REPUBLIQUE DU CAMEROUN

Paix - Travail - Patrie

MINISTERE DES POSTES ET TELECOMMUNICATIONS

REPUBLIC OF CAMEROON

Peace - Work - Fatherland

MINISTRY OF POSTS AND TELECOMMUNICATIONS

LA REALISATION DE L'ETUDE DE FAISABILITE EN VUE DE LA MISE EN PLACE D'UNE PLATEFORME NATIONNALE DE LUTTE CONTRE LA CYBERCRIMINALITE.

MARCHE N°0000002482/OS/MTP/SG/DAG/SDBM/SMA/2023 DU 20 JUIN 2023 RELATIF A LA LETTRE COMMANDE POUR LA REALISATION DE L'ETUDE DE FAISABILITE EN VUE DE LA MISE EN PLACE D'UNE PLATEFORME NATIONNALE DE LUTTE CONTRE LA CYBERCRIMINALITE, PASSE APRES APPEL D'OFFRES NATIONAL RESTEINT N° 0000012/AONO/MPT/CIPM/2022 DU 16 SEPTEMBRE 2022.

PLAN D'ACTION

KÍAMA

Le prestataire	L'Ingénieur du marché	Le Chef de Service de marché

Ce plan d'action est établi en conformité avec l'article 23 du marché.

SOMMAIRE

1- AVANT-PROPOS

Le présent document est confidentiel et sa confidentialité consiste à :

- La non divulgation des informations de configurations et paramétrages auprès de tierce partie ;
- La non reproduction des informations considérées confidentielles, sauf accord du Ministère des Postes et Télécommunications ;
- Les savoir-faire y contenus ne doivent profiter qu'au Ministère des Postes et Télécommunications ;
- Considérer toutes les informations déclarées Confidentielles.

2- Introduction et contexte

Contexte

A mesure que les technologies de l'information s'ancrent dans notre société, la cybercriminalité devient une menace commune à l'échelle mondiale. Avec plus de 4,5 milliards de personnes connectées, la moitié de la population mondiale est susceptible d'être victime de la cybercriminalité.

La pandémie de COVID-19 a accéléré la fusion des mondes physique et virtuel, et accru la dépendance à la connectivité pour la plupart de nos activités quotidiennes, tant professionnelles que personnelles.

L'environnement cybercriminel de plus en plus complexes et les difficultés inhérentes aux enquêtes exerçant une pression supplémentaire sur les services chargés de l'application de la loi.

Si le secteur privé a su se transformer, le secteur public reste confronté à des difficultés liées à une manque d'information, de stratégies, des ressources, d'infrastructure et de partenariats.

Il est essentiel que les services chargés de l'application de la loi reconnaissent que les mesures, pratiques et politiques actuelles ne suffisent probablement pas pour lutter contre la cybercriminalité, qui ne cesse d'évoluer, et déterminent les mesures à prendre pour combler ces lacunes.

Le secteur public doit s'améliorer en termes de préparation, d'efficacité et d'orientation en vue d'atteindre une cyber-résilience collective. La cybercriminalité est à la fois la responsabilité de tous et un objectif commun que nous devons sans cesse œuvrer à la réaliser.

Le monde est de plus en plus connecté et le MINPOSTEL entend continuer à jouer un rôle central et unique au sein des services chargés de l'application de loi en matière de lutte contre la cybercriminalité au Cameroun.

Nous sommes entrés dans une ère où les mondes physique et virtuel fusionnent, et où la transformation numérique accroit notre dépendance à la connectivité.

Les services chargés de l'application de loi du monde entier ont été les premiers témoins des tendances criminelles uniques nées de la pandémie de COVID-19, notamment à la diversification et l'intensification de l'impact de la cybercriminalité. Ce phénomène donne donc à repenser la stratégie nationale et à adapter le réseau national des services chargés de l'application de la loi.

Un rapport d'INTERPOL publié en aout 2022, qui étudie l'impact de la pandémie de coronavirus sur le contexte mondial des cybermenaces, a déterminé que les stratégies nationales de lutte contre la cybercriminalité permettaient d'accroitre la résilience des

infrastructure et services nationaux, de combattre efficacement les cybermenaces et de protéger les populations des cyberattaques pendant la pandémie et au-delà.

Objet du projet

L'étude de faisabilité pour la mise en place d'une plateforme nationale de lutte contre la cybercriminalité au Cameroun.

Consistance des prestations

Les prestations s'effectueront en deux phase et porteront sur :

Première phase : Etat des lieux et diagnostic.

