Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMÉES

Règlement du défi cyber « Détection d'images falsifiées ou générées »

AGENCE INNOVATION DÉFENSE

TABLE DES MATIERES

I. CONTEXTE DU DEFI

La guerre de l'information est partie intégrante de toute stratégie militaire, les armées françaises font l'objet d'attaques informationnelles dans le cyberespace, orchestrées par des groupes ou des États hostiles à leur action. La lutte informatique d'influence (L2I) désigne les opérations militaires conduites dans la couche informationnelle du cyberespace pour détecter, caractériser et contrer les attaques. Ce défi s'intéresse plus particulièrement à la capacité à détecter des « images falsifiées ou générées par des techniques d'intelligence artificielle », utilisées par exemple pour créer un faux discours d'un responsable politique ou de fausses exactions de soldats en opérations.

II. OBJECTIFS DU DEFI

Le défi vise à capter les solutions innovantes permettant la détection d'images falsifiées ou générées et à avoir une première évaluation de leur capacité à détecter des menaces à l'état de l'art. Il porte plus particulièrement sur le volet **capacité de détection automatique** (sans intervention humaine). La capacité de détection porte sur :

- Des images complètement générées par IA
- Des images partiellement modifiées par IA
- Des images partiellement modifiées par traitements d'image classiques

Le présent règlement détermine les règles et modalités de participation au Défi « Détection d'images falsifiées ou générées ».

III. DÉROULEMENT DU DEFI

Déroulement du défi	
Novembre 2023	Lancement du défi et ouverture des inscriptions
Phase 1 présélection	
Mardi 20 février 2024	Date limite de dépôt des dossiers de candidatures
Vendredi 08 mars 2024	Annonce des candidats retenus pour l'audition
Mardi 19 mars 2024	Audition des candidats retenus à l'Innovation Defense Lab avec envoi préalable des supports de présentation pour le 15 mars
Vendredi 29 mars 2024	Annonce des lauréats sélectionnés pour la phase 2 avec envoi de la procédure d'évaluation et des échantillons de tests
Phase 2 évaluation	
Mercredi 03 avril 2024	Présentation et échange par visio sur la procédure d'évaluation avec les candidats sélectionnés
Lundi 03 juin 2024	Envoi des données d'évaluation (les délais de transmission des résultats par les candidats seront précisés dans la procédure d'évaluation)
Mercredi 26 juin 2024	Désignation des trois meilleurs solutions
ECW 2024	Présentation des trois meilleurs solutions à la conférence CAID 2024 (Conference on Artificial Intelligence for Defense)

L'AID se réserve le droit de modifier les dates des jalons intermédiaires du défi si des impératifs opérationnels l'imposent.

Phase 1 présélection

La phase de présélection se déroule selon les modalités suivantes :

- Etape 1 : les candidats élaborent leurs **dossiers de candidature** et les transmettent au plus tard au jalon indiqué ci-dessus.
- Etape 2 : le comité de sélection analyse les dossiers de candidature reçus au regard des critères de classement définis dans le présent règlement. Les candidats ayant remis les dossiers jugés les plus pertinents sont reçus en **audition** à l'Innovation défense lab (15e arrondissement de Paris).

Lors des auditions, les candidats devront présenter :

- le porteur et les partenaires éventuels avec leurs rôles respectifs, en soulignant les compétences et expériences pertinentes par rapport au sujet du défi
- une description technique de leur solution de détection et de la feuille de route associée

- si possible, une présentation de résultats de détection

Au terme de ces deux étapes, le comité de sélection choisira les candidats retenus pour la phase 2 selon les critères de sélection définis à l'Art.6.

L'AID communique à tous les candidats par courrier électronique envoyé à l'adresse renseignée lors de l'inscription les résultats de la présélection, avec pour les candidats retenus pour la phase 2, l'envoi de la procédure d'évaluation et des échantillons de tests

Phase 2 évaluation

La phase d'évaluation se déroule selon les modalités suivantes :

- Etape 1 : une réunion en visio est organisée pour **présenter les modalités d'évaluation**. Les candidats vérifient avec les données de tests leur capacité à utiliser le jeu de données d'évaluation
- Etape 2 : le jeu de données d'évaluation est transmis et les candidats **déroulent la procédure d'évaluation** et renvoient les résultats au jalons indiqués ci-dessus. Le comité de sélection effectue un classement des résultats reçus selon les critères de la procédure d'évaluation.
- Etape 3 : information des résultats aux candidats avec identification des trois meilleurs,
- Etape 4 : les trois lauréats retenus présentent leurs solutions lors de la **conférence CAID 2024** (Conference on Artificial Intelligence for Defense) à **l'ECW** (European Cyber Week).

IV. MODALITÉS DE PARTICIPATION AU DEFI

L'inscription et la participation au défi sont gratuites. Les candidats ne peuvent prétendre à aucune indemnité pour leur participation.

