DOSSIER D'INFORMATION

# LA DGA ET L'AID ACCOMPAGNENT LES PROJETS CYBER INNOVANTS


## Forum International de la Cybersécurité (FIC)

28, 29 et 30 janvier 2020

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

# DIRECTION GÉNÉRALE DE L'ARMEMENT (DGA)

**Force d'expertise, d'essais et d'ingénierie au sein du ministère des Armées, la Direction générale de l'armement (DGA) a pour missions d'équiper les armées de façon souveraine, de préparer le futur des systèmes de défense, de promouvoir la coopération européenne et de soutenir les exportations.**

Pour accompagner la montée en puissance de la cyberdéfense érigée en priorité nationale dans la Loi de Programmation Militaire, la Direction générale de l'armement (DGA) se fixe deux priorités : maintenir un haut niveau d'expertise étatique et garantir une Base industrielle et technologique de défense (BITD) dotée des compétences clé en matière de cybersécurité. Pour réussir, la DGA, en lien avec l'Agence de l'innovation de défense (AID), a mis en place une stratégie basée sur l'innovation et le renforcement de synergies avec les acteurs industriels et académiques. Couveuse d'entreprise, espace de travail collaboratif ouvert aux start-up, PME et chercheurs, dispositifs contractuels plus souples… la DGA muscle son dispositif « cyber » pour maintenir les armées à la pointe de la cybersécurité et gagner la bataille du numérique. La DGA s'appuie pour cela sur le savoir-faire du centre d'expertise DGA Maîtrise de l'information qui dispose de compétences uniques en Europe, ainsi que sur la cyberdéfense factory basée à Rennes, relai local de l'Agence de l'innovation de défense.

## DGA MAÎTRISE DE L'INFORMATION, CENTRE D'EXPERTISE ET D'ESSAIS UNIQUE EN EUROPE

La DGA est l'expert technique référent du ministère des Armées en matière de cybersécurité. De l'anticipation de la menace à la mise en œuvre de cybersolutions pour les armées et les hautes autorités de l'État, elle assure, depuis la conception d'algorithmes cryptographiques jusqu'aux architectures sécurisées de systèmes d'armements complets ;

- Le développement et l'évaluation de produits de cybersécurité ;
- La prise en compte de la cybersécurité dans tous les programmes d'armement ;
- Le développement des capacités de lutte informatique offensive au profit des armées. En raison de la sensibilité et de la dynamique du domaine, les équipes du COMYBER et les équipes cyber de la DGA travaillent en étroite coopération à l'élaboration et à la mise en œuvre d'une feuille de route capacitaire ;
- L'animation de la R&T (recherche et technologie) cyber en lien avec les autres entités étatiques, l'industrie et le monde de la recherche.

Pour disposer d'une capacité d'expertise à la hauteur des enjeux majeurs portés par la cyberdéfense, la DGA poursuit le recrutement sur le site de DGA Maîtrise de l'information d'ingénieurs de haut niveau, spécialisés dans l'analyse et la prévention des attaques informatiques. 100 nouveaux experts en cybersécurité rejoindront la DGA en 2020 pour atteindre un effectif de 900 en 2025.

Le centre d'expertise et d'essais, implanté à Bruz (35) compte 1450 agents, dont 80% d'ingénieurs.

SUIVEZ-NOUS SUR :

www.defense.gouv.fr/dga
www.ixarm.com

**DIRECTION GÉNÉRALE DE L'ARMEMENT**
60 boulevard du général Martial Valin
CS 21623 - 75 509 Paris Cedex 15 - France

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

**Rendez-vous sur le stand du ministère !**

Venez découvrir des innovations développées par des PME/TPE et start up avec le soutien la DGA et de l'Agence de l'innovation de défense

# LA DGA ET L'AID ACCOMPAGNENT LES PROJETS CYBER INNOVANTS

Pour assurer la supériorité technologique et opérationnelle des armées, innover est une nécessité. Une nécessité renforcée par l'arrivée de technologies de rupture, comme l'intelligence artificielle. Dans ce contexte, la Direction générale de l'armement (DGA) et l'Agence de l'innovation de défense poursuivent leur stratégie d'ouverture et de captation rapide des technologies du civil. Objectif : maintenir une dynamique d'innovation pour mieux anticiper l'évolution de la menace cyber et faire face aux défis futurs.

