COMMISSION
EUROPÉENNE

Strasbourg, le 15.12.2015
C(2015) 9206 final

ANNEX 1

ANNEXE

à la

RECOMMANDATION DE LA COMMISSION

portant adoption du manuel pratique pour la mise en œuvre et la gestion du système européen de surveillance des frontières (manuel EUROSUR)

Table des matières

1 Introduction

Le présent manuel propose des lignes directrices générales, techniques et opérationnelles ainsi que des recommandations et des meilleures pratiques relatives à la mise en œuvre et à la gestion du système européen de surveillance des frontières (Eurosur) créé par le règlement (UE) n° 1052/2013[1].

Ce manuel s'adresse aux États membres, à l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne («l'Agence») ainsi qu'aux autres organes et organismes de l'UE participant à Eurosur.

Ce manuel ne crée aucune obligation juridiquement contraignante pour les États membres, l'Agence ou les autres organes et organismes de l'UE et n'établit aucun droit ou devoir nouveau pour les autorités nationales responsables de la surveillance des frontières ou tout autre organisme à qui il s'adresserait. Seuls le règlement (UE) n° 1052/2013, sur lequel le manuel est basé, ou les autres actes législatifs auxquels il renvoie[2], peuvent produire des effets juridiquement contraignants et être invoqués devant une juridiction nationale.

Le manuel est régulièrement révisé à la lumière des expériences et des enseignements tirés de la mise en œuvre du règlement (UE) n° 1052/2013.

[1] Règlement (UE) n° 1052/2013 du Parlement européen et du Conseil du 22 octobre 2013 portant création du système européen de surveillance des frontières (Eurosur).

[2] Par exemple, le règlement (CE) n° 562/2006 du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) ou la Charte des droits fondamentaux de l'Union européenne.

2 Règles générales

2.1 Objectifs et cadre d'Eurosur[3]

Eurosur est un système polyvalent utilisé pour détecter, prévenir et lutter contre l'immigration illégale et la criminalité transfrontalière aux frontières extérieures, contribuant ainsi au développement de l'acquis de Schengen. Son but est de contribuer à assurer la protection des migrants et à sauver la vie de ceux qui tentent de franchir les frontières extérieures.

Pour atteindre ces objectifs, Eurosur fournit un *cadre* commun pour l'échange d'informations et la coopération entre toutes les autorités compétentes en matière de surveillance des frontières extérieures terrestres et maritimes[4]. Eurosur suit une approche axée sur le renseignement et l'analyse des risques, ce qui permet aux agences nationales et européennes de mieux comprendre la situation aux frontières extérieures et de réagir plus rapidement aux nouveaux itinéraires et méthodes utilisés pour l'immigration illégale et la criminalité transfrontalière. Ses éléments clés sont notamment l'échange d'informations quasiment en temps réel, l'échange régulier de renseignements et une coopération étroite entre les autorités aux niveaux national et européen.

Le *cadre Eurosur* se compose de plusieurs éléments[5] étroitement liés:

Au niveau national, les autorités coopèrent via les *centres nationaux de coordination* pour la surveillance des frontières et échangent des informations via les *tableaux de situation nationaux*. Au niveau européen, les centres nationaux de coordination échangent des informations entre eux et avec l'Agence via le *réseau de communication Eurosur*, avec un accès illimité au *tableau de situation européen* et au *tableau commun du renseignement en amont des frontières*.

L'Agence coopère également avec d'autres organes et organismes de l'UE (p.ex. le service européen pour l'action extérieure, Europol, Eurojust et l'Agence des droits fondamentaux) afin d'exploiter au maximum les informations, les capacités et les systèmes disponibles. L'Agence coordonne par exemple l'*application commune des outils de surveillance* en coopération avec l'Agence européenne pour la sécurité maritime et le Centre satellitaire de l'UE afin de fournir aux centres nationaux de coordination et à elle-même des renseignements sur les frontières extérieures et les zones en amont des frontières.

Eurosur permet aux États membres de réagir plus rapidement aux incidents ainsi qu'aux situations critiques qui surviennent aux frontières extérieures. Pour ce faire, les frontières extérieures terrestres et maritimes ont été divisées en «tronçons de frontière». Un niveau d'impact a été attribué à chacun de ceux-ci. Cette approche permet d'identifier les zones sensibles des frontières extérieures et, si nécessaire, de réagir de manière normalisée au niveau national et d'obtenir le soutien de l'Agence.

Pour atteindre les objectifs d'Eurosur, les États membres échangent également des informations et travaillent avec les pays tiers voisins sur la base d'accords et dans le cadre de réseaux régionaux spécifiques fondés sur ces accords.

[3] Articles 1 et 4 du règlement (UE) n° 1052/2013.

[4] Le cadre Eurosur peut également être utilisé pour la surveillance des frontières aériennes ainsi que pour les contrôles aux frontières si les États membres fournissent volontairement ces informations à Eurosur.

