SHIELD
PCP

SHIELD PCP Consultation Ouverte du Marché (COM)

Webinar en français

27 février 2026

Informations

Cette session est enregistrée et les enregistrements seront partagés.

Les présentations seront partagées.

Merci de garder vos micros en silencieux pendant les présentations et de les activer uniquement lors des moments d'interaction.

Les caméras sont facultatives.

Vous pouvez utiliser le chat pour poser des questions et faire des commentaires.

Funded by the European Union

Ordre du jour

Heures	Sujet	Présentateur
13:00 – 13:05	**Bienvenue et remarques d'ouverture**	*Ministère de l'Intérieur français*
13:05 – 13:45	**Présentation du projet PCP SHIELD (objectifs, cas d'usage, processus PCP, pilotes)**	*Ministère de l'Intérieur français* *CIVIPOL* *SNCF*
13:45 – 14:00	**Présentation des résultats de l'analyse de l'état de l'art**	*DIGINNOV*
14:00 – 14:20	**Objectifs et activités de la COM**	*Ministère de l'Intérieur français* *CIVIPOL*
14:20 – 14:50	**Session interactive**	*SNCF*
14:50 – 15:00	**Conclusions et prochaines étapes**	*Ministère de l'Intérieur français - CIVIPOL*

Funded by the European Union

SHIELD
PCP

Présentation du projet SHIELD PCP (objectifs, cas d'usage, processus PCP, pilotes)

Ministère français de l'Intérieur – CIVIPOL - SNCF

SHIELD PCP

Renforcer la sécurité par l'innovation

SHIELD PCP est un projet financé par la Commission européenne, qui rassemble les intervenants de première ligne, les autorités publiques et les fournisseurs de technologie afin de cocréer des solutions innovantes pour la protection des espaces publics.

L'objectif principal est de doter les acteurs de la sécurité de technologies de pointe acquises par le biais de processus innovants, en offrant des solutions qui permettent une coordination et une coopération transparentes entre toutes les parties prenantes, en particulier les forces de l'ordre.

Par le biais de l'approche des achats publics avant commercialisation, le projet transforme des besoins opérationnels avérés en solutions technologiques innovantes, renforçant la sécurité et la coordination des réponses dans des contextes de gestion de foules complexes et dynamiques.

Funded by the European Union

Eléments clés

L'objectif principal de **SHIELD PCP** est d'encourager l'innovation en donnant aux acheteurs publics les moyens d'agir.

SHIELD PCP contribuera à accroître l'impact du travail effectué dans l'écosystème de la recherche et de l'innovation en matière de sécurité de l'UE.

Funded by the European Union

Comment le projet a– t-il démarré?

De SHIELD4CROWD à SHIELD PCP

SHIELD4CROWD a construit les bases d'une approche européenne de la protection des espaces publics par le biais de l'innovation et des achats publics avant commercialisation (PCP).

En identifiant les vulnérabilités communes, en cartographiant les lacunes technologiques et en réunissant les praticiens de la sécurité à travers l'Europe, le projet a préparé le terrain pour **SHIELD PCP**, qui transforme les besoins partagés en actions d'innovation concrètes.

Funded by
the European Union

Défi

Les espaces publics accueillent souvent des foules nombreuses et dynamiques, qu'il s'agisse de mouvements urbains quotidiens ou d'événements majeurs. Pour assurer la sécurité dans de tels environnements, il faut une coordination en temps réel entre les agences, des systèmes de communication fiables et une connaissance précise de la situation.

SHIELD PCP se concentre sur quatre domaines de capacité essentiels :

- **Coordination du centre de commandement** : intégration des données et des systèmes de contrôle pour une gestion en temps réel.
- **Communication sécurisée :** Assurer un flux d'informations fiable entre les premiers intervenants et le public.
- **Surveillance des foules** : Analyse en temps réel de la densité de la foule, des mouvements et des comportements anormaux.
- **Surveillance des mouvements** : Détecter les schémas de mouvement et, si nécessaire, se concentrer uniquement sur des individus ou des groupes spécifiques afin d'apporter une réponse rapide.

Funded by the European Union

Nos objectifs

Affiner et valider les **besoins** technologiques et opérationnels **des praticiens de la sécurité.**

Construire **un réseau solide** d'acheteurs publics et d'utilisateurs finaux à travers l'Europe.

Développer, prototyper et valider de **nouveaux outils de sécurité** par le biais d'un processus PCP progressif.

Veiller à ce que toutes les solutions respectent les **normes éthiques, juridiques et sociales**

Préparer une **voie** claire **pour l'adoption par le marché**, y compris les futurs achats à grande échelle.

Funded by the European Union

Informations générales

- Nom complet du projet :

  SECURITY HARMONIZED INNOVATION FOR ENHANCED LAW ENFORCEMENT CAPABILITIES IN DYNAMIC CROWD PROTECTION THROUGH PRE-COMMERCIAL PROCUREMENT

- Financé par : **HORIZON Europe**
- Calendrier : **1er octobre 2025 - 30 septembre 2028**
- Consortium : **12 partenaires** de **7 pays**
- Site web : https://shieldpcp.eu
- Projet : GA N° **101225962**

Funded by the European Union

Consortium

CORVERS
COMMERCIAL & LEGAL AFFAIRS

MINISTERIO DEL INTERIOR

ISEM INSTITUTE

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Isdefe

SNCF

CIVIPOL

novadays

DigInnov

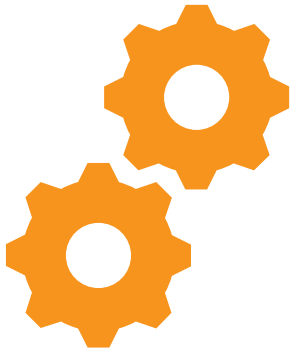
SAFE

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

Polish Platform
For Homeland Security

Funded by the European Union

Résultats attendus



Grâce au processus d'**achats publics avant commercialisation (PCP**), le **projet SHIELD PCP** développera et testera **des solutions prototypes** dans des environnements opérationnels réels en France, en Espagne et en Slovaquie

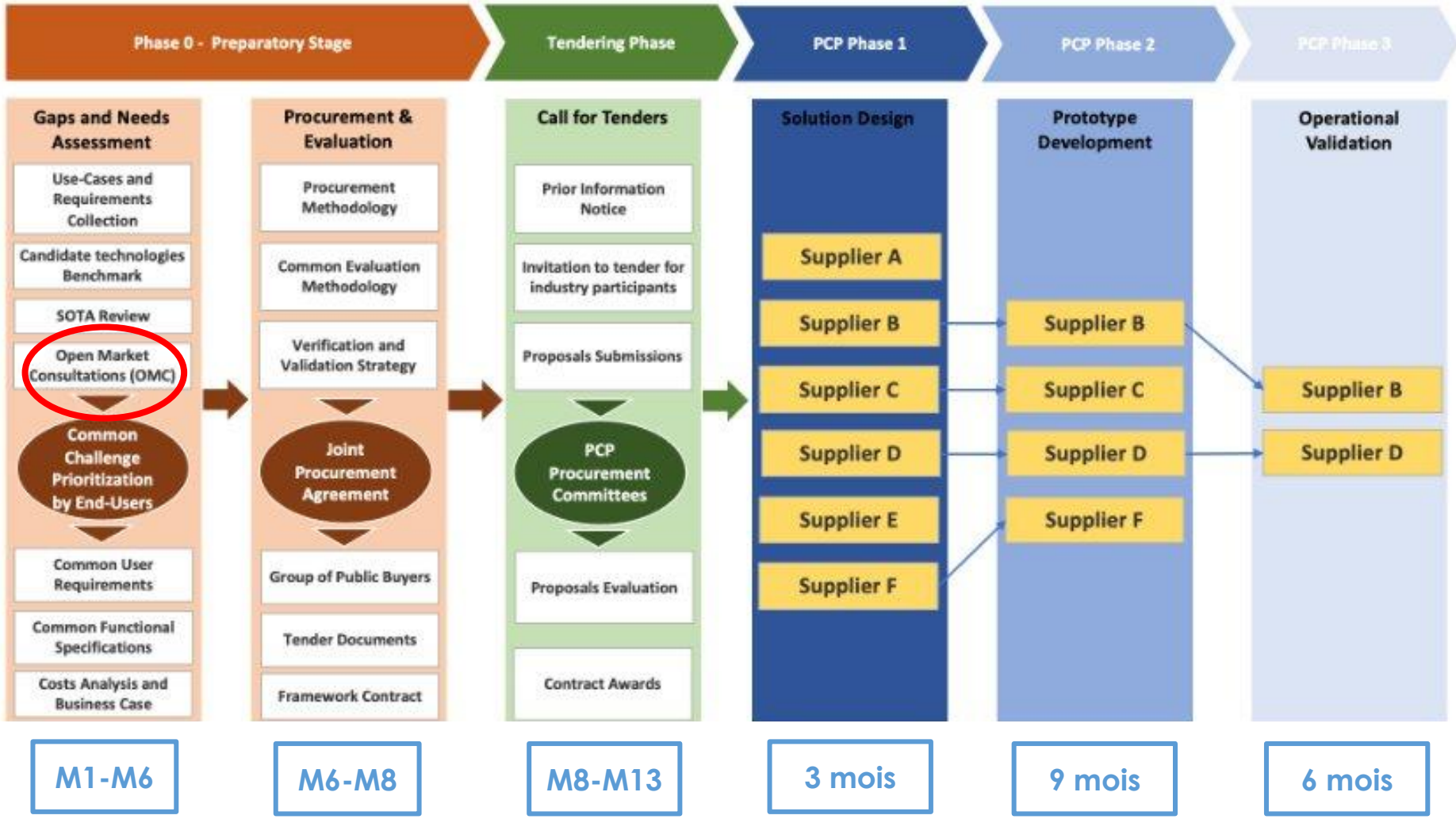
Le projet ne fournira pas de produits prêts à être commercialisés, mais des **concepts testés et une feuille de route claire** pour un futur déploiement à grande échelle par le biais **d'achats publics de solutions innovantes (PPI**) ou d'autres mécanismes de financement

Cette approche renforce la coopération, stimule l'innovation et améliore la capacité de l'Europe à protéger les espaces publics

Funded by the European Union

Phases d'acquisition de l'innovation du SHIELD PCP

Nous sommes ici



Funded by the European Union

Appel d'offres

Publication : Mai 2026

Réception des offres : Juin-août 2026

Une période suffisante sera prévue pour préparer et soumettre des propositions.