Cette phase porte sur la collecte des données au Cameroun et le benchmark international sur les plateformes similaires.

Deuxième phase : Elaboration du plan directeur de mise en œuvre de la plateforme

Cette phase porte sur l'élaboration du plan directeur de mise en œuvre de la plateforme en se basant sur la solution technique, des mécanismes de mise en œuvre de la plateforme et le cadre de fonctionnel choisie par le Cameroun. Elle devra s'appuyer les résultats de la première phase pour consolider son étude à travers l'analyse et planification de projet de mise en œuvre de la plateforme.

3- Analyse de la situation et des lacunes

L'analyse de la situation a permis de faire les constats suivants :

1. Les termes de référence ne donnent pas de précision sur les pays à visiter dans le cadre de l'étude de Benchmark ;
2. L'encadrement des voyages dans le cadre de l'étude de Benchmark : existe-t-il des pays répondants aux critères d'étude de Benchmark avec lesquels nous avons des partenariats pouvant nous donner accès aux architectures de leurs applications de cybercriminalité ;
3. Les structures à visiter dans le cadre de Benchmark ne sont pas précisées dans le contrat.

   Afin de bien mener la mission, il importe de corriger ces manquements en communiquant à KIAMA SA des précisions sur les points ci-dessus.

4- Objectif et livrables.

Globalement l'objectif de ce projet est de disposer d'un document cadre destiné à la mise en place d'une plateforme nationale de lutte contre la cybercriminalité au Cameroun.

Les livrables :

Les livrables de ce projet sont :

- Le plan d'action conformément à l'article 23 du contrat
- Le document sur l'état des lieux et diagnostic des différentes cyberattaques enregistrées dans le Cameroun ces derniers années et des plateformes existant en matières de cyber sécurité.
- Document de plan directeur de mise en œuvre de la plateforme
- Rapport de séminaire de pré restitutions
- Rapport de séminaire de restitutions
- Rapport de missions
- Rapport de suivi du projet

5- Proposition d'une stratégie de mise en œuvre

Notre stratégie pour la réalisation de cette prestation est une démarche en deux phases :

Phase 1 : état des lieux et diagnostic

Nous allons dans cette phase mener les actions suivantes :

a. Collecte des données au Cameroun

- Collecter toutes les informations relatives sur les plateformes de lutte contre la cybercriminalité existante auprès des régulateurs (ANTIC, ART), les opérateurs des réseaux de communications électroniques (CAMTEL, MTN, ORANGE, NEXTTEL), les fournisseurs d'accès et de service internet, les services de sécurité (MINDEF, DGSN, SED, DGRE, INTERPOL) ;
- Identifier les lieux et sites d'hébergement de ces plateformes ;
- Évaluer le fonctionnement de ces plateformes ;
- Étudier les méthodes de collecte et de traitement des plaintes des victimes des cybercriminels de manière générale et à travers ces plateformes particulièrement ;
- Étudier l'interaction entre ces différentes plateformes ;
- Ressortir les limites de fonctionnement de ces plateformes et les méthodes existantes en matière de lutte contre la cybercriminalité.

b. Benchmark

En collaboration avec le maitre d'ouvrage, nous allons visiter la Cote d'Ivoire, le Sénégal et la France pour nous acquérir de leur solution technique de lutte contre la cybercriminalité. L'objectif de ces voyages d'étude permettront de consolider la collecte des données et de produire des résultats probants. Pour cela nous allons :

- Ressortir et présenter les architectures des plateformes déployées dans les pays visités ;
- Faire une analyse critique par rapport au contexte camerounais.
- Faire un diagnostic général sans complaisance relatif aux données collectées dans cette phase en rapport à la mise en place d'une plateforme de lutte contre la cybercriminalité au Cameroun.

c. Atelier de pré-restitution

Après la collecte, le benchmark, l'analyse et l'exploitation des données, nous allons procéder lors d'un atelier à une pré-restitution des résultats de la première phase. Durant cet atelier, nous présenterons les scenarios possibles de solutions techniques, des mécanismes de mise en œuvre de la plateforme et le cadre fonctionnel des différentes plateformes étudiées. Nous exposerons également sur les forces et les faiblesses de chaque solution et ferons une orientation stratégique pour le choix de la solution technique, tout en argumentant sur les raisons qui justifient ce choix pour le Cameroun.