[5] Les centres nationaux de coordination, les tableaux de situation nationaux, le système de communication Eurosur, le tableau de situation européen, le tableau commun du renseignement en amont des frontières, et l'application commune des outils de surveillance (voir l'article 4 du règlement (UE) n° 1052/2013).

Lorsqu'ils échangent des informations et coopèrent dans le cadre d'Eurosur, les États membres et l'Agence doivent respecter les exigences relatives à la protection des droits fondamentaux, en particulier le principe de non-refoulement et la protection des données à caractère personnel.

2.2 Champ d'application[6]

Domaine	Dans les limites	Facultatif	Hors limites
Contrôle aux frontières (surveillance et vérifications)	• Surveillance des frontières extérieures terrestres et maritimes[7]	• Surveillance des frontières extérieures aériennes • Vérifications aux points de passage frontaliers	• Frontières intérieures
Surveillance des frontières	• Surveillance • Détection • Identification • Pistage • Prévention • Interception	-	Mesures légales et administratives après l'interception (p.ex. procédures d'asile, réadmission, retour, enquêtes judiciaires)
Connaissance de la situation[8]	• Événements, informations et analyses sur:[9] les franchissements non autorisés des frontières; la criminalité transfrontalière; les risques pour la vie des	la position, le statut et le type de moyens utilisés dans une mission de surveillance des frontières/de maintien de l'ordre sur les tronçons de la frontière	la position, le statut et le type de moyens militaires qui ne servent pas à faciliter une mission de maintien de l'ordre.

[6] Article 2 du règlement (UE) n° 1052/2013.
[7] Y compris les frontières extérieures temporaires.
[8] En ce qui concerne les frontières extérieures maritimes, Eurosur soutient le développement de l'environnement commun de partage de l'information (CISE) pour la surveillance de l'espace maritime de l'UE. Une fois établi, le CISE fournira un cadre plus large pour la connaissance de la situation maritime en favorisant les échanges d'informations entre les autorités publiques de divers secteurs, de la sûreté et sécurité maritimes au contrôle des pêches en passant par la protection de l'environnement marin, la douane, le contrôle aux frontières, l'application générale de la loi et la défense.
[9] Les dispositions figurant dans le présent manuel ne modifient en aucune façon les exigences définies pour les autorités nationales obligeant celles-ci à partager des informations via les autres systèmes dédiés basés sur la législation de l'UE (p.ex. les autorités douanières, via le système communautaire de gestion des risques en matière douanière, basé sur le règlement (CEE) n° 2454/93 de la Commission).

	migrants; • la position, le statut et le type de moyens des autorités nationales compétentes en matière de surveillance des frontières extérieures dans le tableau de situation national (NSP); moyens de l'Agence dans le tableau de situation européen (ESP) et le tableau commun du renseignement en amont des frontières (CPIP);	extérieure voisine d'un autre État membre;	
Capacité de réaction	• les franchissements non autorisés des frontières; • la criminalité transfrontalière;	-	la coordination des opérations de recherche et de sauvetage en mer
Données à caractère personnel	Données à caractère personnel relatives aux numéros d'identification des navires dans l'ESP/CPIP	Données à caractère personnel dans le NSP	tout autre donnée à caractère personnel figurant dans l'ESP/CPIP

2.3 Définitions - Aux fins du présent manuel, on entend par[10]*:*

1) «surveillance», l'observation d'une situation ou d'une zone géographique;

2) «détection», la prise de connaissance de la présence et de l'emplacement d'un objet d'intérêt;

3) «identification», l'établissement de l'identité unique ou des caractéristiques spécifiques de l'objet d'intérêt;

4) «pistage», la détermination de l'emplacement antérieur, actuel et futur d'un objet d'intérêt;

5) «prévention», les activités qui entravent ou empêchent la réalisation d'une action;

6) «mesures d'interception», désignent les mesures prises pour empêcher l'objet d'intérêt d'avancer;

[10] Voir l'article 3 du règlement (UE) n° 1052/2013. Les définitions relatives au traitement des informations doivent être utilisées conformément au modèle d'évaluation commune et intégrée des risques (CIRAM) v.2.0.

