MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

EXAMEN PROFESSIONNEL D'INGENIEUR PRINCIPAL DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2024 -

Lundi 26 juin 2023

Etude de cas à partir de deux dossiers techniques de trente pages maximum, soumis au choix du candidat le jour de l'épreuve écrite, permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

Durée : 4 heures

Sujet n° 1

Le dossier documentaire comporte 29 pages. (hors les 2 pages de l'énoncé du sujet).

Il vous est rappelé que votre identité ne doit figurer que dans l'en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettez en fin d'épreuve entrainera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A …, B…, Y…, Z…).

IMPORTANT

1. **Les copies seront rendues en l'état au service organisateur.**
   A l'issue de l'épreuve, celui-ci procédera à l'anonymisation de la copie.
2. **Ne pas utiliser de correcteur ou d'effaceur sur les copies.**
3. **Ecrire exclusivement en noir ou en bleu – Pas d'autre couleur.**
4. **Il est rappelé aux candidats qu'aucun signe distinctif ne doit apparaitre sur la copie.**

Sujet n°1

Gestion d'un événement sportif dans le cadre des J.O. 2024

Vous êtes ingénieur principal des systèmes d'information et de communication au sein de la direction zonale des systèmes d'information et de communication (DZSIC) d'un secrétariat général pour l'administration du ministère de l'intérieur (SGAMI).

Dans le cadre des JO 2024, un événement sportif se déroulera au sein d'un site qui accueillera une discipline phare d'un sport collectif.

Le préfet délégué à la zone de défense et de sécurité dans laquelle se déroulera cette discipline souhaite que le SGAMI de la zone considérée assure la maîtrise d'oeuvre du projet. Dans ce cadre, il aura la charge de la conception de l'infrastructure nécessaire pour permettre le bon déroulement de cette compétition.

En tant que chef de projet au sein de cette DZSIC, vous êtes chargé de proposer le système d'information du PC de commandement avancé de la préfecture (PCO), qui sera interconnecté via le réseau interministériel de l'Etat (RIE) avec les sites suivants :

- le centre opérationnel départemental de la préfecture (COD) ;
- le centre d'information et de commandement (CIC) de la direction départementale de la sécurité publique (DDSP) ;
- le centre national de commandement stratégique des JO 2024 du ministère de l'intérieur et des outre-mer (MIOM).

En tant que chef du projet il vous est demandé de rédiger une note à l'attention du préfet délégué à la zone de défense et de sécurité intégrant vos propositions selon les axes suivants :

- prendre en compte l'utilisation de la vidéosurveillance algorithmique au sein des systèmes d'information déployés pour cet événement ;
- assurer la continuité et l'interopérabilité des moyens de communication des forces de sécurité intérieure (FSI) déployés sur ce site ;
- assurer une sécurité accrue du système d'information déployé au sein des PCO et COD précités et prendre en compte les problématiques de cybersécurité et de résilience.

Vous pouvez envisager l'hébergement des diverses données collectées dans votre datacenter zonal (DCZ) et ainsi, prévoir l'architecture numérique correspondante.

De même, il vous est demandé de prendre en considération la réception et l'affichage de l'ensemble des flux vidéos de cette manifestation.

Enfin, vous décrirez dans votre note les différentes étapes de ce projet à mettre en œuvre d'ici l'été 2024.

Dossier documentaire

Document 1

Source : https://www.ssi.gouv.fr/actualite/jeux-olympiques-et-paralympiques-de-paris-2024-lanssi-dans-les-starting-blocks/

Jeux olympiques et paralympiques de Paris 2024 : l'ANSSI dans les starting-blocks

Paris et la France se préparent à accueillir du 26 juillet au 8 septembre 2024 les Jeux olympiques et paralympiques. Cet événement hors normes représente : **15 000 athlètes** venus de **206 nations**, **22 villes** qui accueilleront les épreuves, **40 sites de compétition**, **878 épreuves** dans **54 sports**, **20 000 journalistes** venus du monde entier, plus de **10 millions de spectateurs** et **4 milliards de téléspectateurs**.

En raison de leur portée médiatique mondiale, les Jeux olympiques et paralympiques de Paris 2024 sont susceptibles d'attirer l'attention de divers acteurs cyber malveillants qui pourraient chercher à profiter de l'événement pour acquérir une certaine visibilité et faire connaître leurs revendications, attenter à l'image et au prestige des compétitions comme à ceux de la France ou tout simplement chercher à obtenir des gains financiers par extorsion. Ces diverses menaces pesant sur les Jeux sont en outre amplifiées par la numérisation de ce type de manifestations en ce qui concerne l'organisation générale, le déroulement des épreuves, les aspects logistiques, les infrastructures ou encore la rediffusion des épreuves via différents médias.

Compte tenu de l'ampleur de la menace, la Première ministre a confié en juillet 2022 à l'ANSSI le pilotage de la stratégie de prévention des cyberattaques des Jeux.

À cette fin, le dispositif mis en place par l'ANSSI, en étroite collaboration avec les différentes structures impliquées dans l'organisation des Jeux – dont en particulier la Délégation Interministérielle aux Jeux Olympiques et Paralympiques (DIJOP), le ministère de l'Intérieur et des Outre-Mer (MIOM) et le comité d'organisation des Jeux olympiques et paralympiques (Paris 2024) – s'articule selon cinq axes principaux :

- parfaire la connaissance des menaces cyber pesant sur les Jeux ;
- sécuriser les systèmes d'information critiques ;
- protéger les données sensibles ;
- sensibiliser l'écosystème des Jeux ;
- se préparer à intervenir en cas d'attaque cyber affectant les Jeux.

Actions préventives de sécurisation

Avec le soutien de la Coordination Nationale pour la Sécurité des Jeux (CNSJ) du Ministère de l'Intérieur et des Outre-mer et de Paris 2024, l'ANSSI, a identifié une cinquantaine d'acteurs critiques pour la préparation et le bon déroulement des Jeux. Des actions spécifiques sont donc actuellement menées afin

de sécuriser leurs systèmes d’information, en particulier au travers d’audit de cybersécurité et d’accompagnements techniques.

Actions de sensibilisation

Un plan de sensibilisation au bénéfice de plusieurs centaines d’acteurs de l’écosystème des Jeux a été défini et sera mis en œuvre à la fin du 1er semestre 2023. Il permettra notamment d’informer sur la menace cyber à l’encontre des grands événements sportifs et de diffuser de nombreuses recommandations et bonnes pratiques de cybersécurité. Par ailleurs, un séminaire de sensibilisation sera organisé par l’ANSSI au début du 2e semestre 2023.

Entraînement

Plusieurs exercices de crise seront organisés en 2023 pour se préparer collectivement à réagir en cas de cyberattaques lors des Jeux. En complément, des exercices « clé en main » seront proposés par l’ANSSI aux acteurs de l’écosystème des Jeux souhaitant s’entraîner à partir d’un scénario adapté à son niveau de maturité. Ces outils seront disponibles à partir du 4e trimestre 2023.

Document 2

Source : https://www.interieur.gouv.fr/actualites/grands-dossiers/jeux-olympiques-et-paralympiques-de-paris-2024/jo-2024-mobilisation-du

JO 2024 : la mobilisation du ministère de l'intérieur et des outre-mer sera sans précédent

Grands dossiers **Publié le 13/03/2023** **Mis à jour le 14/03/2023**

À 500 jours des Jeux olympiques de Paris 2024, Paris et la France se préparent à accueillir la XXXIIIe olympiade de l'ère moderne du 26 juillet au 15 août 2024. Cet événement planétaire nécessitera une mobilisation totale et sans précédent du ministère de l'Intérieur et des Outre-mer.

Dans 500 jours précisément, la France accueillera un événement hors norme : **10 500 athlètes** venus de **206 nations, 40 sites de compétition** à protéger simultanément, dont la moitié en Ile-de-France et 7 dans Paris intramuros, **6 000 journalistes** venus du monde entier, une **dizaine de millions de spectateurs**, et **4 milliards de téléspectateurs**, sans compter les **22 villes** qui accueilleront des épreuves, jusqu'en **Polynésie française**…

Pour laisser place à la fête, la sécurisation de l'événement devra être optimale. Une règle prévaudra pour tous les Jeux : il n'y aura qu'un seul pilote des opérations. C'est le ministre de l'Intérieur et des Outre-mer qui est responsable de la coordination et de la stratégie nationale sur la sécurité. Le préfet de police aura la charge du déploiement opérationnel en Île-de-France.

Un engagement total du ministère

Le ministère de l'Intérieur et des Outre-mer a d'ores et déjà anticipé son organisation pour ce rendez-vous phare.

Les forces de sécurité intérieure seront en première ligne pour assurer la sécurité de l'événement, des spectateurs et des athlètes. La mobilisation prévue est évaluée à environ **30 000 policiers et gendarmes par jour**.