Pour capter au plus vite le meilleur des technologies civiles et accélérer leur développement, le ministère des Armées dispose de solutions d'accompagnement adaptées au niveau de maturité de l'innovation et à la nature du porteur de projet.

***Découvrez à titre d'exemple les projets innovants présentés sur le stand.***

# LA DGA PRÉSENTE LA START UP GLIMPS ET SON INNOVATION UNIQUE EN EUROPE

La start-up rennaise GLIMPS présente sur le stand du ministère des Armées, une innovation unique en Europe, capable de détecter une cyberattaque en un temps record. Fondée par quatre anciens ingénieurs de la DGA, la jeune pousse est aussi la première société à rejoindre la cyberdéfense Factory, un plateau collaboratif créé par la DGA en octobre dernier pour capter le meilleur de l'innovation civile.

**Les attaques cyber se multiplient et menacent les usagers comme les entreprises, y compris les plus puissantes au monde. Pour cyberprotéger les systèmes d'information de cette menace galopante, l'un des défis porte sur la rapidité de détection des intrusions. Une opération de plus en plus délicate pour des systèmes embarquant un nombre gigantesque de données. C'est dans ce contexte que la start up GLIMPS développe un outil de détection automatique de virus.**

Aujourd'hui, détecter une vulnérabilité sur un système d'information (logiciel, radio, système de surveillance,… ) est très complexe car tout système, quel qu'il soit, embarque un nombre d'informations gigantesque : il se compose de milliers voire de millions de lignes de codes. La détection de virus nécessite de pouvoir identifier tous les codes du système. Il s'agit d'une opération fastidieuse, réalisée le plus souvent de manière manuelle et qui peut prendre des semaines voire des mois de travail très répétitif et peu enrichissant.

Avec l'innovation développée par la start-up GLIMPS, s'appuyant sur les technologies d'intelligence articifielle, il est possible de détecter, caractériser et analyser les nouvelles menaces de manière quasi instantané. La solution permet même de documenter tout le code connu, qu'il s'agisse de code open source (bibliothèques statiques) ou de code propriétaire public (runtime d'environnement tel que Delphi ou MSVC, firmware d'OS embarqué...).

Comment ca fonctionne ? L'outil d'analyse de malware s'appuie sur une technologie de détection de code, indépendante des options de compilation, de la chaîne de compilation utilisée et même de l'architecture (x86, ARM, PPC, MIPS…).

La technologie de la start-up rennaise est ainsi capable d'identifier le code des briques logicielles sous de multiples formes, permettant de détecter une menace qui cible spécifiquement une entreprise même si le virus a été modifié pour échapper aux technologies de détection par signature.

Grâce à l'intelligence artificielle, la technologie offre la possibilité de traiter des bases de plusieurs centaines de Téraoctet de malwares instantanément.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

DGA

# DÉFI CYBER « DECEPTIVE SECURITY » : PRÉSENTATION DES DEUX PROJETS FINALISTES ET ANNONCE DU VAINQUEUR PENDANT LE SALON

**Organisé par la DGA en relation avec le COMCYBER et l'Agence de l'innovation de défense, le Défi cyber, baptisé « Deceptive Security » lancé en juin 2019 vise à faire émerger une solution innovante, expérimentable par les forces armées, permettant de faciliter l'analyse des cyberattaques visant les réseaux du ministère des Armées. Dans un marché dominé par de grands acteurs internationaux, la DGA a fait le choix de challenger des startup et PME/ETI française.**

Les finalistes de ce challenge sont les PME AMOSSYS et SESAME IT. Leurs projets sont à découvrir sur le stand du ministère. Le vainqueur sera annoncé pendant le salon et pourra tester son prototype au sein du ministère des Armées.