7) «autorités nationales», l'ensemble des autorités chargées de la surveillance des frontières extérieures terrestres et maritimes conformément au droit national et, le cas échéant, des contrôles aux frontières et de la surveillance des frontières aériennes;

8) «système national de surveillance des frontières», une structure unique ou une combinaison de systèmes de surveillance et de suivi rassemblant les activités de surveillance des frontières extérieures d'un État membre, sous la coordination du centre national de coordination conformément au droit national, et facilitant les échanges d'informations entre toutes les autorités nationales chargées de la surveillance des frontières extérieures;

9) «moyens propres», le matériel fixe ou mobile et les ressources humaines à la disposition d'un État membre ou de l'Agence pour surveiller les frontières extérieures et y patrouiller;

10) «statut des moyens», le niveau de préparation et la disponibilité des moyens;

11) «événement», un incident (situation ayant trait à l'immigration illégale, à la criminalité transfrontalière ou à un risque pour la vie des migrants), une situation de crise (par exemple dans un pays tiers voisin), ou toute autre situation ayant un impact significatif sur la sécurité des frontières;

12) «franchissements non autorisés des frontières», tout acte consistant à franchir la frontière aux points de passage frontaliers ou en dehors de ceux-ci en violation des règles relatives au franchissement des frontières extérieures établies dans le code frontières Schengen;

13) «données à caractère personnel», toute information concernant une personne physique identifiée ou identifiable («personne concernée»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

14) «traitement de données à caractère personnel», toute opération effectuée ou non à l'aide de procédés automatisés, appliquée à des données à caractère personnel, telle que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, la recherche, la consultation, l'utilisation, la communication par transmission, la diffusion ou tout autre moyen de mettre ces données à disposition, le rapprochement ou l'association ainsi que le verrouillage, l'effacement ou la destruction;

15) «pays tiers voisin», un pays tiers possédant soit une frontière terrestre ou maritime, soit un bassin maritime en commun avec un État membre.

2.4 Protection des droits fondamentaux et mesures contribuant à sauver la vie des migrants[11]

1. Les autorités nationales respectent les instruments internationaux et européens relatifs aux droits fondamentaux[12], et notamment l'acquis de l'UE en matière d'asile et le droit international des réfugiés. Elles respectent la dignité humaine des personnes impliquées dans l'immigration illégale et la criminalité transfrontalière et ne doivent pas introduire de discriminations fondées sur le sexe, la race, le milieu social ou l'origine ethnique, la langue, la religion ou les croyances, les opinions politiques ou autres, le handicap, l'âge ou l'orientation sexuelle. Toutes les mesures qu'elles prennent dans l'exercice de leurs fonctions doivent être proportionnées à leurs objectifs.

2. Lors de la collecte d'informations pendant les activités de surveillance des frontières, le droit à la vie privée et le droit à la protection des données à caractère personnel de toutes les personnes concernées doivent être respectés, conformément à la législation nationale et européenne.

3. Les autorités respectent leur obligation de porter assistance à tout navire ou personne en détresse en mer et, pendant les opérations de surveillance en mer, veillent à ce que leurs unités participantes satisfassent à cette obligation, conformément au droit international et dans le respect des droits fondamentaux. Dans le cadre de la coopération opérationnelle coordonnée par l'Agence, elles adhèrent aux règles établies par le règlement (UE) n° 656/201413.

4. Lorsque des individus, y compris des femmes enceintes ou des personnes blessées, malades ou déshydratées, ont besoin d'une assistance médicale, le centre de coordination responsable (le centre de coordination des opérations de sauvetage en mer, le centre de coordination local, régional ou national, en fonction de la situation) doit veiller à ce que les mesures nécessaires, notamment une demande d'aide médicale, soient prises dans les plus brefs délais. La sécurité de l'équipage et des personnes concernées est capitale et toutes les mesures doivent être prises afin de garantir cette sécurité à tout moment.

5. Les gardes-côtes et le personnel de toutes les autorités nationales compétentes sont formés à l'identification des enfants et des personnes vulnérables14, à la prise de contact avec ces personnes et à la manière de les aider à accéder aux mesures de protection ou d'assistance

[11] Article 2, paragraphe 4, du règlement (UE) n° 1052/2013.
[12] Notamment la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, la Charte des droits fondamentaux de l'Union européenne et la Convention de 1951 relative au statut des réfugiés et son protocole de 1967.
[13] Règlement (UE) n° 656/2014 du 15 mai 2014 établissant des règles pour la surveillance des frontières maritimes extérieures dans le cadre de la coopération opérationnelle coordonnée par l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne.
[14] P.ex. les femmes enceintes, les femmes avec des enfants en bas âge, les mineurs non accompagnés, les personnes susceptibles d'être exploitées et les victimes d'exploitation ou de la traite des êtres humains. Voir également le manuel intitulé «*VEGA Children Handbook*» (Frontex, 2015) et les lignes directrices relatives à l'identification des victimes de la traite des êtres humains, notamment à l'intention des services consulaires et des gardes-frontières (Commission européenne, 2013).

appropriées15. Le personnel reçoit des informations sur les mécanismes d'orientation nationaux16 et sur la manière de préserver les preuves d'infractions à la frontière en vue d'éventuelles futures procédures en justice.

6. Les autorités nationales veillent, en pleine conformité avec le principe de non-refoulement, à ce que les personnes qui demandent une protection internationale soient identifiées, reçoivent une assistance adéquate, soient dûment informées de leurs droits et sur la marche à suivre pour accéder aux procédures pertinentes (y compris la possibilité de demander l'asile) et soient rapidement orientées vers les autorités nationales responsables de la réception de leur demande d'asile.