Les réserves des écoles de police et de gendarmerie - **7 000 effectifs**, et les réservistes – **8 500 effectifs** – seront mobilisés en renfort.

Décision a été prise de suspendre, le temps des Jeux, la distinction entre zones de compétence police et de gendarmerie. Cela permettra une organisation par missions.

L'engagement de **25 000 personnels de sécurité privée, des agents des polices municipales et des militaires des forces armées** sera nécessaire pour parfaire le dispositif global de sécurité.

Une gouvernance et une structure de commandement

Une gouvernance dédiée a été mise en place. Celle-ci est articulée autour de la Coordination nationale pour la sécurité des Jeux olympiques et paralympiques 2024 et des grands événements sportifs internationaux (CNSJ). Elle assure la coordination des différents services du ministère, représente le pôle sécurité auprès du délégué interministériel aux Jeux olympiques et paralympiques (DIJOP) et participe au comité de pilotage entre les organisateurs et l'État.

Un centre national de commandement stratégique (CNCS), outil interministériel, sera mis en place spécifiquement pour la coupe du monde de rugby et les JOP.

Cette structure temporaire sera activée entre septembre et octobre 2023 puis entre avril et septembre 2024 (relais de la flamme, jeux olympiques et paralympiques). Sous la conduite du ministre de l'Intérieur et des Outre-mer, le CNCS aura pour missions d'analyser, de synthétiser et de transmettre les informations reçues sur le déroulement des Jeux en terme de sécurité. Il pourra également assurer l'information des spectateurs de l'évènement, des membres de la famille olympique et plus généralement de la population dans tous les domaines pouvant avoir une incidence sur la sécurité de l'évènement.

Le ministère s'est également doté d'un Centre de Renseignement Olympique (CRO), un échelon de synthèse chargé d'intégrer les informations recueillies par les services composant la communauté française du renseignement.

L'appui des technologies de sécurité

Un investissement de près de **50 M€** est prévu pour le déploiement de caméras de vidéo protection, dont **400 nouvelles caméras** dans la capitale et au moins 500 dans les communes limitrophes.

Le ministère de l'Intérieur et des Outre-mer est également impliqué dans la lutte anti drones, placée sous l'autorité du ministre des Armées et du gouverneur militaire de Paris, en matière d'analyse de vulnérabilité des sites.

Le projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024, qui sera débattu à l'Assemblée nationale en séance publique **du 21 au 23 mars**, vise à renforcer la sécurisation des Jeux et protéger la population, en détectant plus rapidement et plus facilement les situations à risque, par un traitement des images par algorithme aux conditions d'emploi strictement encadrées et à usage expérimental. Il s'agit aussi de fluidifier le contrôle à l'entrée des sites de compétition et de célébration et de mieux coordonner les équipes mobilisées pour la sécurité dans les transports.

Plans zéro délinquance établis par les préfets

Les préfets mettent en place des plans « **zéro délinquance** » sur les lieux d'accueil des Jeux, qui se traduisent dans chaque département concerné par des opérations anti-délinquance ciblées. **5 500 opérations**, dont **3 500 en Ile-de-France** sont ainsi prévues. L'objectif est de lutter contre la délinquance générale, par exemple contre les vols d'appropriation, mais aussi contre les trafics, les commerces illicites, ou encore le non-respect des mesures d'hygiène et sanitaires. Ces plans prévoient des opérations quotidiennes jusqu'à la tenue des Jeux Olympiques.

En parallèle, des opérations de visibilité quotidiennes et hebdomadaires sont organisées dans les transports en commun qui desservent les sites olympiques, avec une priorité donnée aux gares et aux lignes de transport concernées.

Mobilisés pour une cérémonie d'ouverture historique

Pour la première fois de l'histoire des Jeux Olympiques, la cérémonie d'ouverture ne se tiendra pas dans un stade fermé mais le long de 6 kilomètres de berges de la Seine, entre les ponts d'Austerlitz et d'Iéna. Selon les projections, plusieurs milliers de spectateurs sont attendus sur les quais, dépassant largement le cadre traditionnel des stades olympiques.

A événement exceptionnel, mobilisation sans équivalent à ce jour : **45 000 policiers et gendarmes** seront présents pour assurer la sécurité de cette cérémonie d'ouverture !

Document 3

Nouvelle réglementation sur la captation d'images de drones dans un cadre administratif
Source : https://www.interieur.gouv.fr/actualites/actualites-du-ministere/nouvelle-reglementation-sur-captation-dimages-de-drones-dans-un-cadre-administratif

Nouvelle réglementation sur la captation d'images de drones dans un cadre administratif

Mis à jour le 02/05/2023 Actualités du ministère Publié le 20/04/2023

Depuis le 19 avril 2023, une nouvelle réglementation encadre la captation et l'utilisation d'images de drones par les forces de l'ordre à des fins de sécurité publique.

La loi relative à la responsabilité pénale et à la sécurité intérieure (RPSI) promulguée en janvier 2022 a permis d'autoriser les services de la police et de la gendarmerie nationales à recourir à la captation d'images au moyen de caméras installées sur des aéronefs, drones, hélicoptères, ballons captifs. Ce cadre législatif a été validé par le Conseil constitutionnel dans sa décision du 20 janvier 2022.

Déjà pratiquée dans de nombreux Etats européens et déjà autorisée aux services de Sécurité civile depuis la loi « sécurité globale », la possibilité de filmer de haut constitue un vrai progrès opérationnel.

La vision « grand angle » est en effet indispensable pour coordonner l'intervention des forces de l'ordre dans certaines circonstances, pour faire du secours aux personnes dans de grands espaces (montagnes, littoraux) ou encore la sécurisation de la circulation sur les axes routiers.

Des finalités strictement limitées par la loi

Cette loi encadre strictement l'usage de ces dispositifs pour la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés, par exemple lorsqu'il y a eu auparavant des agressions, vols, trafics d'armes pour ne citer que quelques exemples. Il est désormais aussi possible d'utiliser des caméras dans ce cadre administratif pour assurer la sécurité des manifestations et sur la voie publique dans un objectif de maintenir ou de rétablir l'ordre public, pour la prévention d'actes de terrorisme, pour la régulation des flux de transport, pour la surveillance des frontières ou encore dans le cadre des secours aux personnes.

Il s'agit de finalités de police administrative : il s'agit de prévenir, sécuriser et secourir, pas de collecter des preuves ou d'enquêter comme en procédure judiciaire.

Un usage entouré de nombreuses garanties

L'emploi des caméras installées sur des aéronefs doit être autorisé par une décision écrite et motivée du préfet, délivrée pour une durée de 3 mois maximum, renouvelable, sauf pour ce qui concerne les rassemblements de personnes sur la voie publique, pour lesquelles l'autorisation ne peut excéder la durée du rassemblement.

Il doit être strictement nécessaire à l'exercice des missions concernées et adapté au regard des circonstances de chaque intervention. De plus, la captation d'images ne peut pas être permanente ; il demeure interdit de capter du son, de recourir à de la reconnaissance faciale et de procéder à des rapprochements automatisés avec d'autres traitements de données personnelles.