Les candidats peuvent être une entreprise ou un groupement d'entreprises pouvant inclure des organismes de recherche [1]. Un candidat ne peut pas concourir à la fois en tant que candidat individuel et candidat au sein d'un groupement.

Seules les sociétés françaises et les organismes de recherche ayant un établissement en France peuvent participer au défi.

V. DOSSIER DE CANDIDATURE ET LIVRABLES

Les candidats transmettent, dans le respect du calendrier défini à l'Article 3, leur dossier de candidature et les livrables demandés à l'adresse suivante :

agence-innovation-defense-defi-cyber.contact.fct@intradef.gouv.fr

Phase 1 de présélection

Au titre de la phase 1 de présélection, les candidats devront remettre un **dossier de candidature** comprenant les éléments et documents suivants au format PDF:

- un point de contact pour le défi (avec nom, adresse mail et téléphone)

[1] Il s'agit d'un partenaire de droit public ayant pour vocation principale d'effectuer de la recherche (tels qu'EPST, université, EPIC de recherche, etc.) et les partenaires/entités de droit privé exerçant une activité de recherche, ayant un établissement en France et n'étant pas des sociétés commerciales

- une fiche pour le porteur et pour chaque partenaire industriel en utilisant le modèle joint « 3_Dossier-défi-cyber_Description-Nom-société » (renommer le document en remplaçant « Nom-société » par le nom du porteur ou partenaire concerné)
- un document technique en utilisant le modèle joint « 4_Dossier-défi-cyber_Description-solution-Nom-porteur » (renommer le document en remplaçant « Nom-porteur » par le nom du porteur), comprenant
    - une description des compétences techniques et travaux antérieurs réalisés en lien avec le sujet du défi pour le porteur et les partenaires, et leurs contributions respectives à la solution qui sera évaluée
    - une description technique de la solution de détection d'images falsifiées ou deepfake, en détaillant l'architecture utilisée, les traitements automatiques de détection (**le défi porte sur les résultats issus de ces traitements automatiques**), les données utilisées pour entrainer les modèles, le processus mis en place afin de rester à l'état de l'art des outils de synthèse et/ou falsification d'images. Si la solution intègre en complément des étapes de post-analyse manuelles le document pourra le préciser
    - un focus sur les aspects innovants de la solution
    - une présentation de la feuille de route technique produit
- une copie d'un extrait Kbis de moins de trois (3) mois pour les partenaires industriels
- le règlement du défi signé par le porteur du projet
- l'engagement de non diffusion des données du défi signé par le porteur du projet et les partenaires

Le dossier pourra utilement être complété de toute autre pièce que le candidat jugera opportun de communiquer ou que le comité de sélection pourra souhaiter.

Phase 2 évaluation

Au titre de la phase 2, les lauréats devront remettre :

- les résultats d'analyse du jeu de données transmis
- l'analyse des limites actuelles identifiées des outils et les éléments de feuille de route prévus le cas échéant

En cas de difficultés ou d'impossibilité de lecture d'un livrable par l'une au moins des parties, il est de la responsabilité du lauréat concerné d'y remédier avant la date de fin de dépôt des livrables finaux. Passé ce délai, les parties se réservent le droit de disqualifier le lauréat en cause du défi.

VI. CRITÈRES DE PRESELECTION ET CLASSEMENT

Exigences et critères de classement de la phase 1 de présélection

Pour évaluer les propositions de projet, le comité de sélection utilise une grille d'évaluation constituée des critères suivants :

Critères	**Points**
Pertinence technique de la solution	30
Caractère innovant de la solution	30
Pertinence de la feuille de route produit	20
Apport des compétences et expériences détenues par le porteur et les partenaires	20

Exigences et critères de classement de la phase 2 d'évaluation

Les critères seront fournis dans la procédure d'évaluation.

VII. PROPRIÉTÉ INTELLECTUELLE

Propriété intellectuelle sur les données du ministère des Armées :

- le ministère des Armées demeure titulaire de tous les droits sur les données soumises aux candidats dans le cadre du défi.

Propriété intellectuelle sur les solutions des lauréats :

- le candidat reste propriétaire de la solution technologique développée dans le cadre du défi.
- chaque candidat est seul juge de l'opportunité et des modalités d'une protection des informations qu'il transmet par la revendication de tels droits.

VIII. COMMUNICATION

Les candidats autorisent l'AID et le ministère des Armées à reproduire leur marque à titre gratuit sur les supports de communication autour du défi, tels que et sans que ce soit exhaustif : écrans sur sites internes et externes, signatures / newsletters e-mail, communiqués de presse, affiches / kakémonos sur salons, réseaux sociaux de l'organisateur ou du commanditaire.

Les candidats autorisent également l'AID et le ministère des Armées à reproduire leur dénomination sociale, leur nom commercial sous les mêmes conditions ainsi que leur logo tel que reproduit dans le dossier de candidature.

La présente autorisation entre en vigueur à compter de la date du début du défi, et pour la durée et les besoins visés dans les finalités susmentionnées.