7. Afin de contribuer à protéger et à sauver la vie des migrants en mer, il est nécessaire de mettre en place des canaux de communication nationaux et des flux de travail entre le centre national de coordination et le centre de coordination des opérations de sauvetage en mer (MRCC) afin d'assurer l'échange d'informations en temps opportun. Cet échange d'informations doit être réalisé en tenant pleinement compte du fait que le MRCC est seul responsable de la coordination des opérations de recherche et de sauvetage (SAR), dans le cadre du rôle que lui ont conférés les instruments juridiques internationaux propres aux opérations SAR17. Cet échange d'informations pourrait inclure:

   a) des informations sur le statut et la position des moyens de patrouille (importants pour les deux centres pour l'évaluation de leur capacité de réaction);

   b) des produits d'analyse des risques partagés par le centre national de coordination avec le MRCC, les flux migratoires pouvant potentiellement entraîner des risques plus élevés pour les vies en mer;

   c) le MRCC et le centre national de coordination peuvent se partager leurs capacités de pistage et de communications terrestres, y compris celles qui sont disponibles via l'Agence;

   d) l'information du MRCC sur les incidents ne nécessitant initialement pas d'actions SAR, mais susceptibles d'en avoir besoin ultérieurement, afin qu'il soit prêt à intervenir en cas de détérioration des conditions et de nécessité d'une action SAR. De même, le centre national de coordination doit être informé de tous les incidents SAR impliquant des migrants.

   e) Le centre national de coordination peut aider le MRCC à choisir le point de débarquement éventuellement nécessaire (la décision à ce sujet pendant les opérations SAR doit être prise par le MRCC). Cela peut être nécessaire pour permettre l'adoption

[15] Voir le chapitre 1.7 du tronc commun de formation.
[16] P.ex. pour les victimes de la traite des êtres humains et pour la protection des enfants.

[17] Convention internationale de 1979 sur la recherche et le sauvetage en mer et autres conventions internationales relevant de l'Organisation maritime internationale.

de dispositions supplémentaires (p.ex. des capacités administratives et d'hébergement au niveau local au point de débarquement).

Meilleure pratique: Le MRCC et le centre national de coordination concluent un accord formel relatif aux échanges d'informations, conformément aux règles applicables à la protection des données, afin de garantir une coopération harmonieuse. Cet accord peut notamment inclure le déploiement d'agents de liaison, l'échange de la liste de produits et de rapports, un accès éventuel aux systèmes informatiques de l'autre partie (en fonction du besoin d'en connaître et dans le respect des règles nationales sur la protection des données) ainsi que des réunions régulières entre les membres du personnel des deux centres, au niveau de la direction et au niveau opérationnel.

Les moyens de patrouille utilisés pour les opérations de surveillance des frontières doivent être équipés pour les opérations SAR.

8. Lorsqu'ils coopèrent avec un pays tiers voisin, les États membres doivent respecter leurs obligations au titre du droit européen et international, notamment le principe de non-refoulement et les règles en matière de protection des données. Ils ne peuvent partager des informations susceptibles d'être utilisées par le pays tiers pour identifier des personnes ou des groupes de personnes dont la demande d'accès à une protection internationale est actuellement examinée ou qui courent un risque grave d'être soumises à la torture, à des traitements ou des punitions inhumains ou dégradants ou à toute autre violation des droits fondamentaux.

Meilleure pratique: Le centre national de coordination crée une procédure opérationnelle standard pour le partage d'informations avec les pays tiers. Lors de l'utilisation de cette procédure, il conviendra de veiller à ce que les informations ne soient pas partagées lorsque le centre national de coordination sait ou devrait savoir qu'elles seront ou risquent d'être utilisées par le pays tiers pour violer des droits fondamentaux. Un journal électronique où figureraient la date, le nom du pays tiers et le type d'informations partagées pourrait être tenu.

3 Lignes directrices opérationnelles

3.1 Centre national de coordination[18]

3.1.1 Fonctions et tâches

Le centre national de coordination est chargé de la coordination et de l'échange d'informations entre toutes les autorités nationales responsables de la surveillance des frontières extérieures terrestres et maritimes, ainsi qu'avec les autres centres nationaux de coordination et l'Agence. La structure organisationnelle et le personnel des centres nationaux de coordination dépendent des circonstances nationales, notamment des niveaux d'impact attribués aux tronçons de frontière extérieure et de la manière dont le centre est intégré à l'autorité qui l'héberge. Les activités du centre national de coordination sont gérées par son chef. Ses fonctions et ses tâches sont décrites dans le tableau ci-dessous.

Fonctions	Tâches[19]

[18] Article 5 du règlement (UE) n° 1052/2013.