Phase 2 : élaboration du plan directeur de la mise en œuvre de la plateforme

Dans cette phase, nous devrons poursuivre notre étude sur la solution technique, des mécanismes de mise en œuvre de la plateforme et le cadre fonctionnel choisi par le Cameroun. Nous allons nous appuyer sur les résultats de la première phase pour consolider notre étude.

a. Analyse et planification de projet de mise en œuvre de la plateforme

Pour cela nous allons :

- identifier et définir sur le plan national les parties prenantes les interactions entre eux ainsi que leurs rôles et responsabilités vis-à-vis de la plateforme ;
- faire une analyse situationnelle actuelle de l'environnement et les conditions de réussites d'une telle plateforme ;
- proposer une architecture contextualisée de la solution technique choisie en se basant sur les architectures des plateformes déployées et réussies dans les pays visités ;
- ressortir les contraintes pouvant exister pour la mise en œuvre de cette plateforme ;
- proposer le ou les institutions de tutelle de la plateforme ;
- proposer et définir les missions opérationnelles et stratégiques de la plateforme de lutte contre la cybercriminalité ;
- identifier les types de personnel, leurs profils, les types de formation, de compétences à acquérir ou à renforcer ;
- définir et proposer une architecture organisationnelle de la plateforme ;
- définir et décrire les profils des postes que devra occuper certains personnels de la plateforme ;
- proposer une architecture organisationnelle et de fonctionnelle de la plateforme en se basant ;
- proposer le modèle de gestion de la plateforme et son modèle économique ;
- proposer le lieu d'hébergement de la plateforme ;
- proposer un manuel de procédures de fonctionnement, d'utilisation et de sécurisation de la plateforme ;
- proposer un cahier de charge à soumettre aux différents intervenants concernés par la plateforme ;
- proposer un cahier de charge de mise en œuvre effective de la plateforme ;
- proposer un plan opérationnel d'intervention de la plateforme sur le cyberespace ;
- ressortir les limites légal et réglementaire relatives au fonctionnement de la plateforme ;
- proposer des projets de textes encadrant le fonctionnement de la plateforme ;
- Proposer les mécanismes et les sources de financement des activités de la plateforme ;
- estimer des coûts globaux de mise en place de la plateforme et le budget de démarrage ;
- proposer un chronogramme et le phasage du projet de déploiement de la plateforme.

b. Séminaire de restitution final

Afin de favoriser l'adhésion de l'ensemble des parties prenantes au projet, les résultats généraux de l'étude donneront lieu à une séance de restitution publique.

Nous allons organiser à cet effet, un atelier de présentation des résultats de l'étude à l'attention de l'ensemble des acteurs du secteur de la sécurité des réseaux et des systèmes d'information.

6- Prochaines étapes de suivi proposés

Nous proposons le découpage suivant en quatre étapes fondamentales pour le bon accomplissement de la mission :

1. **Activités préparatoires : Du 26 juin 2023 au 09 juillet 2023.**

Il sera question dans cette étape d'initier le lancement de la mission ; ceci se fera après la prise de contact des deux équipes projets (MINPOSTEL et KIAMA) puis l'élaboration d'un plan d'action qui sera présenté et discuté lors de la réunion de lancement.

2. **État des lieux et diagnostic**

Cette étape permettra de réaliser la première phase principale de notre étude ; elle comporte trois activités principales :

- **Collecte des données au Cameroun : 10 juillet 2023 au 30 juillet 2023**

Lors de cette activité, il sera question de :

  - Élaborer des questionnaires de collecte de données à adresser aux différents acteur cibles ;
  - Administrer les questionnaires
  - Analyser les données collectées pour produire une synthèse.

- **Réalisation du Benchmark : 10 juillet 2023 au 06 aout 2023**

Lors de cette activité, il sera question de :

  - Visiter deux (02) pays africains et un (01) pays européen ou asiatique avec des plateformes de lutte contre la cybercriminalité ;
  - Analyser les architectures des plateformes visitées en comparaison au contexte camerounais.

- **L'organisation de l'atelier de pré-restitution : 07 aout 2023 au 13 aout 2023**

Cette activité sera l'occasion pour nous de présenter les résultats de notre état des lieux et diagnostic afin de recueillir des commentaires et suggestions qui nous guideront dans la suite de l'étude.

3. **Élaboration du plan directeur de mise en œuvre de la plateforme : 07 aout au 10 Septembre 2023**

Ceci va se faire en deux temps :

Dans un premier temps, nous allons utiliser les résultats de l'étape précédente pour identifier les parties prenantes et définir leurs rôles puis pour proposer une architecture technique et organisationnelle de notre plateforme.