L'appel d'offres décrira les exigences, les sites pilotes et les critères d'évaluation.

L'évaluation prendra en compte

1. l'innovation technique et la faisabilité
2. le coût et le rapport qualité-prix
3. l'impact opérationnel et le potentiel d'évolution
4. l'impact social et éthique

Funded by the European Union

Appels d'offres

Annonce : Octobre 2026

Les offres seront soumises à :

- Des contrôles administratifs d'éligibilité
- Une évaluation en fonction de critères d'exclusion, de sélection et de réussite/échec
- Notation des critères techniques et financiers

Les fournisseurs sélectionnés pour la phase 1 seront invités à poursuivre.

Funded by the European Union

Phases de développement du PCP

Phase 1
Conception de la solution

Durée du projet : ~3 mois

Phase 2
Développement et test du prototype

Durée de la phase 2 ~9 mois

Phase 3
Essais opérationnels en environnement réel

Durée de la phase 3 ~6 mois

Funded by the European Union

SHIELD
PCP

Projet SHIELD PCP (cas d'usage, pilotes)

Ministère de l'Intérieur

Pilote 1 - Panique au stade de football

Où / Qui	• **Stade MŠK Žilina (Slovaquie) Utilisateurs finaux : MOI, ISEMI** • **Soutien : Police nationale, forces et services de première ligne, sécurité du stade, police municipale, SAMU**
Problème principal	• Un match de football à haut risque dégénère en panique générale lorsque des ultras allument des obus fumigènes à l'intérieur du stade, provoquant des incendies, une visibilité réduite, des voies d'évacuation bloquées et des mouvements de foule incontrôlés.
Objectif du SHIELD PCP	• Amélioration de la **coordination multi-agences** (police, FRS, services médicaux d'urgence, sécurité). • Partage d'une **image opérationnelle commune (COP)** en temps réel entre les agences. • **Détection** précoce **des groupes et comportements suspects et des objets interdits.** • **Surveillance des mouvements de foule** et détection des embouteillages. • **Identification des auteurs** avant et pendant l'escalade. • **Communication** ciblée **aux spectateurs** pour réduire la panique et guider l'évacuation.

Pilote 2 - Journée de match Drone Attack

Où / Qui	• **Stade Metropolitano, Madrid (ES)** • **Utilisateur final : Policía Nacional** • **Support : LaLiga, SAMUR (**service municipal d'urgence et de secours)**, 112, Police locale, Metro, EMT (**ambulancier urgentiste)
Problème principal	• Un match de football est perturbé par des **drones armés et incontrôlés**, provoquant des explosions, une panique générale et des mouvements de foule dangereux vers les sorties et les points d'accès au métro.
SHIELD PCP Focus	• Détection, suivi et neutralisation des **drones commerciaux et des drones armés** • **Réponse anti-drone résiliente** malgré la manipulation des fréquences radio. • **Image opérationnelle commune (COP)** en temps réel entre les agences • **Coordination multi-agences** par le biais d'un commandement et d'un contrôle unifiés • **Détection des mouvements de foule et gestion des flux d'évacuation** • **Communication sécurisée avec le public** pour réduire la panique et guider l'évacuation en toute sécurité

Funded by the European Union

Pilote 3 - Coordination multi-acteurs après une attaque massive au couteau

Où / Qui	• **Gare du Nord (Paris-Nord), France** • **Utilisateurs finaux : FMI, SNCF** • **Soutien : Préfecture de Police (BRI, CCOS : commandement des opérations spéciales, SDRPT : police des transports en commun), Brigade des Sapeurs-Pompiers de Paris, DNPAF, Gendarmerie Nationale, Opération Sentinelle, SNCF & entreprises privées**
Problème principal	• **Des attaques simultanées** au **couteau** à l'intérieur de la gare et dans les rues avoisinantes provoquent le chaos parmi des milliers de voyageurs, nécessitant une compréhension rapide de la situation et une réponse coordonnée de plusieurs agences.
Objectif du SHIELD PCP	• **Compréhension rapide de la situation** grâce à la fusion de données multi-sources • Partage d'une **image opérationnelle commune (COP)** entre la police, les transports et les services de secours • **Coordination multi-agences** avec réduction du temps de latence dans la prise de décision • **Surveillance du comportement de la foule** et détection de l'affluence • **Gestion intelligente des flux d'évacuation** à l'intérieur des gares et des espaces publics • **Communication ciblée** aux voyageurs et au personnel pour réduire la panique et guider l'évacuation en toute sécurité.

Critères et exigences

Image opérationnelle commune et tableaux de bord	COP partagée en temps réel avec des cartes multicouches (points d'intérêt, intervenants, sorties/routes, encombrements, angles morts), ainsi qu'une console opérationnelle unifiée et des tableaux de bord d'indicateurs clés de performance.
Surveillance et analyse des foules	Analyse vidéo/capteur AI pour détecter les comportements anormaux, les déclenchements de panique et les surcharges, générer des alertes et calculer des itinéraires d'évacuation dynamiques et des cartes thermiques de densité.
Géolocalisation, suivi et géofencing	Suivi en temps réel, à l'intérieur comme à l'extérieur, des intervenants, des biens, des suspects et des drones, avec corrélation de la géolocalisation, détection de la faible visibilité et alarmes de zones restreintes géoréférencées.
Gestion des drones et des anti-drones	Module anti-drone dédié intégrant la détection/classification/suivi avec des contre-mesures légales, et fusionnant les trajectoires des drones avec les foules et les intervenants pour prédire les zones d'impact.
Détection des menaces comportementales	Détection par l'IA de groupes coordonnés, de visages dissimulés, d'objets ressemblant à des armes et d'actes violents/dangereux à l'aide d'indices comportementaux non biométriques conformes au RGPD.
Enregistrement, analyse post-incident et preuves	Enregistrement inviolable des décisions, des actions et des échanges de données avec des métadonnées complètes, ainsi que des rapports post-incidents automatisés et une reconstitution de la chronologie.
Architecture et interopérabilité	Architecture ouverte, modulaire et basée sur des normes, avec des API sécurisées, des intergiciels, une synchronisation temporelle et une prise en charge des formats pour intégrer les systèmes existants sans perturber les flux de travail.
Information et alerte du public	Messages publics approuvés par l'opérateur, multicanaux et multilingues (sonorisation, écrans, SMS/applications, diffusion cellulaire) avec des conseils d'évacuation géo-ciblés et accessibles.
Intelligence multimédia et VMS	Partage sécurisé et prioritaire de photos/clips/vidéos en direct et compatibilité avec les principales plateformes VMS pour faciliter la visualisation opérationnelle et la détection pilotée par l'IA.
Aide à la décision et IA	Analyse prédictive, hiérarchisation des menaces et recommandations de réponse dans un environnement unifié d'aide à la décision, avec un apprentissage continu et une grande facilité d'utilisation sous la pression du temps.
Plateforme et déploiement multi-agences	Plateforme interopérable unique permettant une intégration progressive, une intégration fédérée, un échange d'informations sécurisé en temps réel et des outils de communication conjoints unifiés.
Hiérarchie de commandement et flux de travail	Hiérarchie de commandement numérisée avec approbations basées sur des règles, tâches structurées/déconfliction et flux de travail d'escalade automatisés alignés sur la priorité des décisions statutaires.
Intégration et fusion des données	L'ingestion et la fusion en temps réel de vidéosurveillance, de caméras corporelles, de rapports, de drones, de radars et de capteurs environnementaux/comportementaux, ainsi que des modes de simulation/sandbox avec des vues de données protégées.
Contrôle d'accès et gouvernance des données	Contrôles multiniveaux du partage des données imposant une séparation stricte, des vues hiérarchiques adaptées aux rôles et un accès aux données intégrées conforme à la gouvernance.
Performance et latence	Mises à jour en temps réel dans des délais très courts, traitement multimodal à haut débit et rendu géospatial de haute qualité et utilisable dans des conditions de stress opérationnel.
Communications et réseaux	Communications sécurisées, redondantes et anti-brouillage avec gestion des surcharges, E2EE/gestion des clés, basculement sur des réseaux hétérogènes et couverture intérieure/souterraine fiable.

Funded by the European Union

SHIELD
PCP

Présentation des résultats de l'état de l'art

DIGINNOV

Méthodologie

1. Sur la base des mots-clés identifiés à partir de la liste des exigences, fournir les brevets et les normes existants :
    - Définir les mots-clés
    - Effectuer la recherche IPlytics (normes et brevets)
    - Analyser les résultats de la recherche pour identifier ceux qui sont pertinents
2. Tout au long du processus de recherche, la liste des mots-clés a été affinée afin d'éliminer les requêtes extrêmement précises qui pourraient potentiellement négliger des éléments pertinents
3. La recherche a été limitée aux années 2015 à 2025 afin de garantir que le matériel inclus était à jour et axé sur la recherche et la technologie modernes.