Gestion	Surveiller et superviser les activités du centre national de coordination, y compris le respect des droits fondamentaux; gérer et administrer le personnel du centre national de coordination; garantir la sécurité du centre national de coordination (personnel, bâtiment et TIC).
Connaissance de la situation et analyse des risques	Créer et diffuser le NSP; dans ce cadre, surveiller la situation opérationnelle à la frontière extérieure et collecter des informations opérationnelles et stratégiques; collecter, traiter, évaluer, valider, filtrer et réunir les informations sur la situation (incidents, moyens et renseignements[20]) au niveau national; traduire et créer des objets pour l'application du NSP; analyser les caractéristiques et les tendances de l'immigration illégale et de la criminalité transfrontalière; élaborer et gérer les exigences en matière de renseignement et créer des produits d'analyse des risques partagés par le NSP, l'ESP et le CPIP afin de faciliter la prise de décisions.
Capacité de réaction[21]	Surveiller la bonne mise en œuvre des activités opérationnelles au niveau local/régional et évaluation des performances nationales; dans ce contexte; veiller à ce que les autorités au niveau local/régional travaillent efficacement ensemble; évaluer la nécessité d'une assistance supplémentaire au niveau local/régional; évaluer les opérations nationales et les contributions aux opérations conjointes/bilatérales.
Liaison	Convenir d'arrangements de travail et de contacts avec les autorités nationales;

[19] Ces tâches peuvent être effectuées soit par le centre national de coordination lui-même, soit par d'autres autorités nationales ou organismes de l'autorité nationale hébergeant le centre, pour autant qu'ils travaillent en collaboration avec celui-ci.

[20] Par exemple, renseignement à base de source ouverte (OSINT), renseignement humain (HUMINT), renseignement par imagerie (IMINT) et renseignement par écoute des signaux (SIGINT).

[21] L'autorité nationale compétente est responsable du commandement et du contrôle des moyens et des ressources. Le centre national de coordination joue un rôle stratégique et de coordination et, en fonction de la répartition des responsabilités décidée au niveau national, il peut également jouer un rôle opérationnel.

	prendre contact avec le réseau des agents de liaison; bénéficier du soutien de l'Agence (point de contact national Frontex)/apporter son soutien à l'Agence.
Planification	Soutenir la planification et le renforcement des capacités en matière de gestion des frontières au niveau national; appuyer la planification des activités de surveillance à long terme.
TIC	Utiliser, contrôler, soutenir, entretenir et développer les systèmes informatiques.
Disponibilité	Le personnel du centre national de coordination assure la disponibilité opérationnelle de celui-ci 24h sur 24, 7 jours sur 7 (p.ex. pendant les postes de nuit); contacter la direction en cas d'urgence; créer et maintenir à jour des listes de contacts téléphoniques et des listes de contrôle.

Le personnel des centres nationaux de coordination doivent posséder des compétences linguistiques suffisamment développées pour pouvoir travailler avec les centres de coordination voisins et les autres centres nationaux de coordination. Le centre national de coordination doit disposer d'une capacité de traduction en interne ou en externe suffisamment importante pour pouvoir garantir des échanges d'informations en temps opportun.

Lorsqu'un État membre accueille une activité opérationnelle coordonnée par l'Agence (p.ex. une opération conjointe), il peut faire usage des infrastructures fournies par le centre national de coordination ou les centres qui y sont subordonnés.

3.1.2 Autorités nationales responsables de la surveillance des frontières[22]

Afin de coordonner leurs activités, les représentants des autorités nationales chargées de la surveillance des frontières extérieures terrestres et maritimes collaborent ensemble de manière permanente au sein du centre national de coordination.

Le centre national de coordination peut également fournir des informations sur la surveillance des frontières aériennes ainsi que sur les contrôles aux points de passage frontaliers si les États membres en décident ainsi. Dans ce cas, il est recommandé que les représentants des autorités nationales responsables de la surveillance des contrôles aux frontières et des contrôles aériens travaillent également au sein du centre national de coordination.

Le centre national de coordination peut inclure des agents de liaison d'autres autorités nationales ou organes pertinents, en fonction des besoins.

3.1.3 Coopération avec les autres autorités nationales[23]

En fonction de la répartition des responsabilités au niveau national et sans préjudice de ses obligations au titre de la législation régissant ses activités, le centre national de coordination

[22] Article 5, paragraphe 3, point a), et article 2, paragraphe 2, du règlement (UE) n° 1052/2013.
[23] Article 5, paragraphe 3, point b), du règlement (UE) n° 1052/2013.

échange des informations et coopère régulièrement, via les canaux appropriés, avec les autorités nationales suivantes:

a) gendarmerie maritime;

b) police/gendarmerie;

c) autorités douanières[24];

d) garde nationale;

e) forces armées;

f) centre de coordination des opérations de sauvetage en mer (MRCC);

g) autorités compétentes en matière de migration;

h) autorités compétentes en matière d'asile.