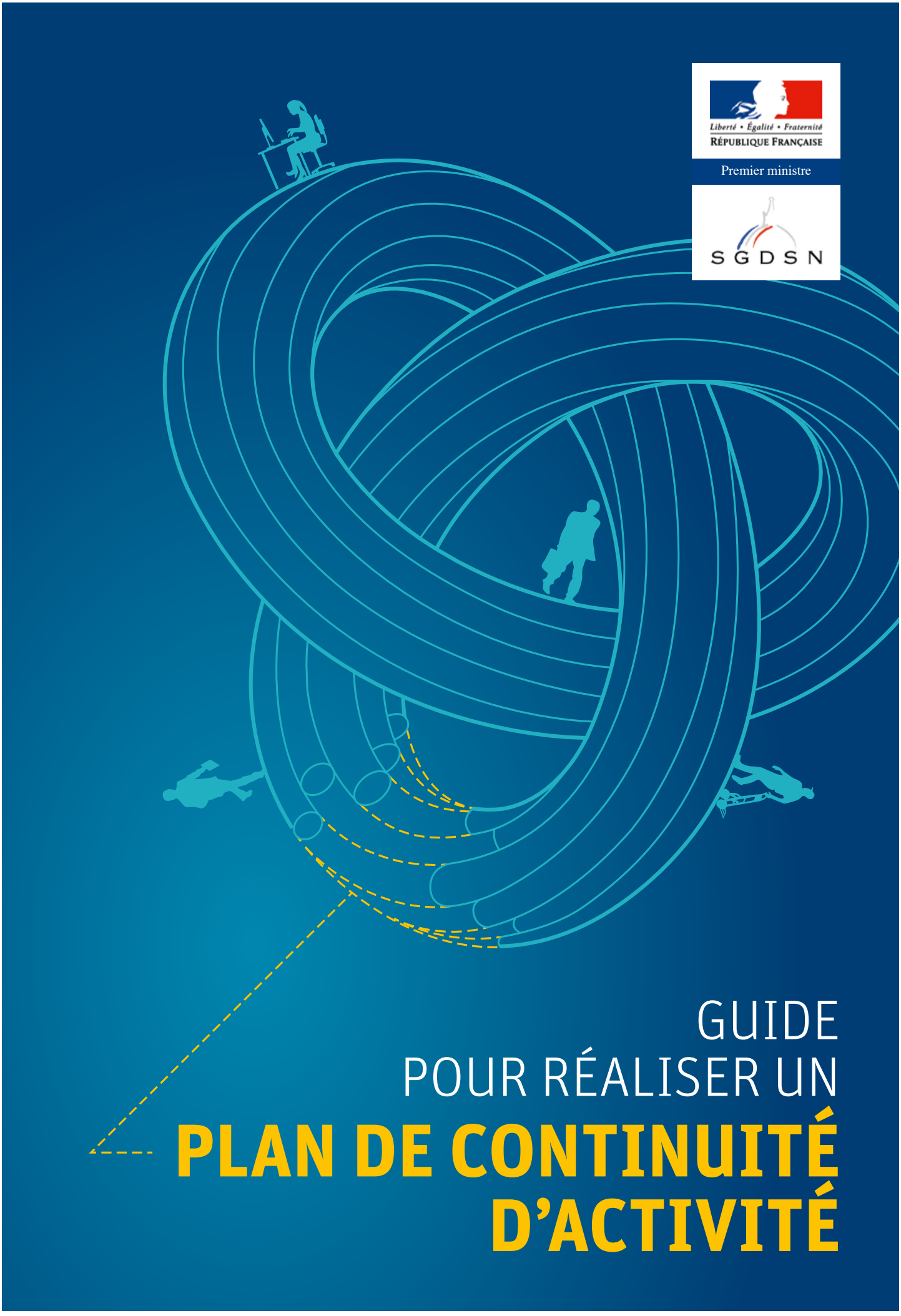
La captation par voie aérienne ne peut viser l'intérieur des domiciles.

Les enregistrements ne peuvent être conservés que pendant une durée maximale de 7 jours à compter de la fin du déploiement du dispositif, sauf procédure pénale, administrative ou disciplinaire. Le public est informé par tout moyen approprié de l'emploi de dispositifs aéroportés, sauf lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis. Le nombre maximal de caméras pouvant être simultanément utilisées dans chaque département est plafonné par un arrêté du ministre de l'Intérieur et des Outre-mer.

Ce cadre législatif a été précisé par un décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés (CNIL).

Dans la limite fixée par l'arrêté du ministre de l'intérieur et des outre-mer pour chaque département, il est désormais possible aux préfets d'autoriser les services de police et de gendarmerie d'avoir recours à ces dispositifs.

L'utilisation de ce dispositif permettra aux policiers et gendarmes en opération d'être plus efficaces dans les opérations menées, de mieux engager les moyens humains et d'avoir un usage optimal des moyens techniques dans le cadre d'un Etat de droit.



GUIDE POUR RÉALISER UN PLAN DE CONTINUITÉ D'ACTIVITÉ

LA DÉMARCHE PRÉSENTÉE PAR ÉTAPES

Sommaire interactif

1 POURQUOI ÉLABORER UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?

2 COMMENT ÉLABORER UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?

3 LES FICHES PRATIQUES

4 LES ANNEXES

IDENTIFIER ET FORMALISER LES BESOINS DE CONTINUITÉ

OBJECTIF

Pour maintenir l'activité au niveau exigé par les objectifs et obligations identifiés, les processus doivent répondre à des objectifs de sécurité, que l'on appelle « attentes » ou « besoins » et qui doivent être identifiés.

➡ À partir des discussions avec les responsables des métiers, il est possible de dégager des attentes, qui peuvent être sériées par critères, sous la forme D.I.C.T.E.S. :

• **Disponibilité,** continuité de service, régularité, résistance aux dysfonctionnements et aux ruptures, robustesse. Ceci doit pouvoir être mesurable, par exemple en termes de fiabilité des prestations.

• **Intégrité,** c'est-à-dire que le service/produit livré est bien celui attendu, dans l'état prescrit. Si ce n'est pas le cas, le service n'est pas rendu, conduisant à un arrêt (plus ou moins long) du service.

• **Confidentialité,** protection des informations sensibles. Une perte de confidentialité peut conduire à l'arrêt de certaines activités très sensibles, voire à la faillite de certaines organisations (cf. les cas présentés en annexe).

• **Traçabilité,** visibilité, connaissance des événements. La traçabilité peut être indispensable pour permettre d'assurer des prestations (par exemple le transport de matières dangereuses).

• **Évolutivité,** capacité à s'adapter aux changements et à l'environnement et donc à assurer la robustesse. L'absence d'évolutivité peut conduire à l'arrêt dans des contextes changeants.

• **Sûreté,** capacité à limiter les effets d'actes malveillants.

➡ **Lors de cette étape, il est souhaitable de quantifier le niveau du besoin de continuité, en utilisant trois indicateurs :**

1. **Le niveau de service minimum** (une perte de service qui maintient le fonctionnement au-dessus de ce seuil affecte peu le service final. A contrario une perte de niveau de service en dessous de ce seuil est considérée comme une indisponibilité). Ce seuil peut être défini comme un pourcentage de conformité minimum ou un pourcentage de produits/services commandés livrés à la date/heure convenue. Durant la phase de reprise d'activité après un sinistre, il est possible de définir des seuils plus faibles, en mode dégradé.

2. **Le niveau d'indisponibilité minimum.** Tout arrêt de durée inférieure à ce niveau est tolérable. Pour des indisponibilités de courtes durées et relativement fréquentes l'exigence est exprimée en durée maximale d'interruption et en fréquence maximale, ce qui se combine en pourcentage de temps d'indisponibilité pendant une durée significative. Pour ce qui concerne un sinistre, rare par définition, la mesure se fait par la durée maximale d'interruption de service acceptable (DMIA).

3. **Les ressources qui restent indispensables** pour permettre la reprise d'activité. Elles peuvent s'exprimer en quantité de stock à préserver, de locaux de repli, ou de niveau de mise à jour des données sauvegardées (ce qui revient à définir la perte de données maximale admissible, depuis la dernière sauvegarde).

Page suivante ➡

> Retour sommaire principal > Retour sommaire fiches pratiques

LE MAINTIEN EN CONDITION OPÉRATIONNELLE DU PCA

OBJECTIF

Identifier les points clés des contrôles à effectuer pour s'assurer que le PCA est opérationnel et le reste dans la durée.

➡ **Le PCA doit bien faire apparaître :**
- La hiérarchisation des priorités.
- L'organisation et le processus pour la prise de décision.
- Les moyens mobilisables.
- Les processus spécifiques au PCA.
- Les dispositifs et les ressources qui doivent être connus et rester disponibles.
- Les contrôles.
- Le dispositif d'amélioration continue.

Une fois le plan établi et validé, les ressources doivent être effectivement identifiées, les modifications indiquées doivent être effectuées, les procédures revues et intégrées dans les processus « métier », et les contrôles doivent être effectifs.

➡ **Le plan doit être vivant et faire l'objet de contrôles réguliers :**
- Vérifications périodiques.
- Entretien des dispositifs de secours.
- Tests des procédures de bascule.
- Exercices et entraînement (simulés ou réels).
- Tenue à jour du plan.
- Mesure du niveau de maturité.
- Révision des procédures et dispositifs.
- Retour d'expérience et exploitation des RETEX.

Rédaction de la documentation du PCA :
- Il est recommandé de disposer d'un outil de gestion documentaire pour gérer et entretenir la documentation.
- Il est recommandé qu'une copie (papier et/ou numérique) de la documentation soit stockée sur un site distant de l'organisation, dans un lieu sécurisé et accessible en fonction des scénarios.

➡ **Les exercices :**
Les exercices sont un moyen pertinent pour valider l'efficience et l'efficacité du PCA. Chaque exercice doit être pensé et organisé en fonction de ce que l'on veut vérifier. Il peut s'agir par exemple de vérifier :
- La procédure d'alerte (par un exercice sur table).
- Le fonctionnement de la cellule de crise (par un exercice simulé, avec activation de la cellule de crise).
- Les procédures techniques de basculement en mode secours (par la mise en œuvre réelle et périodique).
- La coordination des différentes parties prenantes, lors d'un exercice de réponse à un incident grave simulé.