Funded by the European Union

Mots clés utilisés

1. Image opérationnelle commune
2. Coordination multi-agences
3. Connaissance de la situation en temps réel
4. Sécurité de l'espace public
5. Plate-forme de gestion des incidents
6. Centre de commandement d'urgence
7. Géorepérage en temps réel
8. Repérage
9. Opérations de sécurité
10. Intervention d'urgence
11. Réponse tactique
12. Surveillance des drones urbains
13. Détection des drones de sécurité
14. Évaluation des menaces dans l'espace aérien
15. Renseignements multimédias
16. Analyse vidéo
17. Gestion des preuves
18. Chaîne de contrôle
19. Temps réel
20. Incident de sécurité
21. Détection des menaces comportementales
22. Analyse prédictive
23. Surveillance de l'espace public
24. Opérations de maintien de l'ordre
25. Analyse du comportement des foules
26. Détection d'anomalies
27. Vision par ordinateur
28. Surveillance des événements publics
29. Fusion de données de capteurs
30. Cadre d'interopérabilité
31. Systèmes hétérogènes
32. Soutien aux premiers intervenants
33. Intégration de la sécurité publique
34. Fusion du commandement et du contrôle
35. Système d'alerte publique
36. Alerte localisée
37. Urgences urbaines
38. Évacuation des foules

Funded by the European Union

Exemples de requêtes utilisées

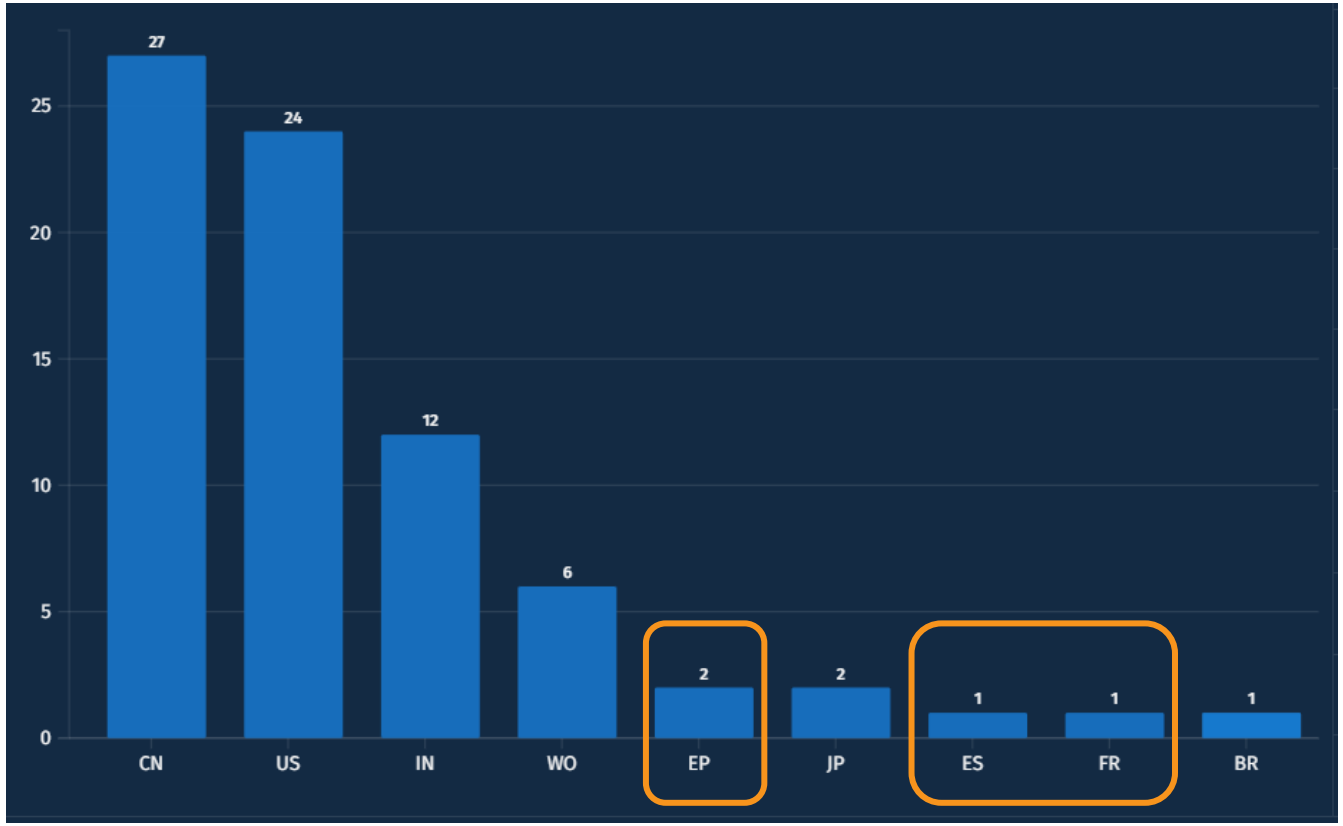
	Requête	Résultats
1	(tous :(image opérationnelle commune)) AND (tous :(coordination multi-agences)) AND (all :(real\-time situational awareness)) AND (all :(public space security)) AND (all :(incident management platform)) AND (all :(emergency command center))	305
2	(tous :(géorepérage en temps réel)) ET (tous : (suivi)) ET (tous : (opérations de sécurité)) ET (tous : (intervention d'urgence)) ET (tous : (intervention tactique))	156
3	(tous : (surveillance des drones urbains)) ET (tous : (détection des drones de sécurité)) ET (tous : (évaluation des menaces dans l'espace aérien))	146
4	(tous :(intelligence multimédia)) ET (tous :(analyse vidéo)) ET (tous :(gestion des preuves)) AND (all :(chain-of\custody)) AND (all :(real\-time)) AND (all :(security incident))	123
5	(tous : (détection des menaces comportementales)) AND (all :(predictive analytics)) AND (all :(public space surveillance)) AND (all :(law enforcement operations))	8
6	(tous : (analyse du comportement des foules)) ET (tous : (détection des anomalies)) ET (tous : (vision par ordinateur)) ET (tous : (surveillance d'événements publics))	78
7	(tous : (fusion de données de capteurs)) ET (tous : (cadre d'interopérabilité)) ET (tous : (opérations de sécurité)) ET (tous : (systèmes hétérogènes)) ET (tous : (soutien aux premiers intervenants)) ET (tous : (intégration de la sécurité publique)) ET (tous : (fusion du commandement et du contrôle))	372
8	(tous : (système d'alerte publique)) ET (tous : (alerte localisée)) ET (tous : (alerte localisée)) ET (tous : (urgences urbaines)) ET (tous : (évacuation des foules))	75

Funded by the European Union

Résultats

- Nous avons identifié plus de 958 brevets, dont 76 sont très pertinents pour notre cas d'utilisation.

- Sur les 83 brevets mondiaux, seuls 4 ont été déposés dans l'UE.



Funded by the European Union

Résultats

Forte couverture par les brevets dans les éléments de base

Surveillance des foules basée sur l'IA

Analyse avancée du comportement des foules et détection des anomalies

Fusion de données multi-capteurs

Intégration de données de capteurs hétérogènes pour une connaissance globale de la situation

Géolocalisation et suivi

Capacités de positionnement et de suivi des mouvements en temps réel

Capacités des drones et des anti-drones

Technologies de déploiement de drones et de contre-mesures

Ces composants font preuve d'une grande maturité dans les domaines de l'analyse, de la détection et de la connaissance de la situation.

Funded by the European Union

Résultats

Lacunes critiques identifiées Domaines où la couverture des brevets est insuffisante

Images opérationnelles communes (COP) partagées

Visualisation basée sur les rôles dans plusieurs agences

Hiérarchie de commandement et gestion des flux de travail

Coordination inter-autorités et chaînes de décision

Outils de prise de décision coordonnée

Systèmes d'aide à la décision collaboratifs multi-agences

Information et alerte du public

Mécanismes de communication intégrés pour les citoyens

Interopérabilité et intégration de l'architecture

Cadres et normes d'intégration au niveau du système

Exigences non fonctionnelles

Facilité d'utilisation, respect de la vie privée dès la conception, gouvernance, modèles de déploiement

Ces éléments sont essentiels pour les opérations intégrées et multi-agences.

Funded by the European Union

Résultats

Aucun brevet ni aucune solution existante ne couvre l'ensemble des besoins du SHIELD PCP.

Le paysage technologique est fragmenté, avec des composants individuels bien développés mais manquant d'intégration holistique.

Funded by the European Union

Aperçu du marché - 10 premiers déposants (TR) - UE

En **Europe**, **Intel** est en tête pour la part de brevets mais enregistre un **faible TR (7,72)**, ce qui indique un impact technique limité. D'autres déposants européens affichent un **TR très faible ou nul**, ce qui suggère des innovations précoces ou incrémentales ayant une faible influence sur les citations. Dans l'ensemble, le paysage européen semble **concentré et peu pertinent sur le plan technique**.

Ultimate Owner	Patents	Fam.	Share	MC	TR
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0
McGill University	1	1	25%	1.2	0

La pertinence technique (TR) indique l'importance d'un brevet en fonction de la fréquence des citations.

- **TR élevée :** technologie très influente et largement citée.
- **Faible TR :** technologie de niche ou moins pertinente, rarement citée.

Ultimate Owner	Patents	Fam.	Share	MC	TR
Inspur Group	1	1	1.3%	0.24	19.12
PIERCE AEROSPACE	1	1	1.3%	2.2	18.49
CIVIL AVIATION MAN INSTITUTE OF CHINA	1	1	1.3%	0.21	13.36
INTELLISHOT HOLDINGS INC	1	1	1.3%	1.33	11.65
Intel	1	1	1.3%	1.1	11.24
Enjoyor	1	1	1.3%	0.15	11.12
QOMPLX	1	1	1.3%	20.01	10.6
Ariake Japan	1	1	1.3%	1.09	7.7
InterDigital	2	1	2.6%	1.33	7.66
GOWARE	1	1	1.3%	0.67	7.04

Funded by the European Union

Aperçu du marché - Les 10 premiers candidats (TR) - Monde

En revanche, le **paysage mondial hors Europe** est dominé par des **candidats au TR élevé**, menés par **Inspur Group (19,12)** et **Pierce Aerospace (18,49)**. Bien qu'ils détiennent de petits portefeuilles, ces acteurs exercent **une forte influence technique**, ce qui met en évidence un environnement d'innovation plus mature et plus influent en dehors de l'Europe.