Le centre national de coordination peut échanger des informations et coopérer, via les canaux appropriés, avec d'autres autorités nationales, y compris:

a) l'autorité maritime;

b) l'autorité de contrôle des pêches;

c) les agents de liaison détachés à l'étranger;

d) les services vétérinaires/phytosanitaires;

e) le parquet;

f) le service consulaire du ministère des affaires étrangères, les ambassades et les consulats;

g) le bureau SIRENE;

h) les autorités responsables de la prévention de la prolifération nucléaire;

i) les autorités de transport;

j) les services de la protection civile;

k) les services de protection de l'environnement;

l) les services de renseignement;

[24] Voir l'article 4, paragraphe 3, du règlement (CEE) n° 2913/92 ainsi que l'article 3 et l'article 5, paragraphe 1, du règlement n° 952/2013 du Conseil (code des douanes de l'Union, applicable à compter du 1er mai 2016). Compte tenu du rôle qu'elles jouent dans la supervision de la circulation des marchandises franchissant les frontières extérieures et de leurs responsabilités en matière d'analyse et de gestion des risques, les autorités douanières peuvent désigner des représentants pour travailler au sein du centre national de coordination.

m) les autorités responsables des mécanismes d'orientation des victimes de la traite des êtres humains et des systèmes de protection des autres groupes vulnérables, tels que les enfants;

n) les autorités sanitaires.

3.1.4 Gestion des ressources et du personnel[25]

Le centre national de coordination soutient la gestion efficace des ressources et du personnel par les autorités nationales responsables de la surveillance des frontières extérieures. Ce faisant, le centre appuie la planification et la mise en œuvre des activités de surveillance des frontières, notamment

a) en élaborant et en tenant à jour un *aperçu de tous les moyens disponibles* appartenant aux autorités nationales responsables de la surveillance des frontières, y compris leur niveau de préparation, leur type et l'utilisation qui en est faite dans le cadre de la couche «opérations» du tableau de situation national;

b) en veillant à ce que les moyens disponibles au niveau national soient alloués aux tronçons de frontière correspondant aux niveaux d'impact qui leur sont attribués.

   Cela peut supposer de réaffecter les moyens fournis par l'autorité nationale d'un tronçon de frontière à un autre, ou en affectant des moyens supplémentaires fournis par une autre autorité nationale en vue de renforcer les mesures de surveillance prises pour un tronçon de frontière donné.

   Pour ce faire, le centre national de coordination veille à ce que les flux de travail et les dispositions nécessaires soient en place pour permettre la réaffectation rapide des moyens, avec l'accord des autorités nationales compétentes;

c) en contribuant au renforcement des capacités de surveillance des frontières et, le cas échéant, de vérification aux frontières, en collaborant étroitement avec les autorités nationales compétentes. Cela peut impliquer de recenser les lacunes et les besoins relatifs

   - aux informations collectées à partir de différents systèmes, capteurs, patrouilles et autres sources;
   - aux compétences et aux outils nécessaires à l'analyse des informations;
   - aux moyens fixes ou mobiles;
   - aux effectifs disponibles et à leur profil;
   - à la formation, y compris celle du personnel du centre national de coordination;

d) en soutenant la planification, la mise en œuvre et l'adaptation des opérations aux niveaux local, régional et national ainsi qu'au niveau de l'UE, en coopération avec l'Agence. Cela peut inclure des questions telles que la communication, l'achat de matériel interopérable ou encore une stratégie nationale de contrôle aux frontières.

[25] Article 5, paragraphe 3, point c), du règlement (UE) n° 1052/2013.

3.1.5 Tableau de situation national[26]

Le centre national de coordination crée et tient à jour le NSP en traitant et en évaluant les informations sur la situation, en gérant le processus national de renseignement et en élaborant des produits d'analyse conformément aux dispositions du chapitre 3.2 du présent manuel. Le centre national de coordination partage régulièrement des informations avec les autorités nationales compétentes via le NSP.

3.1.6 Planification et exécution des activités de renseignement nationales[27]

Le centre national de coordination soutient la planification et la mise en œuvre des activités de surveillance nationales en contrôlant les activités de surveillance aux niveaux local, régional, national et européen et formule des suggestions sur l'adaptation des pratiques en fonction de l'expérience acquise.

3.1.7 Système national de surveillance des frontières[28]

Chaque État membre possédant des frontières extérieures terrestres et/ou maritimes crée et tient à jour un système national de surveillance des frontières, composé d'une structure unique ou d'une combinaison de systèmes nationaux de surveillance et de contrôle. Les activités de surveillance mises en oeuvre à chaque tronçon de frontière extérieure correspondent au niveau d'impact attribué à ce tronçon (voir le chapitre 3.3.6) grâce aux équipements et patrouilles fixes et mobiles.

Le centre national de coordination coordonne le système national de surveillance des frontières conformément au droit national en contrôlant le fonctionnement du système, y compris les niveaux d'impact attribués et les procédures opérationnelles, et apporte sa contribution à l'élaboration du système et des procédures.