Dans un second temps nous allons élaborer le plan directeur de la plateforme.

4. Activités de clôture : du 11 septembre au 24 septembre 2023

Il sera question ici de rédiger le rapport final de l'étude et d'organiser un séminaire de restitution final.

7- Planning provisoire de réalisation du marché

		PHASE D'ÉVOLUTION DU PROJET (JOURS) *J0 = 26/06/2023*												
N°	**Activités**	**1 à 7j**	**8e à 14 j**	**15e à 21 j**	**22e à 28 j**	**29e à 35 j**	**36e à 42 j**	**43e à 49 j**	**50e à 56 j**	**57e à 62 j**	**63e à 69 j**	**70e à 76 j**	**77e à 83 j**	**84e à 90 j**
1.	**Activités préparatoires**													
1.1.	Prise de contact et préparation de l'étude													
1.2.	Élaboration du plan d'action du marché (confère l'article 23, page 8)													
1.3.	Réunion de lancement													
2.	**Phase 1 : état des lieux et diagnostic**													
2.1.	Collecte des données au Cameroun : • Élaboration d'une fiche de collecte des données • Collecte des données auprès des régulateurs, des opérateurs, des FAI et des services de sécurité • Synthèse													
2.2.	Benchmark • Visite de deux (02) pays africains et un (01) pays européen ou asiatique avec des plateformes de lutte contre la cybercriminalité • Analyse des architectures des plateformes visitées et comparaison au contexte camerounais													
2.3.	Atelier de pré-restitution • Présentation des résultats de la première phase, y compris les scénarios possibles de solutions techniques et les forces/faiblesses de chaque solution • Recueil des commentaires et suggestions des parties prenantes													
3.	**Phase 2 : Élaboration du plan directeur de mise en œuvre de la plateforme**													
3.1.	Analyse et planification de projet : • Identifier les parties prenantes nationales et définir leurs rôles et responsabilités dans la plateforme.													

	• Proposer une architecture technique et organisationnelle de la plateforme basée sur les résultats de la première phase													
3.2.	Élaboration du plan directeur • Définition des missions opérationnelles et stratégiques de la plateforme. • Établissement d'un manuel de procédures de fonctionnement, d'utilisation et de sécurisation de la plateforme. • Estimation des coûts globaux de mise en place de la plateforme et élaboration du budget de démarrage. • Proposition des mécanismes et sources de financement pour les activités de la plateforme • Rédaction des projets de textes encadrant le fonctionnement de la plateforme.													
4.	**Activités de clôture**													
4.1.	Préparation du rapport final de l'étude de faisabilité, y compris tous les résultats, les recommandations et le chronogramme de mise en œuvre de la plateforme													
4.2.	Séminaire de restitution final													

8- Mode opératoire

État des lieux et diagnostic

Collecte des données au Cameroun

Méthodes de collecte : interview et fiche de collecte

- Collecter toutes les informations relatives à la cybercriminalité dans les structures suivantes :

- **Des régulateurs :** ANTIC et ART
- **Les opérateurs des réseaux de communications électriques :** CAMTEL, ORANGE, MTN, NEXTTEL
- **Les fournisseurs d'accès et de service internet**
- **Les services de sécurité** : MINDEF, DGSN, SED, DGRE, INTERPOL

Plus précisément les informations concernant :

- *L'identité de ces plateformes de luttes contre la cybercriminalité*
- *Le rôle de chaque structure dans la lutte contre la cybercriminalité ;*
- *Les méthodes de lutte contre la cybercriminalité dans ces différentes structures ;*
- *Les lieux et sites d'hébergement de ces plateformes ;*
- *Le fonctionnement de ces plateformes ;*
- *L'architecture de ces plateformes*
- *Les méthodes de collecte et de traitement des plaintes des victimes des cybercriminels ;*
- *Les différents cyberattaque enregistrés ces dernières années*
- *Les interactions entre les différentes structures en matière de lutte contre la cybercriminalité*
- *Toutes autres informations relatives à la cybercriminalité*

Benchmark

Les trois pays pour le Benchmark sont : la Tunisie, la Côte d'Ivoire et la France.

Les structures à visiter dans chacun de ces pays sont les suivantes :

Les structures Etatiques de lutte contre la cybercriminalité en TUNISIE :

- **L'Agence Nationale de la Sécurité Informatique (ANSI)** : Créée en 2001, l'ANSI est chargée de la sécurité des systèmes d'information de l'Etat et des entreprises publiques. Elle est également chargée de la coordination et de la mise en place de la politique nationale en matière de sécurité informatique.