Ultimate Owner	Patents	Fam.	Share	MC	TR
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0
McGill University	1	1	25%	1.2	0

Ultimate Owner	Patents	Fam.	Share	MC	TR
Inspur Group	1	1	1.3%	0.24	19.12
PIERCE AEROSPACE	1	1	1.3%	2.2	18.49
CIVIL AVIATION MAN INSTITUTE OF CHINA	1	1	1.3%	0.21	13.36
INTELLISHOT HOLDINGS INC	1	1	1.3%	1.33	11.65
Intel	1	1	1.3%	1.1	11.24
Enjoyor	1	1	1.3%	0.15	11.12
QOMPLX	1	1	1.3%	20.01	10.6
Ariake Japan	1	1	1.3%	1.09	7.7
InterDigital	2	1	2.6%	1.33	7.66
GOWARE	1	1	1.3%	0.67	7.04

Funded by the European Union

Aperçu du marché - 10 premiers déposants (CM) - UE

En **Europe**, l'activité en matière de brevets se caractérise par une **couverture de marché uniformément faible**, tous les principaux déposants affichant des **valeurs CM proches ou inférieures à 1**. Cela indique une **empreinte commerciale limitée**, suggérant que les dépôts européens dans cet espace restent **à un stade précoce ou étroitement ciblés**, avec peu d'indications d'un déploiement à grande échelle sur le marché.

Ultimate Owner	Patents	Fam.	Share	MC	TR
McGill University	1	1	25%	1.2	0
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0

La couverture du marché (CM) indique la portée géographique d'un brevet et la valeur commerciale perçue.

- **CM élevée :** protection internationale étendue, potentiel de marché mondial perçu comme élevé.
- **CM faible :** protection géographique limitée, potentiel de marché international perçu comme plus faible.

Ultimate Owner	Patents	Fam.	Share	MC	TR
QOMPLX	1	1	1.3%	20.01	10.6
Strong Force Innovation	4	1	5.1%	19.96	4.3
Johnson Controls	1	1	1.3%	19.8	2.33
LUCOMM TECH	1	1	1.3%	18.47	4.48
LUCOMM TECH INC	1	1	1.3%	18.47	4.48
LUCOMM TECHNOLOGIES	1	1	1.3%	18.47	4.48
MOBILE MAVEN LLC	1	1	1.3%	11.26	2.92
YARDARM TECHNOLOGIES INC	3	1	3.8%	8.74	5.56
AI CONCEPTS	1	1	1.3%	5.36	0
Eaton	1	1	1.3%	2.35	0

Funded by the European Union

Aperçu du marché - Les 10 premiers candidats (CM) - Monde

En revanche, le **paysage mondial hors Europe** est dominé par des candidats ayant des **valeurs CM très élevées**, notamment **QOMPLX (20,01)**, **Strong Force Innovation (19,96)** et **Johnson Controls (19,8)**, plusieurs autres étant regroupés autour de **CM ≈ 18-11**. Cela indique que la **portée du marché est nettement plus large** que celle des candidats européens.

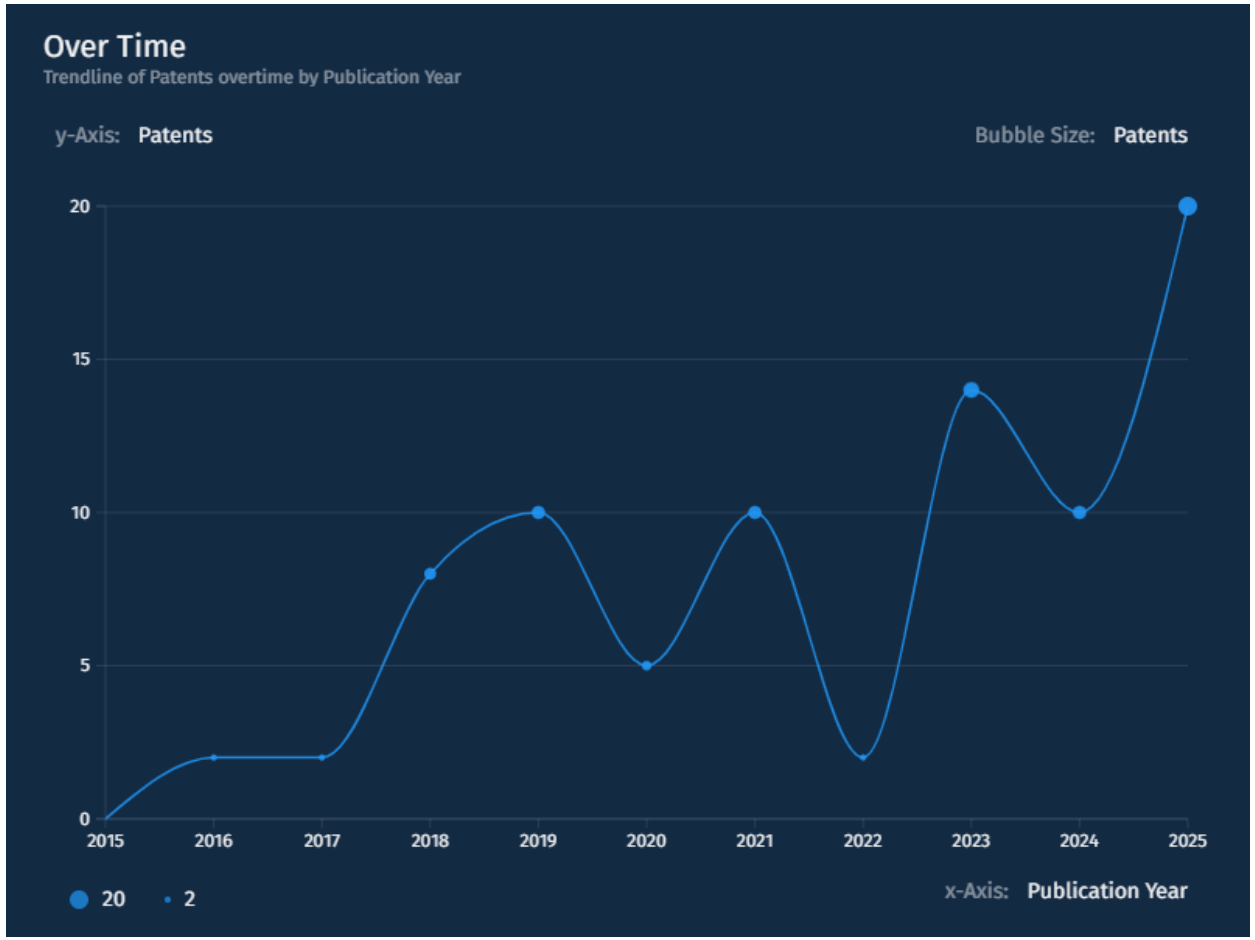
Ultimate Owner	Patents	Fam.	Share	MC	TR
McGill University	1	1	25%	1.2	0
Intel	1	1	25%	1.02	7.72
INOCESS	1	1	25%	0.06	0
KALLISTO AI SL	1	1	25%	0.01	0

Ultimate Owner	Patents	Fam.	Share	MC	TR
QOMPLX	1	1	1.3%	20.01	10.6
Strong Force Innovation	4	1	5.1%	19.96	4.3
Johnson Controls	1	1	1.3%	19.8	2.33
LUCOMM TECH	1	1	1.3%	18.47	4.48
LUCOMM TECH INC	1	1	1.3%	18.47	4.48
LUCOMM TECHNOLOGIES	1	1	1.3%	18.47	4.48
MOBILE MAVEN LLC	1	1	1.3%	11.26	2.92
YARDARM TECHNOLOGIES INC	3	1	3.8%	8.74	5.56
AI CONCEPTS	1	1	1.3%	5.36	0
Eaton	1	1	1.3%	2.35	0

Funded by the European Union

Vue d'ensemble du marché – Publication de brevets au fil du temps

L'activité en matière de brevets montre une **augmentation progressive** avec des fluctuations intermittentes, suivie d'un **fort rebond à partir de 2023**. La forte augmentation vers **2025** indique un **nouvel élan d'innovation** et une concentration croissante de la R&D dans ce domaine.



Funded by the European Union

Aperçu du marché - Géographie

L'activité en matière de brevets est fortement concentrée en dehors de l'Europe, avec en tête la **Chine (29 brevets)** et les **États-Unis (26 brevets)**, suivis par l'**Inde (12 brevets)**, ce qui positionne l'Asie et l'Amérique du Nord comme les principaux centres d'innovation.

L'empreinte de l'Europe reste limitée (PE : 3 brevets) et 1 en Espagne, reflétant une présence régionale plus petite et soulignant que, bien que l'innovation existe, elle n'a pas encore atteint l'échelle mondiale - **indiquant une opportunité de renforcer la collaboration et l'investissement en R&D au sein de la région.**