Le centre national de coordination possède un accès direct et en temps réel aux éléments pertinents du système national de surveillance des frontières, y compris aux sous-systèmes mis en place au niveau local/régional et aux systèmes de surveillance gérés par les autres autorités nationales. Si le centre national de coordination reçoit des informations sur un tronçon de frontière émanant de deux systèmes nationaux de surveillance ou plus, il combine ces informations.

3.1.8 Mesurer les effets de la surveillance[29]

Le centre national de coordination soutient l'évaluation régulière des effets des activités nationales de surveillance des frontières, en collectant et en analysant les informations et en élaborant un aperçu des événements et des activités réalisées pour y répondre, en précisant leur efficacité ainsi que les ressources et le personnel utilisés.

3.1.9 Coopération avec les autres centres nationaux de coordination[30]

Au sein d'Eurosur, le centre national de coordination constitue le point de contact unique pour les échanges d'informations et la coopération avec les autres centres nationaux de coordination et l'Agence.

[26] Article 5, paragraphe 3, point d), du règlement (UE) n° 1052/2013.
[27] Article 5, paragraphe 3, point e), du règlement (UE) n° 1052/2013.
[28] Article 5, paragraphe 3, point f), du règlement (UE) n° 1052/2013.
[29] Article 5, paragraphe 3, point g), du règlement (CE) n° 1052/2013.
[30] Article 5, paragraphe 3, point h), du règlement (CE) n° 1052/2013.

3.1.10 Heures d'exploitation[31]

Le centre national de coordination est actif 24h sur 24, 7 jours sur 7: la présence d'au moins un officier/chef d'équipe est donc garantie.

3.1.11 Notification de la création et de la surveillance du centre national de coordination[32]

Chaque État membre doit notifier à la Commission européenne la création de son centre national de coordination. La Commission transmet régulièrement aux États membres et à l'Agence un rapport technique sur la mise en place et le développement des centres nationaux de coordination.

Le centre national de coordination informe régulièrement l'Agence des évolutions pertinentes de ses activités et de ses structures. Il peut notamment transmettre des informations sur les responsabilités, fonctions et missions supplémentaires confiées au centre national de coordination, les autres autorités coopérant avec le centre, les mises à jour techniques ou toute autre information utile.

3.1.12 Affectation de tâches à d'autres autorités nationales[33]

Les États membres peuvent demander à des autorités régionales, locales, fonctionnelles ou autres de prendre en charge la connaissance de la situation et la capacité de réaction dans leurs zones de compétence respectives, pour autant

1) qu'elles soient en position de prendre des décisions opérationnelles;

2) que les ressources octroyées permettent une gestion effective et efficace des ressources et du personnel, facilitent la planification et la mise en œuvre des activités de surveillance des frontières nationales ou aident à coordonner le système national de surveillance des frontières; et

3) que cette décision n'affecte en rien la capacité du centre national de coordination de coopérer et d'échanger des informations avec les autres centres nationaux de coordination et l'Agence.

Dans certains cas prédéfinis, le centre national de coordination peut autoriser les autorités régionales, locales, fonctionnelles ou autres à communiquer et à échanger des informations avec les autorités régionales ou avec le centre national de coordination d'un autre État membre ou les autorités responsables d'un pays tiers, pour autant qu'elles informent régulièrement le centre national de coordination de leurs communications et de leurs échanges d'informations.

Lorsqu'il coordonne les activités de surveillance des frontières avec les autorités fonctionnelles et autres, le centre national de coordination veille à ce que les responsabilités et l'autonomie (p.ex. fonctions de commandement et de contrôle) de chacune de ces autorités soient pleinement respectées.

[31] Article 5, paragraphe 4, du règlement (UE) n° 1052/2013.
[32] Article 5, paragraphe 1, et article 22 du règlement (CE) nº 1052/2013.
[33] Article 17 du règlement (UE) n° 1052/2013.

3.1.13 Règlement intérieur

L'autorité responsable du centre national de coordination possède un *règlement de procédure* spécifiant la procédure à suivre pour échanger des informations et travailler avec les autorités nationales compétentes. Ce règlement couvre également la gestion, le stockage, la transmission, le traitement et la suppression des données à caractère personnel et des informations sensibles non classifiées et informations classifiées.

3.1.14 Coopération entre les agences au niveau national

Chaque État membre répartit lui-même les responsabilités entre ses autorités nationales compétentes en matière de surveillance des frontières extérieures. Les autorités nationales doivent tenir compte de leurs domaines de compétence respectifs et éviter de prendre des mesures susceptibles d'avoir une incidence directe ou indirecte sur les autres autorités dans l'exécution de leurs tâches.

S'il n'existe pas de modèle unique pour la coopération entre les agences, une coopération améliorée, notamment entre les autorités civiles et les autorités militaires, peut permettre d'utiliser de manière plus efficace et effective les informations, les capacités et les systèmes disponibles au niveau national.