Piéger un cyber attaquant pour observer et comprendre son mode opératoire : c'est sur ce principe que reposent les innovations développées par les PME AMOSSYS et SESAME IT.

- Le produit, baptisé BEEZH Platform développé par la PME AMOSSYS, est ainsi capable de reconstituer de manière très réaliste un système d'information, laissant penser à l'attaquant qu'il a réussi à pénétrer le réseau informatique ciblé. Sa particularité ? Les nombreuses possibilités de personnalisation et la capacité à générer en permanence de l'activité utilisateur pour produire un système crédible et cohérent.
- Le projet LOKI, développé par la PME SESAME IT consiste à leurrer les cyberattaquants en les attirant dans un réseau parallèle. Comment ? en déployant un réseau de leurres réalistes et crédibles. La technologie permet de reproduire tous les types de réseaux, de manière automatisée. Elle permet de détecter en temps réel une tentative d'intrusion et offre aussi la possibilité de mener des actions offensives, en disséminant des fichiers piégés dans le réseau de leurres.

# LA DGA, UNE FORCE D'INNOVATION TECHNIQUE UNIQUE AU SEIN DU MINISTÈRE DES ARMÉES

**Le projet SCAAM*, une innovation 100% made in DGA !**

Avec l'apport de l'intelligence artificielle (IA), les futures attaques cyber seront plus sophistiquées et pourront déjouer les mécanismes de sécurité les plus robustes des solutions cryptographiques, menaçant la sécurité des systèmes militaires. Pour faire face à ce défi majeur, la Direction générale de l'armement (DGA) a lancé le projet SCAAM qui vise à anticiper et comprendre la menace pour concevoir des composants cryptographiques hautement sécurisés destinés à protéger les équipements militaires de demain.

Il s'agit en premier lieu de maitriser la menace pour conserver une longueur d'avance. Pour cela, les experts de la DGA analysent au quotidien cette « cybermenace » progressant à une vitesse galopante. Avec les dernières avancées technologiques, un acteur malveillant pourrait hacker un équipement comme un missile ou un système de communication, pour accéder à ses données et prendre son contrôle. Comment ? En mesurant son rayonnement électromagnétique pour en extraire sa clé de chiffrement. Aujourd'hui, il s'agit d'une attaque d'une extrême complexité nécessitant plusieurs semaines de calculs mais qui pourrait demain, avec l'arrivée de l'IA, être à la portée de nombreux cyberattaquants.

Pour se prémunir de cette nouvelle menace redoutable, la DGA doit relever le défi de concevoir et développer des mécanismes de sécurité et des composants cryptographiques capables de résister à ces nouvelles attaques. La force de la DGA est d'associer expertise cyber et expertise en IA. Les premiers résultats de ces travaux sont éloquents. Déjà, les ingénieurs de la DGA ont mis au point des algorithmes qui se placent au meilleur niveau mondial.

**SCAAM : Side Channel Attack par Apprentissage Machine*

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

DGA

# ESPACE PITCH : RENCONTRE AVEC LES ACTEURS DE LA CYBERSÉCURITÉ

**Rendez-vous sur l'espace d'échanges du stand où des start-up, PME/TPE, chercheurs, entrepreneurs présenteront leur innovation développée avec le soutien de l'Agence de l'innovation de défense.**

Au programme aussi :

- Présentation par l'Agence de l'innovation de défense des dispositifs d'accompagnement et de soutien destinés aux industriels et chercheurs pour booster leur projet d'innovation.
- Rencontre avec des recruteurs de la DGA pour découvrir les métiers et formations dans domaine cyber.

Venez prendre rendez-vous au plot de l'Agence de l'innovation de défense pour y présenter votre projet d'innovation.

*Voir Programme en annexe*

**Les industriels de la cybersécurité sont invités à venir présenter leur projet sur le stand du ministère des Armées, auprès de l'Agence de l'innovation de défense.**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

DGA