- **La Brigade Nationale de la Police Judiciaire (BNPJ)** : La BNPJ est une unité de la police nationale tunisienne chargée de la lutte contre la criminalité en ligne, y compris la cybercriminalité. Elle est responsable de la collecte d'informations, de l'analyse des données et de l'enquête sur les crimes informatiques.
- **Le Ministère de la Justice** : Le Ministère de la Justice est responsable de la poursuite judiciaire des cybercriminels. Il travaille en étroite collaboration avec les autres organismes et institutions étatiques pour identifier, enquêter et poursuivre les auteurs de crimes informatiques.
- **Le Centre National de Cryptologie (CNC)** : Le CNC est un organisme spécialisé dans la sécurité des systèmes d'information, notamment dans le domaine de la cryptologie. Il est chargé de la recherche et du développement de technologies de sécurité pour protéger les systèmes d'information contre les attaques informatiques.
- **Le Ministère des Technologies de la Communication et de l'Economie** Numérique : Le Ministère des Technologies de la Communication et de l'Economie Numérique est responsable de la réglementation et de la promotion de l'utilisation des technologies de l'information et de la communication en Tunisie. Il travaille également en étroite collaboration avec les autres organismes et institutions étatiques pour lutter contre la cybercriminalité.

Les structures Etatiques de lutte contre la cybercriminalité en Côte d'ivoire :

- **La Brigade de Recherche et d'Investigation (BRI) :** La BRI est une unité de la police nationale ivoirienne chargée de la lutte contre la cybercriminalité. Elle est responsable de la collecte d'informations, de l'analyse des données et de l'enquête sur les crimes informatiques.
- **Le Centre de Coordination et de Lutte contre les Cybercriminalités (CCLCC)** : Le CCLCC est un organisme spécialisé dans la lutte contre la cybercriminalité en Côte d'Ivoire. Il est chargé de la collecte d'informations sur les activités criminelles en ligne, de l'analyse des données et de la coordination des actions des différentes institutions étatiques impliquées dans la lutte contre la cybercriminalité.
- **Le Ministère de la Justice** : Le Ministère de la Justice est responsable de la poursuite judiciaire des cybercriminels. Il travaille en étroite collaboration avec les autres organismes et institutions étatiques pour identifier, enquêter et poursuivre les auteurs de crimes informatiques.
- **L'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI)** : L'ARTCI est chargée de la réglementation et de la supervision des services de télécommunications en Côte d'Ivoire. Elle travaille en étroite collaboration avec les autres organismes et institutions étatiques pour lutter contre la cybercriminalité.
- **La Cellule Nationale de Traitement des Informations Financières (CENTIF)** : La CENTIF est un organisme chargé de lutter contre le blanchiment d'argent et le financement du terrorisme en Côte d'Ivoire. Elle collabore également avec les autres organismes et institutions étatiques pour identifier et empêcher les activités criminelles en ligne, notamment la cybercriminalité financière.

Les structures Etatiques de lutte contre la cybercriminalité en France :

- **L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)** : créé en 2000, l'OCLCTIC est une unité spécialisée de la police nationale française. Il est chargé d'enquêter sur les infractions commises à l'aide des technologies de l'information et de la communication, telles que le piratage informatique, la fraude en ligne, le terrorisme en ligne, la pédopornographie, etc.
- **La Direction générale de la sécurité intérieure (DGSI)** : la DGSI est une agence de renseignement qui a pour mission de protéger les intérêts nationaux français contre les menaces terroristes, les activités d'espionnage et la cybercriminalité. Elle travaille en étroite collaboration avec l'OCLCTIC pour identifier, surveiller et neutraliser les groupes criminels et terroristes en ligne.
- **Le Centre de lutte contre les criminalités numériques (C3N)** : le C3N est une unité spécialisée de la gendarmerie nationale française. Il est chargé de lutter contre les infractions liées aux nouvelles technologies, notamment la cybercriminalité, le cyberharcèlement, la fraude en ligne, etc. Le C3N collabore également avec les autres organismes et institutions étatiques pour prévenir et détecter les menaces informatiques.
- **L'Agence nationale de la sécurité des systèmes d'information (ANSSI)** : l'ANSSI est une autorité administrative en charge de la sécurité des systèmes d'information en France. Elle est responsable de la protection des réseaux informatiques de l'Etat, des entreprises et des infrastructures critiques contre les cyberattaques. Elle collabore également avec les autres organismes et institutions étatiques pour renforcer la sécurité informatique en France.
- **Le Parquet national financier (PNF)** : le PNF est un organe judiciaire spécialisé dans la lutte contre la corruption, la fraude fiscale et la cybercriminalité économique. Il travaille en étroite collaboration avec les autres organismes et institutions étatiques pour enquêter, poursuivre et sanctionner les auteurs de crimes informatiques et économiques.