Exercices de validation du PCA :
- Il est recommandé de s'assurer que la formation des personnels aux procédures techniques a bien été ciblée et réalisée avant de déclencher les premiers exercices.
- Il est recommandé de tester les éléments critiques du plan au moins une fois par an.
- Il est recommandé de tester régulièrement la procédure de récupération des sauvegardes et de s'assurer de son efficacité et de ses performances par rapport aux besoins de l'organisation.

Le contrôle documentaire et les rencontres avec les responsables de la mise en œuvre du PCA :
Il est possible de vérifier par un simple contrôle documentaire que les ressources, procédures et organisations prévues dans le PCA répondent bien sur le papier à ces objectifs. Il s'agit

Page suivante

Document 5

Lancement du projet "Réseau Radio du Futur" (RRF), le réseau très haut-débit souverain des services de sécurité et de secours

interieur.gouv.fr/actualites/communiques/lancement-du-projet-reseau-radio-du-futur-rrf-reseau-tres-haut-debit

Une des toutes premières missions de l'Etat est de protéger et de secourir la population, lors de situations de crise ou pour faire face aux menaces et accidents du quotidien (agressions, accidents de la route, incendies ...). Chacun de ces événements montre que la performance des outils de communication des services de sécurité et de secours est un élément essentiel de la protection des personnes et des biens.

Le Réseau radio du Futur (RRF) est la réponse de l'Etat pour moderniser les moyens de communication des acteurs de la sécurité et du secours. Aujourd'hui, les policiers, les gendarmes, les sapeurs-pompiers, les médecins du SAMU utilisent des équipements radio conçus au début des années 1990, propres à chaque force, et qui ne permettent pas la transmission d'importantes quantités de données ou d'images en temps réel depuis le terrain.

Avec le RRF, la France va se doter d'un réseau de communication très haut débit (4G

puis 5G) commun à l'ensemble des acteurs de la sécurité et du secours, leur permettant de communiquer instantanément les uns avec les autres en bénéficiant de nouvelles fonctionnalités : appels vidéo, partage de position en direct, envoi d'électrocardiogrammes etc. Le RRF prend en compte l'ensemble des utilisateurs participant au continuum de sécurité et de secours et permet de raccorder les agents sur le terrain aux salles de commandement. Il bénéficie d'une adhésion forte des acteurs auxquels il s'adresse, qu'il s'agisse des services de l'Etat ou de services relevant des collectivités locales.

De par son infrastructure très robuste, le RRF apportera à ses utilisateurs un réseau hautement résilient, garantissant la continuité et la sécurité des communications sur l'ensemble du territoire.

Par-delà ses enjeux opérationnels de protection de la population, le RRF est un véritable projet industriel qui fait de la France un acteur central dans le domaine stratégique des radiocommunications critiques à l'échelle mondiale. Avec un investissement de plus de 700 millions d'euros du ministère de l'Intérieur, il constitue une opportunité unique de consolider la filière industrielle française et d'en tirer les bénéfices en termes d'emplois - ainsi qu'à l'export - avec la structuration d'une offre crédible face aux autres acteurs mondiaux.

Avec la notification du marché de réalisation du RRF aux industriels retenus, le ministère de l'intérieur débutera la construction du futur réseau dès septembre 2022. La construction puis les tests d'une première version du RRF s'étendront sur une période de 19 mois, permettant de sécuriser la robustesse technique de la solution et son appropriation par les futurs utilisateurs.
A partir de 2024, le RRF deviendra l'épine dorsale des communications opérationnelles des services de sécurité, de secours et des acteurs de la gestion de crise.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Secrétariat général

Paris, le
Réf. : 21-023741-A

Le préfet, secrétaire général

à

Monsieur le préfet de police
Mesdames et messieurs les préfets
des Alpes-Maritimes, Bouches-du-Rhône, Charente, Charente-Maritime, Essonne, Gironde, Hauts-de-Seine, Haute-Garonne, Loire, Loire-Atlantique, Mayenne, Nord, Oise, Pas-de-Calais, Rhône, Seine-et-Marne, Seine-Saint-Denis, Val-de-Marne, Var, Vaucluse et Yvelines
Pour attribution

Mesdames et messieurs les préfets de région
Pour information

Objet : coordination territoriale du déploiement du dispositif « Réseau Radio du Futur » (RRF)
PJ : 3

Le programme Réseau Radio du Futur a été lancé en 2016 (à la suite des évènements tragiques de Paris, Saint-Denis et Nice) sous l'égide du ministère de l'Intérieur. Il vise à créer un nouveau système de communication mobile critique complet à usage de l'ensemble des forces de sécurité et de secours, dont vous aurez également l'usage au titre de votre rôle de coordination.

Le déploiement de cet outil se fera progressivement, par plaques territoriales, en direction des services de police et de gendarmerie nationales, des préfectures, des SDIS et des SAMU.

Votre département fait partie de la première vague de déploiement prévue dans 22 départements. Ce déploiement devra avoir été finalisé en 2023. Pour votre complète information, ont été retenus au titre de cette première vague :

- les départements qui accueilleront des événements sportifs au titre de la coupe du monde de rugby de 2023 et des Jeux olympiques de 2024 ;
- 8 autres départements, répondant à des enjeux de priorités stratégiques pour le ministère ou à des enjeux de continuité territoriale opérationnelle.

En tant que représentant de l'État, vous jouerez un rôle majeur dans la réussite de ce déploiement.

En effet, la stratégie de déploiement retenue nécessite une coordination forte des opérations au niveau départemental :

- pour s'assurer de la mobilisation effective de l'ensemble des entités utilisatrices de RRF et du bon avancement des travaux préparatoires à l'ouverture du service RRF ;

Place Beauvau
75800 PARIS Cedex 08
Standard : 01 49 27 49 27 – 01 40 07 60 60
Adresse internet : www.interieur.gouv.fr

- pour veiller à la cohérence des calendriers de préparation du déploiement des entités concernées ;
- pour vous associer, en fonction des options retenues au plan national, à la définition des doctrines d'emploi de RRF pour les besoins de communication en interopérabilité entre forces.

En tant que chef de file des politiques de sécurité, de prévention et de gestion des crises, je vous demande ainsi d'assurer, en lien avec la direction de programme RRF, la coordination des travaux et des acteurs territoriaux dans la préparation du déploiement de RRF et, en premier lieu, les forces de police et de gendarmerie nationales, le SDIS et le SAMU. Je vous invite à travailler en proximité avec celles des communes de votre département qui déploieront également RRF en 2023.

Pour les départements hôtes de la coupe du monde de rugby en 2023, les travaux de préparation du déploiement doivent être lancés dès le mois de septembre 2021. Ils concernent : les Alpes-Maritimes, les Bouches-du-Rhône, la Gironde, la Haute-Garonne, la Loire, la Loire-Atlantique, le Nord, le Rhône, Paris et la petite couronne.

Pour les autres départements déployés en 2023, les travaux de préparation du déploiement devront être lancés début 2022. Sont concernés : la Charente, la Charente-Maritime, l'Essonne, l'Oise, la Mayenne, le Pas-de-Calais, la Seine-et-Marne, le Var, le Vaucluse et les Yvelines.

La réussite du déploiement de RRF d'un point de vue technique repose pour partie sur le respect par les opérateurs de réseaux radioélectriques des engagements pris au titre du « *New Deal* mobile ». Je vous rappelle à ce titre le rôle que vous jouez dans la mise en place et l'animation des comités de concertation départementaux d'accès aux réseaux de communication électronique fixes et mobiles, et compte sur votre mobilisation pour en assurer le bon fonctionnement.

Les services des préfectures et des sous-préfectures seront également utilisateurs de RRF. La préparation du déploiement de RRF pour les besoins propres de la préfecture nécessitera principalement de recenser les services concernés par RRF pour identifier les besoins en équipements, de raccorder les centres opérationnels départementaux et les postes de commandement opérationnel à RRF, d'initialiser le système d'information RRF, d'organiser les formations et le support aux utilisateurs. A ce titre, je vous demande de piloter, avec le concours de la direction de programme RRF, la préparation du déploiement de RRF pour les besoins de vos services et d'identifier au sein de vos équipes un chef de projet RRF qui sera le point de contact privilégié des équipes de déploiement de la direction de programme RRF.

La direction de programme RRF et la DMAT (sous-direction de l'administration territoriale/bureau de l'organisation et des missions de l'administration territoriale) seront à vos côtés pour vous appuyer dans la préparation et l'organisation du déploiement.

A ce titre :

- la direction de programme RRF désignera un chef de projet qui sera votre interlocuteur de référence dans la conduite des opérations ;
- elle mettra à votre disposition les méthodes, outils et documents qui vous seront utiles pour préparer le déploiement, et qui seront construits en s'appuyant sur les retours d'expérience des travaux d'ores et déjà engagés sur les Bouches-du-Rhône et les Alpes-Maritimes.

