une stratégie militaire qui consiste à mener des opérations dans le cyberespace pour influencer l’information. Elle n’est pas légale en soi, mais elle dépend du cadre juridique et éthique de chaque pays et de la nature des opérations.

Gérard

:

Lundi de la cybersécurité d’octobre

lundi 16 octobre 18h-20h

Solange Ghernaouti

Professeure à l’Université de Lausanne

Cybersécurité et enjeux environnementaux