Les candidats comprennent que ces autorisations ont pour objet de contribuer à la mise en valeur de leur projet.

Toute communication par les candidats concernant tout ou partie du défi doit faire l'objet d'une demande d'autorisation préalable à l'Administration, avec soumission des grandes lignes puis si avis favorable, transmission du contenu rédigé de la communication pour autorisation finale.

IX. RESPONSABILITÉ

La responsabilité du ministère des Armées ne pourra être engagée en cas de panne ou de dysfonctionnement du réseau de télécommunication utilisé, qui aurait notamment pour effet d'empêcher l'identification ou l'accès à tout site internet utile pour la participation au défi.

La participation au défi implique la connaissance et l'acceptation des caractéristiques, des limites et des risques du réseau internet et des technologies qui y sont liées, notamment eu égard aux performances, au temps de réponse, à la sécurité des logiciels et du matériel informatique face aux diverses attaques potentielles du type virus, bombe logique ou cheval de Troie et à la perte ou au détournement de données. En conséquence, le ministère des Armées ne pourra être en aucun cas tenue pour responsable des dommages causés au candidat du fait de ces caractéristiques, limites et risques acceptés.

L'AID ne pourra, en aucun cas, être tenue pour responsables du dommage causé par le défaut ou le retard d'acheminement des livrables et notamment du refus de prise en compte de ces livrables en raison d'une soumission hors des délais fixés dans le règlement, par le défaut ou le délai d'acheminement de tout courrier électronique envoyé dans le cadre du défi ou par toute altération portée aux livrables indépendamment du fait de l'AID.

L'AID ne pourra être tenue pour responsable en cas de modification totale ou partielle, de suspension, d'interruption, de report ou d'annulation du défi pour des raisons indépendantes de sa volonté. Dans de telles hypothèses, l'AID informera dans les plus brefs délais les candidats par courriel.

L'AID ne pourra être tenue pour responsable des conséquences d'une disqualification d'un candidat en raison de sa violation du règlement.

X. CONFIDENTIALITÉ

Est une « **Information Confidentielle** » toute information appartenant au ministère des Armées ou au candidat, communiquée ou rendue disponible par, ou au nom de, la « **Partie Divulgatrice** » la « **Partie Réceptrice** », directement ou indirectement, qu'elle soit ou non formellement identifiée comme étant confidentielle, notamment sans limitation, liste de clients, registres, rapports, analyses, déclarations fiscales, compilations, études, formulaires, méthodes des affaires ou de management, plans d'affaires, données marketing, documents de design, dessins, information d'ingénierie, analyses financières, plans, formules, savoir-faire, idées, inventions, informations de marché, plans marketing, procès, produits et informations afférentes, secrets d'affaires et toute information obtenue directement ou indirectement, par la Partie Réceptrice par l'inspection, la révision ou l'analyse des documents qui lui ont été communiqués ou mis à sa disposition. L'Information Confidentielle peut être tangible ou intangible et peut être communiquée oralement, par écrit, par moyen ou sur support électronique, par observation visuelle ou par d'autres moyens et comprend également toutes copies, extraits et résumés.

La Partie Réceptrice utilisera les Informations Confidentielles uniquement pour les finalités pour lesquelles elles ont été communiquées et s'interdit d'utiliser, divulguer à tout tiers, d'exploiter commercialement, dupliquer, copier, transmettre ou autrement diffuser ou permettre toute action de ce type, a tout moment avant ou après la fin du défi, sauf pour les besoins autorisés par ce défi. La divulgation de l'Information Confidentielle que ce soit en interne du Commanditaire comme en externe n'est pas autorisé sans l'accord écrit de la Partie Divulgatrice.

La Partie Réceptrice s'engage à prendre des mesures raisonnables pour garder secrètes les Informations Confidentielles et pour éviter toute divulgation, diffusion ou utilisation non-autorisée de ces informations. Les *« mesures raisonnables »* incluent, sans limitation : la protection contre l'accès, l'utilisation et la divulgation non-autorisée. La Partie réceptrice

s'engage à notifier promptement et par écrit à l'autre Partie de toute utilisation non-autorisée, divulgation, perte d'Information Confidentielle de la Partie divulgatrice en violation du présent Règlement, la notification incluant le rappel des mesures prises ou envisagées par la Partie Réceptrice pour remédier à la situation.

Les obligations figurant dans cet Article sont applicables pendant la durée du défi et survivront pour une période de cinq (5) ans après la fin du défi.

XI. ANNULATION ET SUSPENSION DU DEFI

L'AID se réserve le droit d'annuler ou de suspendre notamment le défi en cas de :

- force majeure ;
- fraude de quelque nature que ce soit.

L'AID ne pourra être tenue pour responsable d'une annulation ou d'une suspension du défi conformément au présent Article et aucune indemnité ou compensation ne sera due aux candidats.

XII. LOI APPLICABLE

Le règlement et le défi sont soumis au droit français.

Entreprise porteur du projet : ……

Fait le ……, à ……..

Signature