Le préfet Guillaume Lambert, directeur de programme RRF, ainsi que ses équipes se tiennent à votre disposition pour avancer dans le déploiement au sein des départements concernés. La direction de programme prendra contact avec vous prochainement pour organiser une réunion de lancement et définir ensemble un plan de travail. Je vous remercie par avance de réserver le meilleur accueil à ses équipes.

Je compte sur votre engagement pour que nous soyons collectivement au rendez-vous du déploiement de RRF sur les départements prioritaires en 2023.

Pour le secrétaire général,
le secrétaire général adjoint
directeur de la modernisation
et de l'administration territoriale

Olivier JACOB

Annexe 1 : présentation des enjeux du déploiement du RRF

Une obsolescence des réseaux radios actuels et un décalage technologique devenu critique

Les réseaux radio bas débit équipant actuellement les services de sécurité et de secours ont été mis en œuvre progressivement depuis la fin des années 1980. Trois réseaux, bâtis sur la même technologie (TETRAPOL), sont actuellement en service en France :

- l'Infrastructure Nationale Partageable des Transmissions (INPT), utilisé par la police nationale, la gendarmerie pour une partie de ses terminaux, la sécurité civile, les sapeurs-pompiers (SDIS) et les SAMU, l'administration pénitentiaire , les douanes, le ministère des Armées et certaines polices municipales,
- RUBIS, utilisé par la gendarmerie nationale, la Marine Nationale, l'Office français à la biodiversité et quelques polices municipales,
- QUARTZ, réseau des services de sécurité et de secours dans les Outremers (Réunion, Mayotte, Antilles).

Ces réseaux proposent des fonctions qui ne répondent pas à tous les besoins des services de sécurité et de secours (à titre d'exemple, interopérabilité très restreinte, partage de données limité et de vidéo inexistant). On observe ainsi un décalage technologique entre les outils de communication professionnelle en mobilité mis à disposition des services de sécurité et de secours et les usages de la société s'appuyant sur des smartphones fonctionnant en 4G.

De la nécessité à répondre aux exigences opérationnelles du terrain en matière de service de sécurité et de secours

L'objectif du RRF est de bâtir, au profit des services en charge des missions relevant du traitement de l'urgence, tant dans le domaine de la sécurité publique que dans celui du secours aux personnes et aux populations, un système national de communication mobile prioritaire, sécurisé et haut débit 4G puis 5G bénéficiant d'un haut niveau de résilience en cas de crise et permettant de remplacer les actuels réseaux radio bas débit.

L'objectif fixé au programme RRF est de disposer d'un service de communication critique haut débit mobile opérationnel pour tous les services de sécurité et de secours au plus tard à compter de 2023 et d'être en service lors du déroulement de la coupe du monde de rugby. Les Jeux Olympiques de 2024 sont également un des jalons clés de la mise en service du RRF.

Le RRF intègre dans ses choix d'architecture, de contractualisation et de périmètre de services offerts, la volonté de valoriser et d'intégrer les actifs existants, notamment ceux de PCSTORM et de NEO2, pour ce qui concerne la police nationale et la gendarmerie nationale (PN/GN). Il prend également en compte le souhait exprimé par la police nationale et la gendarmerie nationale d'avoir le choix de recourir à l'offre générique des services du RRF ou de pouvoir choisir eux-mêmes leurs terminaux ou applicatifs, dans le respect du cadre de cohérence technique et d'inter-opérabilité du RRF, lequel vise à garantir de disposer d'un service interopérable entre tous les acteurs.

Réseau Radio du Futur : une réponse globale basée sur l'interopérabilité :

- **Un système complet de communication mobile haut débit, prioritaire, rapide, fiable, sécurisé et résilient** : aligné sur les technologies normalisées actuelles (4G) et évolutif dans le temps (permettant le passage à la 5G).
- **Une couverture radio importante par construction** : le RRF s'appuie sur les infrastructures haut débit de deux opérateurs mobiles.
    - Généralisation de la 4G sur l'ensemble des sites de chaque opérateur du programme RRF ;
    - Couverture de 100% des axes routiers prioritaires (55 000 km) en voix, SMS et très haut débit 4G par trois (3) des principaux opérateurs ;
    - 90% des lignes du réseau ferré régional (23 000 km) pour les titulaires de fréquences 1800 MHz ;
    - Couverture de 5 000 nouvelles zones par opérateur pour apporter un service de voix / SMS et très haut débit mobile (4G).

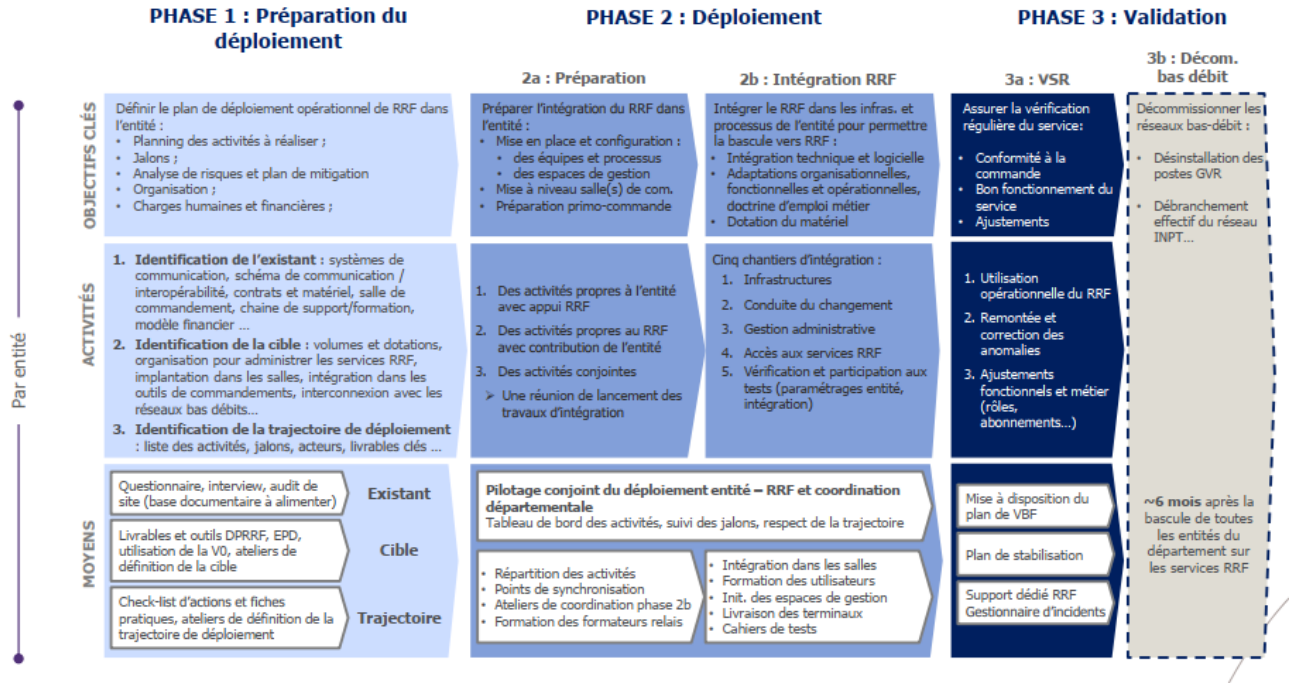
- **Une interopérabilité native et enrichie** : Le RRF doit également garantir une interopérabilité des communications en mobilité de l'ensemble des acteurs de la sécurité et du secours, qu'il s'agisse des services en charge de la sécurité publique, de la sécurité civile mais également des autres entités intervenant dans le champ du PPDR comme par exemple les SAMU, les douanes, l'administration pénitentiaire, les forces armées, les polices municipales, les associations agréées de sécurité civile ou certains opérateurs d'importance vitale.

- **Un réseau résilient** : une continuité des communications quelles que soient les circonstances :
    - une architecture basée sur 2 opérateurs permettant une redondance en cas de défaillance du premier,
    - un mécanisme de priorité/préemption prévu par les spécifications 3GPP,
    - une mise en place de capacités radio additionnelles et déployables mises en œuvre directement par les opérateurs ou sur la bande de fréquence 700 Mhz PPDR à la main des utilisateurs du RRF (relais véhiculaires).

- De nombreuses fonctionnalités grâce aux applications du RRF accessibles depuis les mobiles et les salles de commandement et adaptées aux besoins des différentes communautés métiers :
    - la possibilité de créer des conférences de groupe de façon dynamique, de transmettre des flux vidéo de situation, des photos ou d'autres documents et de converser en vidéo,
    - des outils complets de gestion et d'exploitation des communications en salles de commandement, notamment des outils permettant l'intégration de ces nouveaux flux de communication dans les systèmes de gestion opérationnelle des différentes entités utilisatrices du RRF. Une version « *standalone* » de l'application MCX RRF pour les salles de commandement permet également de bénéficier de l'ensemble des fonctionnalités proposées par le RRF sans intégration.