Funded by the European Union

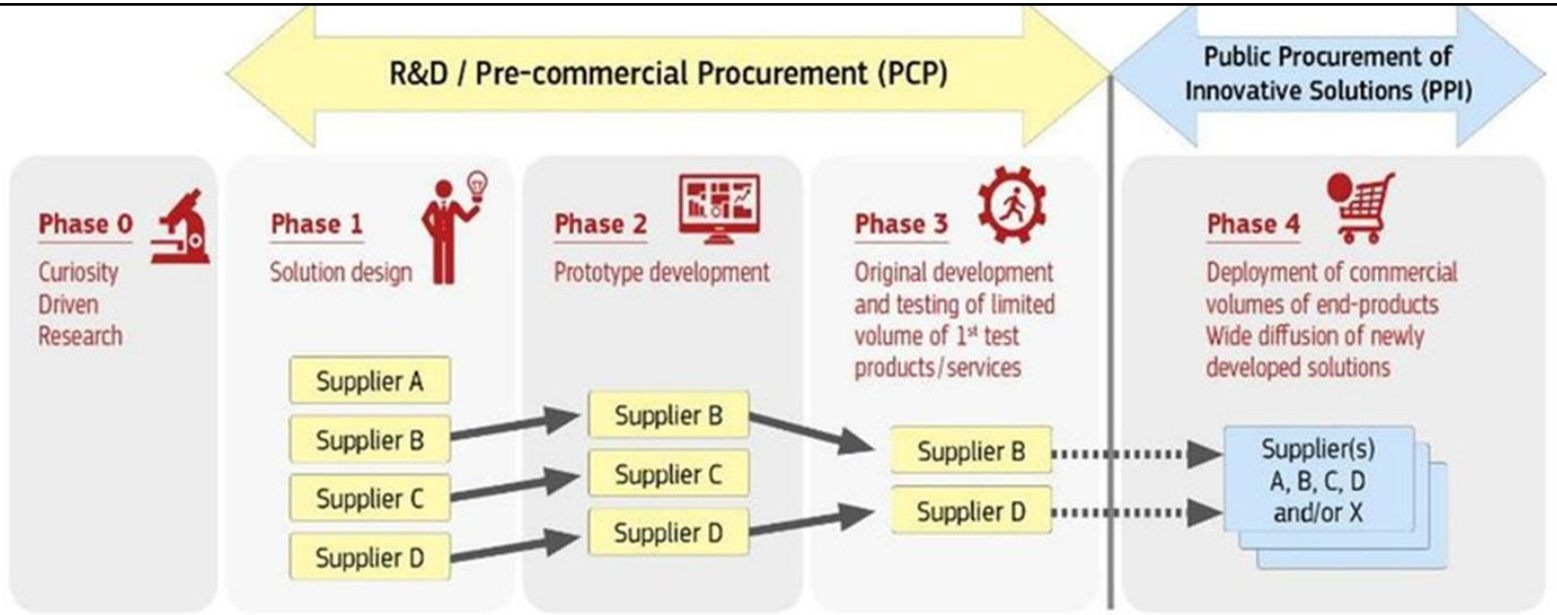
SHIELD PCP

Objectifs et activités de la Consultation Ouverte du Marché (COM)

Ministère de l'Intérieur - CIVIPOL

Achats publics d'innovation

*La passation de marchés d'innovation se produit lorsque **les acheteurs publics** acquièrent le **développement** ou le **déploiement** de **solutions innovantes pionnières** pour répondre à **des besoins** spécifiques à **moyen et long terme du secteur public**.*

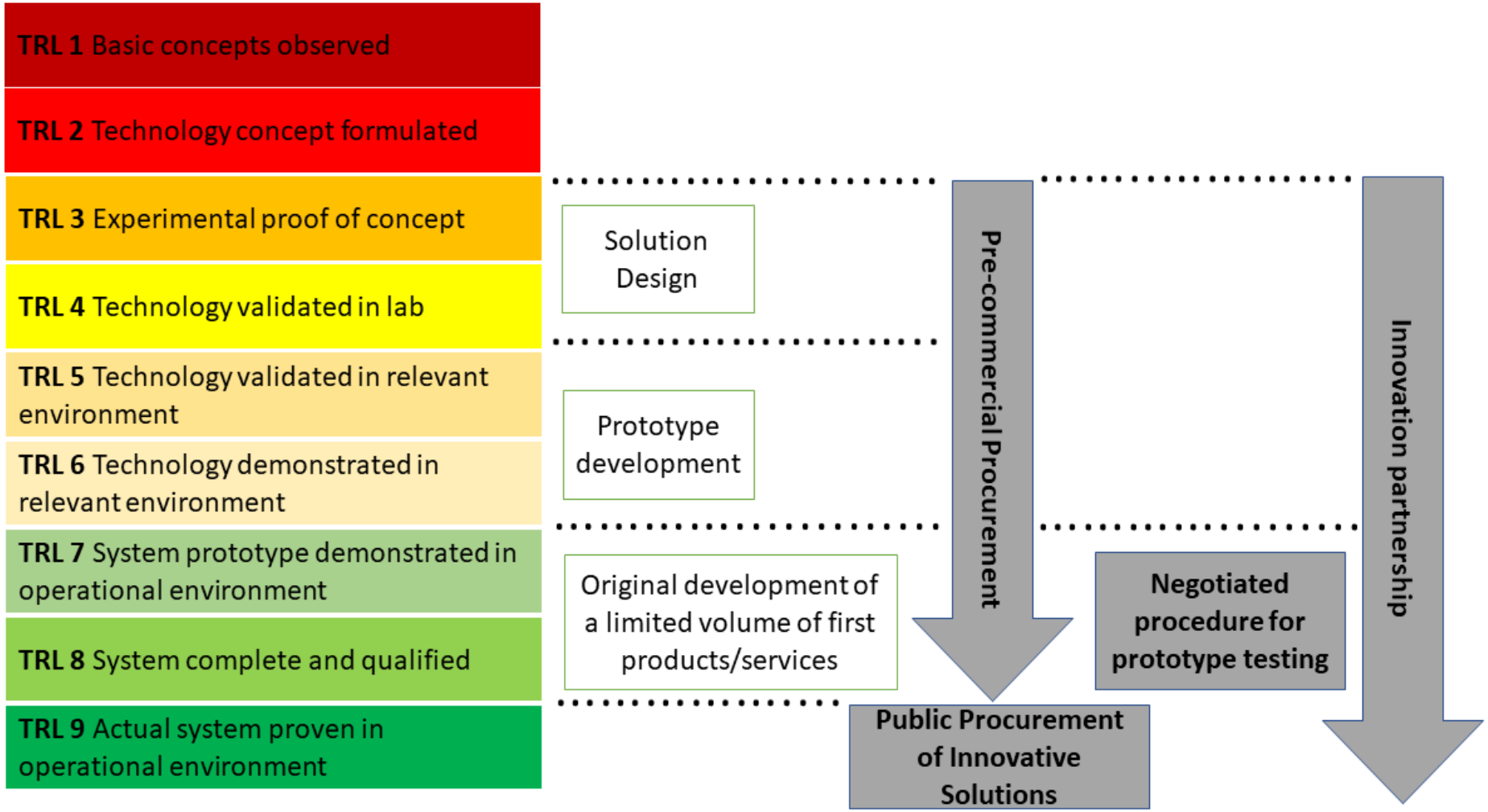


Source : Commission européenne, 2016

- Les marchés publics d'innovation sont un outil permettant de relever des défis sociétaux urgents dans différents secteurs : Soins de santé, changement climatique, efficacité énergétique, transports, sécurité, etc.

Funded by the European Union

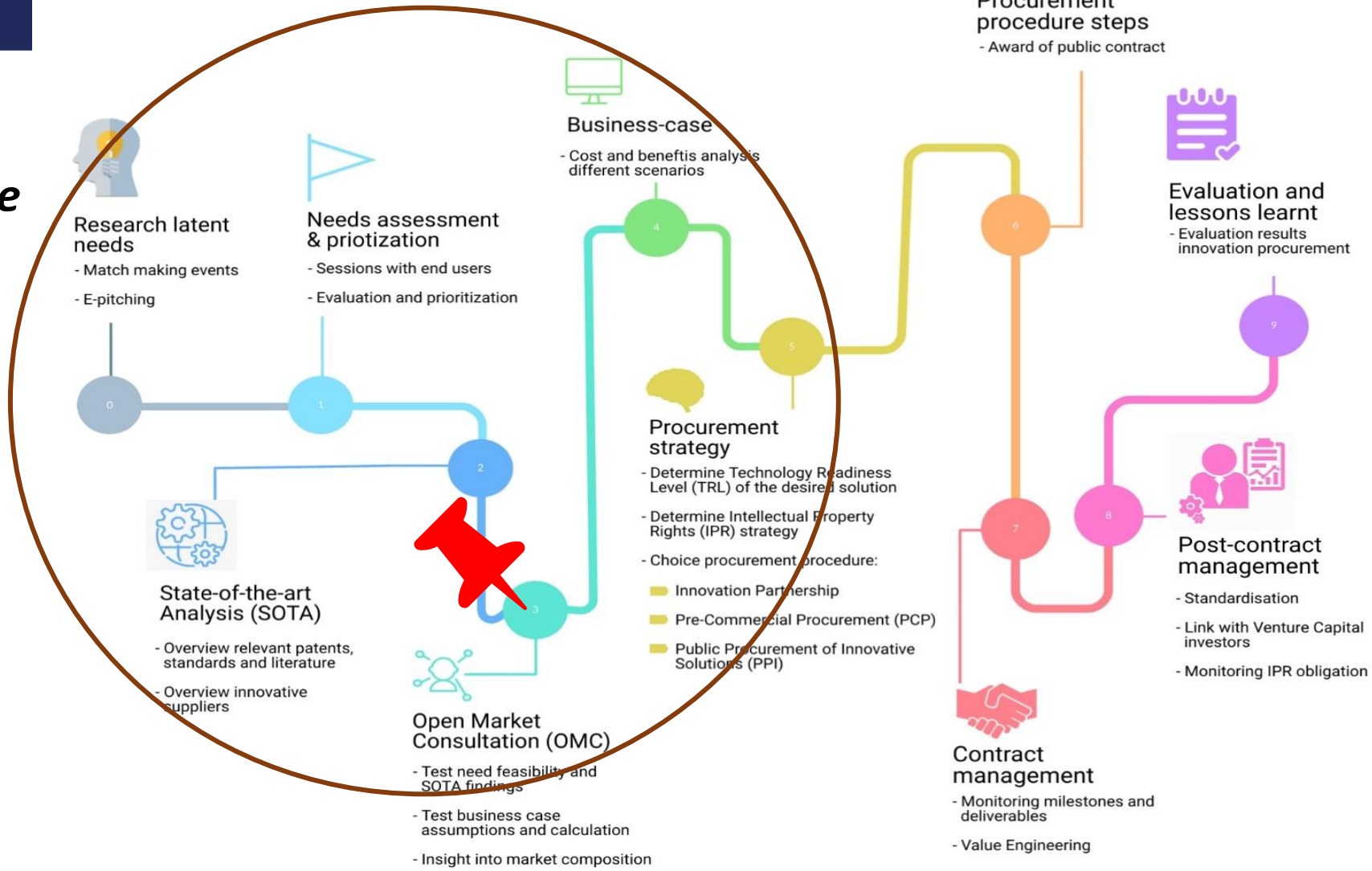
Niveau de maturité technologique



Funded by the European Union

eafip methodology step-by-step

Phase préparatoire



Funded by the European Union

Qu'est-ce qu'une Consultation Ouverte du Marché (COM) ?