Collecte des données

- **Méthode de collecte** : interview

Les informations à collecter :

- *L'identité des différentes plateformes déployées pour la lutte contre la cybercriminalité*
- *Les parties prenantes les interactions entre eux ainsi que leurs rôles et responsabilité vis-à-vis de la plateforme*
- *L'architecture des plateformes déployé pour lutter contre la cybercriminalité*
- *Les institutions de tutelle de la plateforme*
- *Les missions opérationnelles et stratégiques de ces plateformes*
- *Les types de personnel, leurs profils, les types de formation, les types de compétences,*

- *L'architecture organisationnelle et fonctionnelle de ces plateformes*
- *L'hébergement de ces plateformes (comment ? et où ?)*
- *Procédures de fonctionnement, d'utilisation et de sécurisation de ces plateformes*
- *Les limites légales et règlementaire relative au fonctionnement de la plateforme.*
- *Les mécanismes et sources de financement des activités de la plateforme*
- *Les textes encadrant le fonctionnement de la plateforme*

Analyse et exploitation des données collectées

- *Ressortir et présenter les architectures des plateformes déployées dans les pays visités*
- *Faire une analyse critique par rapport au contexte Camerounais*
- *Faire un diagnostic général relatif aux données collectées en rapport à la mise en place d'une plateforme de lutte contre la cybercriminalité*

Organisation des ateliers de pré restitution

- *Présentation des scenarios possible de solutions techniques*
- *Présentation des mécanismes de mise en place de la plateforme et des cadres fonctionnels des différentes plateformes étudiées*
- *Présenter les forces et les faiblesses de chaque solution et faire une orientation stratégique pour le choix de solution technique et donner les raisons qui justifie ce choix pour le Cameroun.*

Élaboration de plan directeur de mise en œuvre de la plateforme

Analyse et planification du projet de mise en œuvre de la plateforme

- *Identifier sur le plan national les parties prenantes les interactions entre eux ainsi que leurs rôles et responsabilités vis-à-vis de la plateforme. ;*
- *Faire une analyse situationnelle actuelle de l'environnement et les conditions de réussites d'une telle plateforme ;*
- *Proposer une architecture contextualisée de la solution technique choisie en se basant sur les architectures des plateforme déployées et réussies dans les pays visités ;*
- *Ressortir les contraintes pouvant exister pour la mise en œuvre de cette plateforme*
- *Proposer le ou les institutions tutelle de la plateforme*
- *Proposer et définir les missions opérationnelles et stratégiques de la plateforme de lutte contre la cybercriminalité*
- *Identifier les types de personnel, leur profil, leur rôle, les types de formation, de compétence à acquérir ou à renforcer ;*
- *Définir et proposer une architecture organisationnelle de la plateforme ;*

- *Définir et décrire les profils des postes que devra occuper certains personnels de la plateforme ;*
- *Proposer une architecture organisationnelle et fonctionnelle de la plateforme ;*
- *Proposer le modèle de gestion de la plateforme et son modèle économique ;*
- *Proposer le lieu d'hébergement de la plateforme ;*
- *Proposer un manuel de procédures de fonctionnement, d'utilisation et de sécurisation de la plateforme ;*
- *Proposer un cahier de charge à soumettre aux différents intervenants concernés par la plateforme*
- *Proposer un cahier de charge de mise en œuvre effective de la plateforme*
- *Ressortir les limites légales et règlementaires relatives au fonctionnement de la plateforme*
- *Proposer un projet de textes encadrant le fonctionnement de la plateforme*
- *Estimer les couts globaux de mise en place de la plateforme et le budget de démarrage*
- *Proposer un chronogramme et le phasage du projet de déploiement de la plateforme*

Séminaire de restitution final

- *Organiser un atelier de présentation des résultats de l'étude à l'attention des acteurs du secteur de la sécurité des réseaux et des système d'information.*

ANNEXES

A1/ TERMES DE REFERENCES