Annexe 2 : démarche de déploiement de RRF

La démarche de déploiement de RRF est organisée en 3 grandes étapes de préparation du déploiement (analyse des écarts avec la cible, définition et planification du plan de travail), de réalisation du déploiement (mise à niveau des pré-requis) et de validation (stabilisation post-démarrage et passage en fonctionnement courant).



La réalisation des phases 2 et 3 est estimée à 12-18 mois selon les entités et le niveau de complexité de leur environnement, ce qui nécessite une forte anticipation du lancement des travaux de préparation.

Organiser le déploiement de RRF nécessite donc :

1/ d'analyser l'existant et les écarts avec les modes de fonctionnement cibles du système RRF :

- Cartographier les moyens de communication mobiles opérationnels existants (architecture des systèmes de communication, des réseaux ...)
- Cartographier les salles de commandement et les équipements / moyens de communication dont elles disposent,
- Décrire l'organisation (acteurs, processus) pour la réalisation des missions de secours et de sécurité,
- Recenser les applications métier utilisées sur le terrain et en salle de commandement pour la réalisation des interventions,
- Cartographier les dispositifs en place pour assurer la formation et le support aux utilisateurs,
- Cartographier l'organisation en place pour la logistique des moyens de communication (configuration, livraison, SAV ...),
- Identifier toutes les particularités éventuelles de l'entité dans ses missions ou dans son organisation.

L'analyse des moyens de communication s'appuie sur un questionnaire adressé à chaque entité à déployer et sur un audit de chaque site, réalisé avec l'appui de la DPRRF, pour préparer la mise à niveau éventuelle des pré-requis techniques (raccordement RIE, couverture in-door, SSI ...).

- 2/ de **définir et planifier la trajectoire de déploiement de RRF**

- Définir et organiser les opérations de mise à niveau technique devant être réalisées en amont du raccordement à RRF,
- Définir les besoins en terminaux et accessoires, à partir du catalogue de l'offre RRF : besoins en dotation individuelle et en dotation collective ; une première estimation est à communiquer à la DPRRF au plus tôt, et dans tous les cas 6 mois avant la commande effective, pour consolider les prévisions de commande et en informer le fournisseur,
- Définir les besoins en relais véhiculaires,
- Evaluer les coûts d'abonnement de RRF pour l'entité au vu de la cible de déploiement visée,
- Identifier les administrateurs fonctionnels de RRF, qui seront les utilisateurs du système de gestion RRF, notamment pour la passation et le suivi des commandes, le suivi de la flotte de terminaux ...
- Définir le processus de support utilisateurs et la chaîne logistique des terminaux et accessoires (en tenant compte des processus en place), de manière à sécuriser l'articulation avec l'organisation mise en place par la DPRRF
- Définir les besoins en formation des utilisateurs : populations à former, modules de formation à mettre en place (identification des besoins éventuelles d'adaptation de l'offre de formation standard RRF), identification des formateurs relais ...
- Préparer la mise en conformité RGPD : production des analyses d'impacts protection des données (AIPD) et mise à jour du registre des traitements,
- Mettre à jour les doctrines d'emploi, en tenant compte des principes de fonctionnement de RRF et des nouvelles fonctionnalités apportées par le système ; un point essentiel sera la définition de doctrines d'emploi permettant l'interopérabilité entre les différentes forces ; ces doctrines d'interopérabilité seront définies au niveau départemental sous l'autorité du préfet, en respectant un cadre national préparé par la DPRRF en collaboration étroite avec les différentes communautés utilisatrices.

La planification des opérations de déploiement doit être assurée de manière à sécuriser la coordination des calendriers de déploiement de l'ensemble des entités à déployer sur le territoire. Cette coordination est assurée par le préfet avec le concours de la DPRRF.

3/ de **réaliser le déploiement opérationnel de RRF et son intégration au sein de chaque service**

- Réaliser les opérations de mise à niveau technique avant raccordement RRF,
- Raccorder les salles de commandement à RRF,
- Préparer et passer la première commande de terminaux et accessoires,
- Mettre en place la chaîne de support,
- Mettre en place la chaîne logistique terminaux et accessoires,
- Déclarer les abonnés dans le système RRF (provisioning) et alimenter le système de gestion RRF avec les données de l'entité à déployer,
- Former les utilisateurs.

Le démarrage de RRF est précédé de tests fonctionnels et techniques permettant de s'assurer du bon fonctionnement de RRF dans l'environnement de l'entité.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale
de la sécurité des systèmes d'information

Maturité SSI

Positionner son organisme en 12 questions

5 niveaux de maturité

La norme ISO/IEC 21827 définit 5 niveaux de maturité SSI. Ils représentent la manière dont une organisation exécute, contrôle, maintient et assure un suivi d'un processus :

1. Pratique informelle : pratiques de base mises en œuvre de manière informelle et réactive sur l'initiative de ceux qui estiment en avoir besoin
2. Pratique répétable et suivie : pratiques de base mises en œuvre de façon planifiée et suivie, avec un support relatif de l'organisme
3. Processus défini : mise en œuvre d'un processus décrit, adapté à l'organisme, généralisé et bien compris par le management et par les exécutants
4. Processus contrôlé : le processus est coordonné et contrôlé à l'aide d'indicateurs permettant de corriger les défauts constatés
5. Processus continuellement optimisé : l'amélioration des processus est dynamique, institutionnalisée et tient compte de l'évolution du contexte

Pourquoi se situer ?

Maîtriser ses coûts SSI

Le niveau de maturité SSI fixe les actions et outils correspondant aux réels enjeux de sécurité. Les dépenses SSI induites correspondront ainsi aux mesures nécessaires et suffisantes.

Adapter ses actions SSI

L'analyse des enjeux de sécurité justifie le niveau des mesures et définit les orientations par domaine SSI. Elle contribue à l'élaboration du plan d'action pour atteindre le niveau adéquat.

Se comparer aux concurrents

Le positionnement d'un organisme en maturité SSI lui permet de se comparer aux organismes du même secteur. Le positionnement par direction, par système d'information ou par processus relativise les priorités en terme de SSI.

Autodiagnostic éclair

Afin de situer le niveau de maturité à atteindre, les mêmes questions peuvent être posées pour un organisme, un service, un système, un projet…

Les conséquences potentielles

Adhérence au système d'information (SI) : comment jugez-vous l'importance de votre SI dans l'accomplissement de vos missions ?

0. Le système d'information est accessoire à l'accomplissement des missions
1. Le système d'information est utile à l'accomplissement des missions
2. Le système d'information est nécessaire à l'accomplissement des missions
3. Le système d'information est vital à l'accomplissement des missions

Niveau des impacts internes : quelles sont les conséquences internes (impacts financiers, juridiques, sur l'activité…) d'un sinistre SSI ?

0. Elles ne peuvent qu'être négligeables
1. Elles peuvent être significatives
2. Elles peuvent être graves
3. Elles peuvent être fatales

Niveau des impacts externes : quelles sont les conséquences externes (image, contrats, sécurité des personnes…) d'un sinistre SSI ?

0. Elles ne peuvent qu'être négligeables
1. Elles peuvent être significatives
2. Elles peuvent être graves
3. Elles peuvent être catastrophiques

Le niveau des conséquences potentielles est égal à la valeur maximale des trois réponses

La sensibilité du patrimoine

Besoins de disponibilité : quelle est l'importance de la disponibilité des SI ?

0. L'inaccessibilité des SI ne gêne pas l'activité
1. Elle perturbe l'activité de manière significative
2. Elle est jugée comme grave pour l'activité
3. Elle peut être fatale pour l'activité

Besoins d'intégrité : quelle est l'importance de l'intégrité des données dans le cadre de l'activité ?

0. L'altération des données ne gêne quasiment pas l'activité
1. Elle perturbe l'activité de manière significative
2. Elle est jugée comme grave pour l'activité
3. Elle peut être fatale pour l'activité

Besoins de confidentialité : quelle est l'importance de la confidentialité dans le cadre de l'activité ?

0. La compromission d'informations ne gêne quasiment pas l'activité
1. Elle perturbe l'activité de manière significative
2. Elle est jugée comme grave pour l'activité
3. Elle peut être fatale pour l'activité

La sensibilité du patrimoine informationnel est égale à la valeur maximale des trois réponses

Le degré d'exposition aux menaces

Fréquence des sinistres SSI : quelle est la fréquence estimée des sinistres SSI ?