Commission européenne, https://projects.research-and-innovation.ec.europa.eu/en/node/11962#:~:text=An%20open%20market%20consultation%20is%20an%20open%20dialogue,to%20meet%20the%20needs%20of%20the%20procurer%20%28s%29.

Avant de lancer une procédure de passation de marché, les **pouvoirs adjudicateurs peuvent mener des consultations de marché en vue de préparer la passation de marché** et d'informer les opérateurs économiques de leurs plans de passation de marché et de leurs besoins.

Les pouvoirs adjudicateurs peuvent également demander ou accepter l'avis d'experts ou d'autorités indépendantes ou de participants au marché. Ces avis peuvent être utilisés dans la planification et le déroulement de la procédure de passation de marché, à condition qu'ils n'aient pas pour effet de fausser la concurrence et qu'ils n'entraînent pas une violation des principes de non-discrimination et de transparence.

Par essence, une consultation de marché ouvert est un **dialogue ouvert entre le(s) acheteur(s) et le marché**, dans le cadre duquel les acheteurs demandent l'avis du marché afin d'identifier sa capacité à répondre aux besoins du(des) acheteur(s).

Funded by the European Union

Pourquoi mener une Consultation Ouverte du Marché (COM) ?

Les consultations ouvertes de marché comblent le fossé entre l'offre et la demande.
Les fournisseurs sont informés des besoins et des attentes des acheteurs.
Les acheteurs sont informés de ce que le marché a à offrir, y compris la chaîne d'approvisionnement, ce qui donne une idée de la résilience et de l'autonomie de l'Europe.

Les **acheteurs** peuvent procéder à des vérifications croisées :

- Analyse des antériorités et recherche de DPI (Droits de Propriété Intellectuelle)
- Analyse du paysage des normes
- L'organisation et les conditions contractuelles clés de la passation de marché
- La faisabilité du projet (par exemple, l'analyse de rentabilité).

Les fournisseurs sont informés des besoins des acheteurs publics.

Funded by the European Union

Objectifs de la Consultation Ouverte du Marché (COM)

Valider les résultats de l'analyse de l'état de l'art et examiner la viabilité des dispositions/fonctionnalités techniques et financières possibles.

Sensibiliser le secteur et les parties prenantes concernées (y compris les autres utilisateurs) au PCP.

Recueillir des informations auprès du secteur et des parties prenantes concernées (y compris les utilisateurs) afin d'affiner les spécifications de l'appel d'offres.

Funded by the European Union

Pourquoi est-il important de consulter le marché ?

Une consultation ouverte du marché révélera **si le besoin est satisfait par une solution commerciale facilement disponible ou si la R&D (PCP) ou une innovation proche du marché (PPI) est nécessaire pour répondre au besoin**.

Lorsque la solution au besoin n'est pas facilement disponible, la consultation du marché ouvert aidera l'acheteur public à choisir la bonne forme de passation de marché en matière d'innovation.

Si la R&D est toujours nécessaire pour répondre au besoin, un PCP est le choix approprié (éventuellement suivi d'un PPI). S'il existe déjà des solutions innovantes appropriées proches du marché, qui ont déjà dépassé le stade de la R&D et sont prêtes à être déployées commercialement par un client de lancement, un PPI est le choix approprié.

Source : EAFIP Toolkit : Boîte à outils EAFIP, Module 2, https://eafip.eu/toolkit/module-2/

Funded by the European Union

Le rôle de la Constulation Ouverte du Marché (COM)

La consultation ouverte du marché est importante à plusieurs égards.

Elle permet de **recouper l'**analyse de marché précédente (SOTA) et de valider le potentiel d'innovation du besoin.

Elle fournit un **retour d'information sur la manière de susciter l'intérêt du marché** pour répondre à l'appel d'offres à venir, sur le type d'acteurs présents sur le marché et sur ce qu'ils peuvent offrir.

Elle **sensibilise** le marché des fournisseurs aux besoins des acheteurs publics.

Elle permet de vérifier la **faisabilité et l'acceptation par le marché** du contrat envisagé (conditions contractuelles essentielles, budget, calendrier, etc.

Funded by the European Union

Calendrier des activités de la COM

Date de l'événement	Événement
24 novembre 2025	Publication de l'avis d'information préalable (PIN) sur TED.
19 décembre 2025	Publication des documents de la COM sur le site web du projet : www.shieldpcp.eu Publication du questionnaire de l'enquête de l'UE.
27 janvier 2026	Webinar COM en français
27 janvier 2026	Webinar COM en espagnol
28 janvier 2026	Webinar COM en slovaque
29 janvier 2026	Webinar COM en polonais
29 janvier 2026	Webinar COM en italien
25 - 26 février 2026	Événement COM en anglais - Paris, France (hybride)
12 mars 2026	Date limite pour la soumission des réponses à la demande d'informations (RFI) sur la plateforme d'enquête de l'UE. (17:00 CET)
19 mars 2026	Publication du rapport sur la COM résumant les conclusions
20 mars 2026	Clôture de la COM

Funded by the European Union

Activités de la COM (étapes)

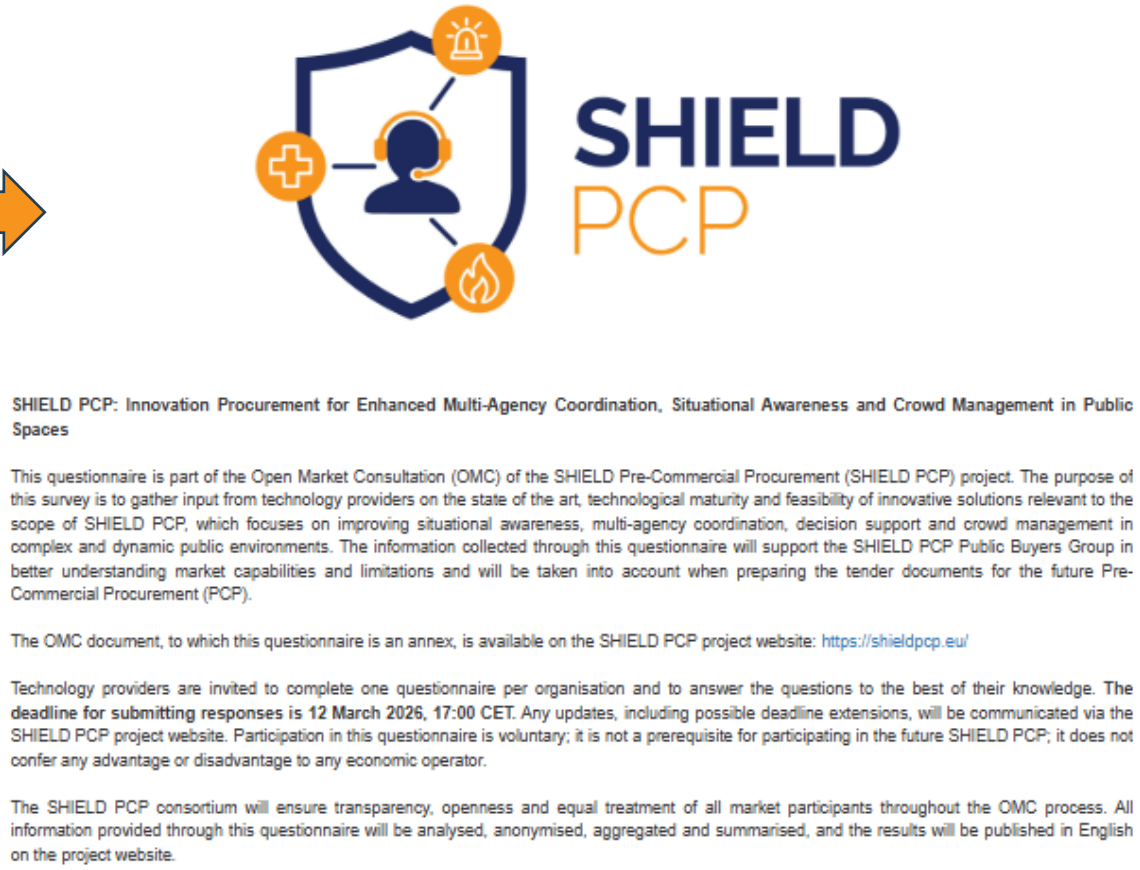
Avis d'information préalable sur la TED.	824607-2025 - Planification - TED
Le document sur la COM a été publié sur le site web du projet.	SHIELD PCP - Document COM
Les questionnaires demande d'informations (RFI) ont été publiés sur la plateforme d'enquête de l'UE.	https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire
Les webinaires COM sont prévus dans différentes langues.	
Les résultats (anonymes) seront publiés dans un rapport sur la COM	

Funded by the European Union

Questionnaire RFI

Veuillez accéder à l'enquête en cliquant sur le lien suivant : **https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire**

La date limite de réponse au questionnaire est fixée au 12 mars 2026.



SHIELD PCP
Request for Information Questionnaire

SHIELD PCP

SHIELD PCP: Innovation Procurement for Enhanced Multi-Agency Coordination, Situational Awareness and Crowd Management in Public Spaces

This questionnaire is part of the Open Market Consultation (OMC) of the SHIELD Pre-Commercial Procurement (SHIELD PCP) project. The purpose of this survey is to gather input from technology providers on the state of the art, technological maturity and feasibility of innovative solutions relevant to the scope of SHIELD PCP, which focuses on improving situational awareness, multi-agency coordination, decision support and crowd management in complex and dynamic public environments. The information collected through this questionnaire will support the SHIELD PCP Public Buyers Group in better understanding market capabilities and limitations and will be taken into account when preparing the tender documents for the future Pre-Commercial Procurement (PCP).