0. Les sinistres SSI (vécus ou imaginables) sont rarissimes (moins d'une fois par an)
1. Plusieurs sinistres SSI dans l'année
2. Plusieurs sinistres SSI par trimestre
3. Plusieurs sinistres SSI par mois

Degré de motivation des attaquants : quel est le degré de motivation des attaquants potentiels ?

0. Une attaque SSI ciblée sur le périmètre est relativement inimaginable
1. Elle est jugée faible
2. Elle peut être forte
3. Elle peut être très importante

Moyens des attaquants : quels sont les moyens des attaquants potentiels ?

0. Les attaquants potentiels ne disposent que de faibles moyens
1. Ils peuvent disposer de moyens significatifs
2. Ils peuvent disposer de moyens importants
3. Leurs moyens sont potentiellement illimités

Le degré d'exposition aux menaces est égal à la valeur maximale des trois réponses

L'importance des vulnérabilités

Hétérogénéité du SI : quel est le niveau de variété du SI ?

0. Le SI est jugé comme homogène
1. Il est jugé comme faiblement hétérogène
2. Il est jugé comme fortement hétérogène
3. Il est jugé comme extrêmement hétérogène

Ouverture du SI : Quel est le degré d'ouverture du système d'information ?

0. Le SI n'est pas ouvert
1. Il n'est ouvert qu'à des systèmes internes
2. Il est ouvert à des systèmes externes mais sous contrôle
3. Il est ouvert à des systèmes externes hors de contrôle

Variabilité du SI : Quel est le niveau de variabilité des composants du système d'information (matériels, logiciels, réseaux, organisations, locaux, personnel…) et du contexte dans lequel il opère (contraintes, exigences réglementaires, menaces…) ?

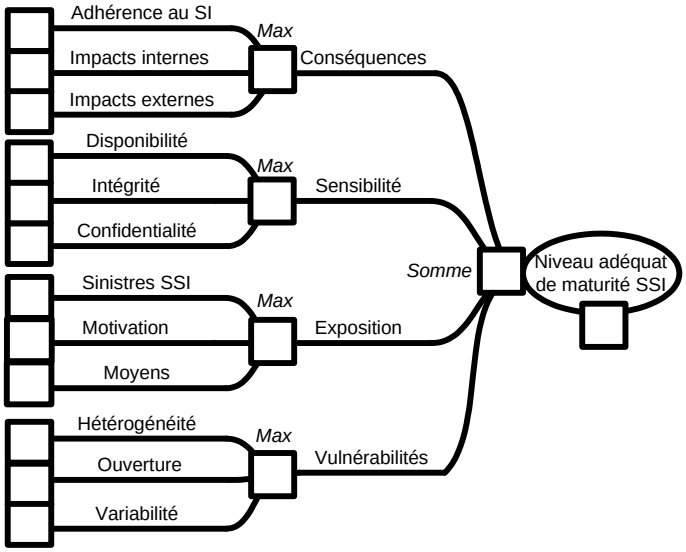
0. Le SI et son contexte sont jugés stables
1. Ils changent peu
2. Ils changent relativement souvent
3. Ils changent très souvent

L'importance des vulnérabilités est égale à la valeur maximale des trois réponses

Détermination du niveau adéquat

Le niveau adéquat de maturité SSI du périmètre choisi dépend de la somme des quatre valeurs que vous venez de calculer :

Somme	Niveau adéquat de maturité SSI
De 0 à 2	1 - Pratique informelle
De 3 à 5	2 - Pratique répétable et suivie
De 6 à 8	3 - Processus définis
De 9 à 10	4 - Processus contrôlés
De 11 à 12	5 - Processus continuellement optimisé



Informations et contacts

conseil.dcssi@sgdn.pm.gouv.fr
http://www.ssi.gouv.fr/fr/confiance/methodes

5. Outils de gestion de crise au sein du COD

La gestion territoriale de crise nécessite la mise en œuvre d'outils pratiques « traditionnels » (tableaux effaçables, des tableaux papiers, des annuaires, des plans, des cartes, téléphones, ordinateurs, télévisions, messagerie numérique, murs d'images, moyens de reprographie, moyens de visio-conférences, réseau…), spécifiques (portail ORSEC, SYNAPSE, SINUS (SIGNAL en 2023), report des systèmes de vidéo-protection de collectivités ou d'opérateurs…) et de sureté et de sécurité (ISIS, HORUS, TEOREM…). Chacun, en quantité comme en qualité, doit trouver sa place au sein des différents espaces du COD.

Cette liste non exhaustive d'outils de gestion de crise ne fait pas mention des outils « métiers » qui doivent être à disposition de certains services ou fonction en particulier.

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

**Direction générale
de la Sécurité civile
et de la gestion des crises**

Sous-direction de la préparation, de l'anticipation et de la gestion des crises
Bureau de la planification, des exercices et des retours d'expérience
DGSCGC/SDPAGC/BPERE/N°
Affaire suivie par : LcL Eric DUFÈS
Tél. : 01 45 64 46 05
Courriel : dgscgc-exo-planif@interieur.gouv.fr

Paris, le 20 mai 2022

Aide à l'organisation des centres opérationnels départementaux à la gestion de crise.

1. Objectifs et missions du COD

Le code de la sécurité intérieure, dans son article L. 115-1., dispose qu'« *en cas de situation de crise susceptible de dépasser la réponse courante des acteurs assurant ou concourant à la protection générale des populations ou à la satisfaction de ses besoins prioritaires définis à l'article L. 732-1, le représentant de l'État dans le département assure la direction des opérations* ». A ce titre, « *il met en place une organisation de gestion de crise* ». Dans ce cadre, il utilise le centre opérationnel départemental (COD), structure opérationnelle d'aide à la décision et, par voie de conséquence, de pilotage des ressources nécessaires à la gestion de la situation exceptionnelle ou de crise. L'organisation du COD est décidée par le préfet en charge de diriger la gestion interservices de crise, conformément aux dispositions du règlement intérieur opérationnel (RIO).

Aussi, le COD permet de rassembler dans un même lieu (cf. Annexe 1 - Figure 7) les représentants des différents services et acteurs concernés par le traitement d'une (ou plusieurs) situation(s) demandant une réponse opérationnelle.

Le COD a dès lors pour principale mission d'assurer le pilotage des différents services impliqués aux fins de coproduire des réponses opérationnelles et communicationnelles de crise. L'emploi du COD vise ainsi à répondre aux quatre objectifs principaux suivants et à exercer les activités qui s'y réfèrent :

1. Faciliter la prise de décisions par la mise en œuvre d'un processus décisionnel interservices adapté.
2. Piloter l'action collective des ressources publiques et privées nécessaires sur le territoire départemental.
3. Renseigner les échelons inférieurs et supérieurs.
4. Assurer la communication (interne et externe) de crise.

Pour parvenir à atteindre ces quatre objectifs principaux, il est primordial de disposer d'espaces suffisants permettant de coordonner les missions dévolues à chaque acteur.

Document 9

Source : https://www.bfmtv.com/tech/intelligence-artificielle/l-assemblee-nationale-valide-le-recours-controverse-a-la-videosurveillance-_AD-202303230433.html

L'Assemblée nationale valide le recours controversé à la vidéosurveillance algorithmique

Les députés ont adopté un article sur la vidéosurveillance "intelligente", dans le cadre du projet de loi olympique.

L'Assemblée nationale a approuvé jeudi 23 mars le recours à de la vidéosurveillance dite "intelligente", basée sur des algorithmes, que l'exécutif veut expérimenter avant et pendant les JO-2024, malgré les craintes de dérives sécuritaires de la gauche.

L'article 7 du projet de loi olympique a été adopté avec 59 voix pour (majorité présidentielle - LR - RN) face à 14 contre (Nupes). Il prévoit à titre expérimental que la sécurisation "de manifestations sportives, récréatives ou culturelles" d'ampleur puisse recourir à des algorithmes.

Expérimentation

Les JO sont en ligne de mire mais l'expérimentation, qui doit s'arrêter fin 2024, pourrait démarrer dès la promulgation de la loi, et concerner par exemple la prochaine Coupe du monde de rugby en septembre-octobre. Le but affiché: analyser les images captées par des caméras ou drones, pour détecter automatiquement des faits ou gestes potentiellement à risque.

La liste des "événements" à détecter doit être fixée par décret, après avis de la Commission nationale de l'informatique et des libertés (Cnil), qui avait appelé mardi 21 mars à ne pas introduire de reconnaissance faciale lors de l'examen de ce texte.

Lors des débats, le ministre de l'Intérieur Gérald Darmanin a cité en exemples "un départ de feu, des goulots d'étranglement de population, un colis ou un sac abandonné". Mais "pas les sweats à capuche", a-t-il assuré, pressé de questions par la gauche.

Les députés de la Nupes s'inquiètent du possible dévoiement de cette technologie, craignant que les JO ne servent que de tremplin pour généraliser par la suite ce type de surveillance à la population.