The OMC document, to which this questionnaire is an annex, is available on the SHIELD PCP project website: https://shieldpcp.eu/

Technology providers are invited to complete one questionnaire per organisation and to answer the questions to the best of their knowledge. **The deadline for submitting responses is 12 March 2026, 17:00 CET.** Any updates, including possible deadline extensions, will be communicated via the SHIELD PCP project website. Participation in this questionnaire is voluntary; it is not a prerequisite for participating in the future SHIELD PCP; it does not confer any advantage or disadvantage to any economic operator.

The SHIELD PCP consortium will ensure transparency, openness and equal treatment of all market participants throughout the OMC process. All information provided through this questionnaire will be analysed, anonymised, aggregated and summarised, and the results will be published in English on the project website.

Funded by the European Union

Questionnaire RFI (défis et critères)

PCP challenge and requirements

* 1- Are you aware of any existing or emerging technologies in the field of protection of public spaces and crowd management (as described in SHIELD PCP)?
  - ○ Yes
  - ○ No

* 2- Are you currently developing or have you developed any solution relevant to any of the following use cases? *(Tick all that apply and describe briefly)*
  - ☐ Use Case 1: Panic at football stadium.
  - ☐ Use Case 2: Drone Attack Match Day.
  - ☐ Use Case 3: Multi-actors coordination after a massive knife attack in a train station.
  - ☐ No solution was developed for any of the use cases above.

* 3- Which of the following capability areas do you consider most critical to address these scenarios? *(Select up to 3 options.)*
  - ☐ Real-time common operational picture (COP) and dashboards for commanders
  - ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
  - ☐ Counter-drone detection and neutralisation systems
  - ☐ AI-supported decision-making tools for incident management
  - ☐ Inter-agency communication and coordination platform
  - ☐ Multi-source data fusion and sensor integration
  - ☐ Evacuation support and crowd routing systems
  - ☐ Public alerting and communication to citizens (e.g. emergency messaging)

4- What are the safety mechanisms and fail-safe features your solution would include to avoid collateral damage or unintended consequences?

5- Do you identify any technical, operational or organisational barriers, gaps or missing needs in relation to the scope and requirements of SHIELD PCP?
  - ○ Yes
  - ○ No

6- Can your solution be modularised or integrated with external platforms or APIs (e.g., EMS, law enforcement systems)?
  - ○ Yes
  - ○ No

7- If you were to participate in the SHIELD PCP, please indicate your indicative time allocation (in months) for each of the following phases: *(Total should not exceed 23 months.)*

	Number of months
* Phase 1: Solution Design:	
* Phase 2: Prototype Development:	
* Phase 3: Validation & Demonstration:	

* Please briefly justify your estimated time:

8- If you were to participate in the SHIELD PCP, please provide your indicative budget allocation (in EUR) per PCP phase: *(Please be aware that there is a predefined budget allocation for this PCP project, and the total available budget will be divided across phases and participating contractors. For the purpose of this question, please assume a total indicative PCP budget of EUR 3,600,000.)*

	Amount of budget
* Phase 1: Solution Design (€):	
* Phase 2: Prototype Development (€):	
* Phase 3: Validation & Demonstration (€):	

This field is required.

* Please briefly justify your estimated budget distribution:

9- Do you feel that the use cases and requirements described (spanning common operational picture, crowd monitoring, geolocation tracking, communications, etc.) cover all the critical needs of the PCP challenge? Are there any significant challenges or needs that you believe are missing from our list?

* 10- Which of the listed requirements in Annex III do you anticipate being the most technically or operationally challenging to implement, and what makes them challenging? Please highlight any requirements you see as high-risk or particularly complex.

* 11- What do you anticipate will be the main cost drivers in developing and deploying an integrated solution for these scenarios? *(Select up to 2 options.)*
  - ☐ Specialised hardware (e.g. sensors, drones, cameras)
  - ☐ Software development (analytics, AI algorithms, user interfaces)
  - ☐ System integration of components and data sources
  - ☐ Communication infrastructure (networks, devices, radios)
  - ☐ Training and change management for end-users
  - ☐ Ongoing maintenance and support of the system.
  - ☐ Other

* 12- Which approach do you believe is more effective for delivering the solution sought in this PCP? *(Select one option.)*
  - ○ A single-vendor integrated platform (one provider/consortium delivering all components as a unified system)
  - ○ A modular solution (multiple specialised components from different providers, designed to interoperate)
  - ○ No strong preference / Either approach can work

13- How important is it that the solution uses open standards and interfaces to interoperate with existing systems and third-party components?
Reset to initial position

Not important — Very important

0 (0 — 5)

14- Can you provide any other recommendations regarding the SHIELD PCP solution(s)?
  - ○ Yes
  - ○ No

Questionnaire (Analyse de l'état-de-l'art)

State-of-the-art analysis

15- Do you think there is room for technological development beyond the state of the art?

- ○ Yes
- ○ No

16- What is the current Technology Readiness Level (TRL) of your solution(s) or their main components?
Please indicate the TRL for the relevant functional requirement groups described in the OMC document (Annex III), if applicable.

17- What are the main limitations of the current state of the art that your solution aims to address, and what improvements would it introduce compared to existing approaches would your solution introduce?

18- Do you rely on any patented technology or standards?

- ○ Yes
- ○ No

19- Are there existing patents or intellectual property barriers that could limit your solution's development or deployment?

- ○ Yes
- ○ No

* 20- Which of the following areas already have mature solutions available on the market (high readiness, e.g. TRL 8–9)? *(Select all that apply.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

* 20- Which of the following areas already have mature solutions available on the market (high readiness, e.g. TRL 8–9)? *(Select all that apply.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

* 21- In which areas do you see the least mature state-of-the-art, requiring the most innovation? *(Select up to 3 options that represent the biggest gaps.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

* 22- Which emerging technologies do you think could significantly enhance solutions for these scenarios? *(Select up to 3 options.)*

- ☐ Artificial Intelligence / Machine Learning
- ☐ Internet of Things (IoT) sensors and smart cameras
- ☐ 5G or advanced wireless communication networks
- ☐ Cloud computing and edge processing for real-time data
- ☐ Advanced drone technologies and robotics
- ☐ Big data analytics and predictive modelling
- ☐ Other

Funded by the European Union

Questionnaire RFI (Divers)

Miscellaneous

23- What additional information, requirements or clarifications (if any) would you need to make a well-founded plan for the development and/or deployment of a solution within SHIELD PCP

* 24- Would your organisation consider participating in the upcoming SHIELD PCP procurement (tender) as a solution provider? *(Select one.)*

- ○ Yes – we would likely participate
- ○ Maybe – we need more information/depends on conditions
- ○ No – unlikely to participate

* 25- Do you intend to participate as a single entity or as part of a consortium?

- ○ Single entity
- ○ Consortium

26- Could you please indicate the name of your proposed solution or innovation?

27- Could you please provide an image or visual representation of your proposed solution or innovation, if available?

Only files of the type png,jpg,jpeg,gif,bmp are allowed

Select file(s) to upload

* 28- Which modules or macro-functionalities does your proposed solution intend to address?

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ None

29- How would you describe your technology, and how does it relate to the SHIELD PCP requirements?

* 30- How would you describe the innovation level of your technology and its differentiation from the current state of the art? *(Please describe the innovation aspects of your solution, the state of the art in the market, and how your solution is differentiated.)*

* 31- What is the target market addressed, and who will use your technology? (*Please indicate which user groups your solution addresses.)*

- ☐ Public bodies (e.g., law enforcement agencies, civil protection authorities, cities, defence sector)
- ☐ Private-sector security operators (e.g., guarding services, event security management)
- ☐ Mixed public-private security operators (e.g., critical infrastructure operators, utilities)

Please provide additional details if needed:

32- What are the main technological, legal, ethical or operational risks and challenges associated with the development and deployment of your solution, and how could these be mitigated? *Please explain.*

33- How do you consider the interoperability of the solution?
Please describe how your solution addresses interoperability with existing systems, standards, platforms, or infrastructure.

* 34- Did you already take part in a European project, or has the development of your solution /technology been co-funded by the European Union? If so, please provide the name of the project, the Grant Agreement number and some further information.

* 35- How did you hear about the project SHIELD PCP?

- ☐ Project website (shieldpcp.eu)
- ☐ Tenders Electronic Daily (TED)
- ☐ European Commission / Horizon Europe communication channels
- ☐ Partner organisation or consortium member
- ☐ Social media (LinkedIn, X/Twitter, etc.)
- ☐ Event, workshop or webinar
- ☐ Email newsletter or mailing list
- ☐ Other (please specify)

36- Do you have any suggestions and/or remarks?

Funded by
the European Union

SHIELD
PCP

Session interactive
QUESTIONS ET RÉPONSES

Tous les participants

Modératrice : LOR Céline - SNCF

Méthodologie

Les pilotes seront présentés. Après chaque pilote, les participants seront invités à répondre à une courte série de sondages en direct via le chat.

Les sondages visent à déterminer comment les solutions du marché pourraient contribuer aux différentes étapes du scénario.

Environ **5 minutes** sont allouées par pilote.

Les résultats des sondages seront agrégés, anonymisés et reflétés dans le rapport final de l'OMC.

Funded by the European Union

Pilote 1 - Panique au stade de football

Funded by the European Union

Pilote 1 - Panique au stade de football

Où / Qui	• **Stade MŠK Žilina (Slovaquie)** • **Utilisateurs finaux : MOI, ISEMI** • **Soutien : Police nationale, FRS, sécurité du stade, police municipale, SAMU**
Problème principal	• Un match de football à haut risque dégénère en panique générale lorsque des ultras allument des obus fumigènes à l'intérieur du stade, provoquant des incendies, une visibilité réduite, des voies d'évacuation bloquées et des mouvements de foule incontrôlés.
SHIELD PCP Focus	• **Détection** précoce **des groupes et comportements suspects et des objets interdits** • **Identification des auteurs** avant et pendant l'escalade • Partage d'une **image opérationnelle commune (COP)** en temps réel entre les agences • Amélioration de la **coordination multi-agences** (police, FRS, EMS, sécurité) • **Surveillance des mouvements de foule** et détection des embouteillages • **Communication** ciblée **aux spectateurs** pour réduire la panique et guider l'évacuation

Funded by the European Union

Questions du sondage pour le scénario de panique dans le stade

Question 1 : Dans le scénario de panique dans un stade, à quelle étape votre solution pourrait-elle contribuer le plus ?

1. Détection précoce de comportements suspects ou d'objets interdits
2. Détection de l'aggravation de l'incident (fumée, incendie, visibilité réduite)
3. Connaissance de la situation en temps réel/image opérationnelle commune
4. Coordination multi-agences et aide à la décision
5. Suivi des mouvements de foule et conseils d'évacuation
6. Communication avec les utilisateurs finaux (spectateurs, personnel, intervenants).

Question 2 : Pour ce projet pilote, comment positionneriez-vous le plus probablement votre contribution ?

1. En fournissant une technologie ou un composant spécifique
2. Intégrer plusieurs technologies dans une solution
3. Fournir des capacités d'analyse ou d'aide à la décision
4. Soutenir le déploiement opérationnel et la validation
5. Nous étudions encore la manière dont nous pourrions apporter notre contribution.

Question 3 : En ce qui concerne ce scénario pilote, votre solution peut être décrite comme suit :

1. Déjà utilisée dans des environnements opérationnels comparables
2. Applicable avec adaptation ou intégration
3. Un composant qui prend en charge une partie du flux de travail
4. Encore en cours de développement ou conceptuelle

Funded by the European Union

Pilote 2 – Attaque de drones dans un stade

Funded by the European Union

Pilote 2 - Attaque de drones dans un stade

Où / Qui	• **Stade Metropolitano, Madrid (ES)** • **Utilisateur final : Policía Nacional** • **Support : LaLiga, SAMUR, 112, Police locale, Metro, EMT**
Problème principal	• Un match de football est perturbé par des **drones armés et incontrôlés**, provoquant des explosions, une panique générale et des mouvements de foule dangereux vers les sorties et les points d'accès au métro.
SHIELD PCP Focus	• Détection, suivi et neutralisation des **drones commerciaux et des drones armés** • **Réponse anti-drone résiliente** malgré la manipulation des fréquences radio. • **Image opérationnelle commune (COP)** en temps réel entre les agences • **Coordination multi-agences** par le biais d'un commandement et d'un contrôle unifiés • **Détection des mouvements de foule et gestion des flux d'évacuation** • **Communication sécurisée avec le public** pour réduire la panique et guider l'évacuation en toute sécurité

Funded by the European Union

Questions du sondage pour le scénario d'attaque par drone

Question 1 : Dans le scénario d'attaque par drone présenté, à quelle étape votre solution pourrait-elle contribuer le plus ?

1. Détection précoce des drones et classification (avant l'escalade)
2. Suivi des drones et évaluation des menaces pendant l'incident
3. Neutralisation / réponse contre les drones
4. Connaissance de la situation en temps réel / image opérationnelle commune (COP)
5. Coordination multi-agences et soutien au commandement
6. Gestion des foules et aide à l'évacuation

Question 2 : Pour ce projet pilote, comment positionneriez-vous le plus probablement votre contribution ?

1. Un composant technologique de base (par exemple, détection, analyse, contre-drone)
2. Une plateforme logicielle de soutien à la coordination ou à la connaissance de la situation
3. Un outil d'aide à la décision ou de commandement et de contrôle
4. Une solution de communication avec les foules ou d'aide à l'évacuation
5. une solution d'intégration de systèmes ou d'interopérabilité.

Question 3 : En ce qui concerne ce scénario pilote, votre solution est décrite comme suit :

1. Prête à être adaptée et testée dans un environnement opérationnel réel
2. Nécessite un développement plus poussé mais répond aux objectifs du projet pilote
3. Un élément de base qui pourrait être combiné avec d'autres solutions
4. Une approche expérimentale ou émergente pertinente pour les phases futures
5. Non applicable à ce projet pilote spécifique

Funded by the European Union

Pilote 3 - Coordination multi-acteurs après une attaque massive au couteau

Funded by the European Union

Pilote 3 - Coordination multi-acteurs après une attaque massive au couteau

Où / Qui	• **Gare du Nord (Paris-Nord), France** • **Utilisateurs finaux : FMI, SNCF** • **Soutien : Préfecture de Police (BRI, CCOS, SDRPT), Brigade des Sapeurs-Pompiers de Paris, DNPAF, Gendarmerie Nationale, Opération Sentinelle, SNCF & entreprises privées**
Problème principal	• **Des attaques simultanées** au **couteau** à l'intérieur de la gare et dans les rues avoisinantes provoquent le chaos parmi des milliers de voyageurs, nécessitant une compréhension rapide de la situation et une réponse coordonnée de plusieurs agences.
Objectif du SHIELD PCP	• **Compréhension rapide de la situation** grâce à la fusion de données multi-sources • Partage d'une **image opérationnelle commune (COP)** entre la police, les transports et les services de secours • **Coordination multi-agences** avec réduction du temps de latence dans la prise de décision • **Surveillance du comportement de la foule** et détection de l'affluence • **Gestion intelligente des flux d'évacuation** à l'intérieur des gares et des espaces publics • **Communication ciblée** aux voyageurs et au personnel pour réduire la panique et guider l'évacuation en toute sécurité.

Funded by the European Union

Questions du sondage

Question 1 : Dans le scénario d'attaque au couteau présenté, à quelle étape votre solution pourrait-elle contribuer le plus ?

1. Détection précoce de l'incident et premières alertes (rapports, capteurs, premiers signaux)
2. Compréhension rapide de la situation et fusion des données
3. Image opérationnelle commune (COP) à l'ensemble des agences
4. Coordination multi-agences et aide à la décision
5. Surveillance des foules et gestion des flux d'évacuation
6. Communication ciblée aux voyageurs et au personnel

Question 2 : Pour ce projet pilote, comment positionneriez-vous votre contribution ?

1. Une plateforme de base soutenant la coordination multi-agences
2. Une capacité ou un module spécialisé (par exemple, analyse, détection, communications)
3. Un composant de fusion de données ou de connaissance de la situation
4. Une couche d'interopérabilité ou d'intégration entre agences/systèmes
5. une solution complémentaire soutenant les outils existants.

Question 3 : En ce qui concerne ce scénario pilote, votre solution se décrit le mieux comme suit :

1. Principalement basée sur des logiciels (software)
2. Principalement basée sur le matériel (hardware)
3. Une solution combinée matériel-logiciel
4. Une solution axée sur les données / l'analyse / l'IA
5. Une solution orientée service ou support opérationnel

Funded by the European Union

Questions & réponses

Funded by
the European Union

SHIELD
PCP

Conclusions et prochaines étapes

CIVIPOL

Conclusions de la Consultation Ouverte du Marché (COM)

- SHIELD PCP vise à mieux comprendre les capacités, la maturité et le potentiel d'innovation du marché pour relever les défis liés à la coordination multi-agences, à la connaissance de la situation et à la gestion des foules dans les espaces publics.

- La consultation ouverte du marché est un processus exploratoire non contraignant conçu pour recueillir des informations structurées auprès des fournisseurs de technologies, des organismes de recherche et des innovateurs.

- Les contributions reçues par le biais du questionnaire de la demande d'information et des événements de la COM aideront le groupe des acheteurs publics à

  ✓ valider et affiner les exigences fonctionnelles

  ✓ Évaluer la faisabilité et l'état de préparation technologique

  ✓ Identifier les risques, les lacunes et les possibilités d'innovation

- La participation à la COM ne crée aucun avantage ou inconvénient pour les futures procédures de passation de marchés.

Funded by the European Union

Prochaines étapes

Le questionnaire RFI reste ouvert jusqu'au **12 mars 2026 (17:00 CET)**
→ Tous les participants sont encouragés à soumettre ou à finaliser leurs réponses

Le consortium SHIELD PCP va
→ Analyser et agréger les retours d'information reçus du marché.
→ Préparer et publier le **rapport sur la COM résumant les conclusions (mars 2026)**

Les résultats de la COM seront utilisés pour :
→ Finaliser la stratégie de passation de marchés.
→ Affiner les exigences techniques et fonctionnelles.
→ Préparer la documentation de l'appel d'offres du futur PCP

Toutes les mises à jour seront communiquées via le site web de SHIELD PCP et les canaux officiels

Funded by the European Union

Merci de votre attention !

HARTMANN Thierry
Commissaire général - Chef de projets innovation -
Direction de la coopération internationale de sécurité _ Ministère de l'Intérieur
Email :thierry.hartmann@interieur.gouv.fr

BEVILACQUA Alberto
Chargé de Mission Fournisseurs Stratégiques et Projets Européens
Direction de l'évaluation de la performance, de l'achat, des finances et de l'immobilier
Service de l'achat, de l'innovation et de la logistique - Ministère de l'Intérieur
Email : alberto.bevilacqua@interieur.gouv.fr

LOR Céline
Collaborative projects manager
SNCF – Direction de la Sûreté
Email : celine.lor@sncf.fr

SAIDI Leila
Responsable de projet
CIVIPOL
Email :leila.saidi@civipol.fr

SALGADO Emilie
Expert - Acheteuse
CIVIPOL
Email : emilie.salgado@experts.civipol.fr

BOUALI Youssef
CEO
DIGINNOV
Email : youssef.bouali@diginnov.eu

SHIELD PCP

contact@shieldpcp.eu

www.shieldpcp.eu

www.linkedin.com/company/shieldpcp

Funded by the European Union