Absence de reconnaissance faciale

L'exécutif insiste sur les garde-fous, l'absence de reconnaissance faciale, et sur la nécessité de sécuriser les Jeux et les millions de spectateurs attendus. "Les événements prédéterminés concernent non pas des personnes mais des situations", a insisté Gérald Darmanin, sans les convaincre. Les associations de défense des libertés sont contre, comme le Conseil national des barreaux.

Les débats ont beaucoup tourné autour du caractère "biométrique" ou non des données, pour par exemple permettre d'isoler et suivre une personne. La majorité et le gouvernement assurent qu'elles ne revêtent pas ce caractère. "Ce seront forcément des données biométriques", a insisté Sandra Regol (écologiste).

Les députés de l'opposition ont tenté de circonscrire davantage l'expérimentation, de la cantonner aux abandons de bagage, ou d'imposer le fait que l'Etat soit seul responsable de l'analyse des données, sans recourir au privé, mais sans succès.

Un amendement du RN Aurélien Lopez-Liguori, président du groupe d'étude sur la sécurité et la souveraineté numériques, a été adopté. Il entend prioriser le recours à des entreprises européennes.

Mais le fait que des députés de la majorité, membres du groupe d'étude, ont cosigné ou sous-amendé un amendement RN, a indigné à gauche. "On est sur une dérive de cette majorité qui ne sait plus où elle va", a dénoncé l'écologiste Jérémie Iordanoff.

À deux ans des JO de Paris, des inquiétudes planent sur la cybersécurité

Clément Legros — Édité par Natacha Zimmermann — 27 juillet 2022 à 7h47

Alors que les Jeux olympiques de Paris approchent, les acteurs publics et privés du secteur de la sécurité informatique collaborent tant bien que mal.

Le président du comité d'organisation des Jeux olympiques et paralympiques de Paris 2024, Tony Estanguet, et la ministre des sports, Amélie Oudéa-Castéra, à Saint-Denis, le 31 mai 2022. | Franck Fife / AFP

Temps de lecture: 4 min

Paris a vu grand pour les Jeux olympiques et paralympiques (JOP) 2024. Encore faut-il réussir à sécuriser ses ambitions. Or, à deux ans de l'ouverture des JOP de Paris, les chiffres donnent le tournis: 7,3 milliards d'euros de budget, 13,4 millions de billets mis en vente, 600.000 spectateurs attendus pour la cérémonie d'ouverture sur les quais de Seine et près de 40 sites en Île-de-France et en régions. Et le risque cyber est partout. Billetterie, données personnelles, systèmes de retransmission vidéo ou de surveillance. Autant de risques d'attaques informatiques qu'il faut prévenir.

En 2016, les organisateurs des Jeux olympiques de Rio avaient relevé environ un demi-milliard d'attaques informatiques (soit 400 par seconde). Quatre ans plus tard, à Tokyo, c'est 815 attaques informatiques par seconde qui étaient enregistrées. Interrogé par l'AFP, le président du comité d'organisation des JO 2024, Tony Estanguet, confirme: *«On ne doute pas qu'on sera attaqués, en permanence. [...] Il ne faut aucune faille dans n'importe quelle entrée possible, au sein des collaborateurs, des logiciels, de l'écosystème.»*

«Il y a eu des moments de friction»

La menace cyber est multiple. Dans un rapport publié en 2021, l'Agence nationale de la sécurité des systèmes d'information (Anssi), acteur majeur de la sécurité informatique des JO de Paris, en dresse le panorama: elle peut être étatique, cybercriminelle, cyberterroriste ou activiste. Et selon Bertrand Le Gorgeu, coordinateur sectoriel pour les grands événements sportifs à l'Anssi, *«c'est la menace étatique qui est, de loin, la plus dangereuse»*.

Pour éviter un remake du fiasco de la finale de la Coupe de la Ligue 2022 au Stade de France, l'ensemble des services de sécurité et de prévention du ministère de l'Intérieur sont mobilisés. Au total, plus d'une dizaine de services sont engagés dans la définition de la stratégie de cyberdéfense des JO de Paris, placés sous l'égide du délégué interministériel aux JOP et de l'instance de coordination nationale pour la sécurité des Jeux olympiques et paralympiques 2024.

Mais d'après une source ministérielle au sein de la délégation chargée de superviser le bon déroulement des expérimentations des outils de cybersécurité, les débuts ont été marqués par de nombreux incidents: *«Il y a eu des moments de friction»*, explique notre source à plusieurs reprises. *«Jusqu'en juin, un grand nombre d'acteurs étaient absents de la discussion et le ministère n'avait pas encore diffusé l'ensemble des appels à manifestation d'intérêt aux industriels.»*

Chargé de mission auprès du ministère, l'expert en cybersécurité et renseignement en sources ouvertes ajoute: *«Il y a une certaine compétition entre les services du ministère de l'Intérieur. Chacun a ses méthodes, ses besoins et tous ne sont pas au même niveau en matière cyber. Des ajustements ont dû être réalisés.»*

Convoquée lundi 25 juillet par le président Emmanuel Macron à l'Élysée, une réunion olympique réunissant une dizaine de ministres, les préfets de police d'Île-de-France et le président du comité d'organisation des Jeux olympiques, Tony Estanguet, a permis de clarifier la chaîne de commandement. Le pilotage de la sécurité de l'événement appartient désormais au ministère de l'Intérieur.

La crainte d'une démobilisation

Placée sous le contrôle de la direction ministérielle aux partenariats, aux stratégies et aux innovations de sécurité, la phase d'expérimentation des technologies de cybersécurité a débuté en avril dernier. La filière industrielle s'y est préparée. Des comités industriels ont été mis en place pour répondre efficacement aux appels à manifestation d'intérêt diffusés par le gouvernement, dans le cadre de la stratégie globale de lutte contre les menaces cyber défendue par la Place Beauvau. Cette phase doit prendre fin en décembre 2022. À l'issue, un rapport sera communiqué aux autorités, en vue de l'acquisition des technologies retenues.

L'importance de tenir les délais est double: pour les industriels, le dédommagement financier de ces expérimentations s'achève au 31 décembre. Dès janvier 2023, l'acquisition des technologies retenues par l'État permettra alors leur test grandeur nature au cours des nombreux événements sportifs et culturels (à l'instar de la Coupe du monde de rugby 2023), qui se tiendront jusqu'au lancement des JO de Paris, prévu pour le 26 juillet 2024.

Contactée par Slate, une source interne au ministère de l'Intérieur assure que *«globalement, toutes les expérimentations devraient être achevées dans les temps»*. Mais les impératifs des différents services causent des ralentissements. Les congés d'été, les nombreux événements sportifs ou culturels de cette période et, surtout, la rentrée sociale à venir font craindre une démobilisation des forces engagées.

«Il va y avoir une rentrée sociale certainement chargée et les différentes forces de sécurité du ministère de l'Intérieur auront chacune d'autres choses à faire», explique notre source *«Tous ces évènements sont propices à ce que les forces ne soient pas toujours aussi disponibles qu'on le voudrait.»*

Péril budgétaire?

Les JO de Paris doivent permettre au cyber et à la sécurité numérique française de devenir *«une filière d'avenir»*. Malgré la présence de plusieurs acteurs internationaux dans l'organisation de ces Jeux olympiques, comme l'Américain Cisco ou le géant chinois Alibaba,

le ministère l'assure: *«Aucune technologie américaine ou israélienne ne sera sélectionnée»*. Les entreprises françaises seront privilégiées, dont 30% au moins de PME.

Dans le cadre du plan de relance mis en place par le gouvernement, 20 millions d'euros ont été débloqués par Bercy. Reste que la Cour des comptes ne cache pas ses craintes. En avril 2021 déjà, chargée d'étudier la gestion de l'organisation de Paris 2024, elle notait comme point positif l'augmentation des investissements en matière de sécurité. Mais la juridiction financière s'inquiète cependant des contours du système informatique déployé dans le cadre des JO français.

Dans un rapport provisoire de 76 pages, révélé par Le Canard enchaîné début juillet, la Cour des comptes renouvelle ses mises en garde. Elle affirme à nouveau qu'il est *«impératif»* d'accélérer la cadence pour relever le *«défi sécuritaire considérable»* que représentent ces *«menaces protéiformes»*.

La version définitive de ce document, qui a été récemment transmis aux autorités, sera publiée d'ici à la fin de l'année, avec les réponses des différentes parties prenant part à l'organisation. Mais selon les médias qui l'ont consulté, il dit déjà en creux la démesure d'un tel événement. La sécurité reste donc un dossier sensible pour les JO de Paris 2024, pour lesquels il faudrait employer 22.000 à 33.000 agents par jour, selon les estimations de la Cour des comptes.