En fonction de la portée de la coopération et des responsabilités attribuées aux autorités compétentes par la législation nationale, cette coopération peut prendre les formes suivantes:

a) *Partage d'informations:* les autorités nationales partagent les informations tirées de leurs systèmes individuels ainsi que des événements et des couches «opérations» et «analyse» du NSP. Les autorités nationales peuvent également partager les informations émanant de leurs infrastructures de surveillance (p.ex. les stations radar, la surveillance des fréquences VHF) au niveau local, de préférence en temps quasi-réel.

b) *Coopération:* les autorités nationales peuvent partager certaines infrastuctures de surveillance (y compris, par exemple, l'établissement et la maintenance des stations radar), s'accorder mutuellement un accès contrôlé à leurs systèmes et bases de données (sur la base du principe du besoin d'en connaître), effectuer des analyses de risques conjointes et coordonner leurs activités de patrouille. Dans ce cadre, les autorités nationales doivent recourir le plus possible au centre national de coordination.

c) *Assistance:* une autorité nationale (p.ex. l'autorité militaire) peut aider une autre (p.ex. les gardes-frontières) à effectuer ses missions de surveillance des frontières. La responsabilité et la compétence de cette tâche relèvent néanmoins toujours de l'autorité initiale. Les autorités nationales compétentes doivent informer le centre national de coordination de la portée et de la durée de la mesure d'assistance, ainsi que des autres informations utiles à cet égard.

d) *Intégration:* dans le meilleur des cas, un système national unique et/ou un centre national unique sont utilisés par les différentes autorités nationales pour exécuter diverses fonctions de surveillance (p.ex. le contrôle des frontières, le contrôle des pêches ou les opérations de recherche et de sauvetage). Une autre possibilité réside dans la désignation, par le législateur national, d'une autorité nationale chargée de l'exécution de plusieurs tâches de surveillance.

Plusieurs formes de coopération peuvent être envisagées:

→ le *personnel* d'une autorité nationale fournit des informations opérationnelles, analytiques, techniques et administratives ainsi qu'un soutien à une autre autorité nationale;

→ les *infrastructures* de surveillance et de communication sont partagées afin d'améliorer la connaissance générale de la situation;

→ l'utilisation des *équipements* (p.ex. moyens de patrouille) est coordonnée afin d'améliorer la capacité de réaction globale;

→ des *procédures opérationnelles types* pour l'échange d'informations et la coopération sont en place;

→ une *formation* est dispensée au personnel des autres autorités afin de permettre une meilleure compréhension mutuelle et un transfert de connaissances plus efficace.

Des accords entre les autorités nationales concernées doivent préciser la portée et les modalités de la coopération, de même que les obligations juridiques, opérationnelles et financières de chaque partenaire. Il convient de privilégier l'utilisation ou l'adaptation d'accords existants avant d'en conclure de nouveaux.

3.1.15 Liste de contacts

Le centre national de coordination dresse et tient à jour une liste de contacts des autorités nationales avec lesquelles il travaille et échange des informations.

3.2 Connaissance de la situation

3.2.1 Relation entre les tableaux de situation et leurs couches[34]

Le tableau de situation national (NSP), qui est mis à jour par le centre national de coordination, apporte une connaissance de la situation au niveau national, tandis que le tableau de situation européen (ESP) et le tableau commun du renseignement en amont des frontières (CPIP), qui sont quant à eux mis à jour par l'Agence, apportent une connaissance de la situation au niveau européen. La relation entre ces tableaux et leur place au sein du cadre Eurosur peuvent être décrites comme suit:

1) NSP

Les centres nationaux de coordination sont chargés d'établir et de mettre à jour le NSP dans chaque État membre. Ce tableau représente l'ensemble des informations fournies par cet État membre à Eurosur et tient donc compte de l'origine des données, des informations et des renseignements qu'il contient. Le NSP peut être établi à l'aide de plateformes techniques capables de gérer les échanges d'informations requis, ce qui permet à l'État membre de fournir des informations pertinentes en temps quasi-réel au tableau de situation européen et au tableau commun du renseignement en amont des frontières.

2) Relation entre l'ESP et le CPIP

L'ESP donne un aperçu général de la situation aux frontières extérieures, sur la base des informations fournies par les centres nationaux de coordination et l'Agence. Il inclut des informations émanant des tableaux de situation nationaux et de l'application commune des outils de surveillance. Le CPIP porte sur les informations et les renseignements relatifs aux zones situées au-delà des frontières extérieures. L'accent est mis sur la fourniture de services, y compris de services d'analyse prévisionnelle, couvrant les zones maritimes et les pays tiers d'origine et de transit. Ces deux tableaux sont associés et assurent donc une continuité géographique. Ils sont tous deux diffusés dans les États membres et mis à la disposition de l'Agence.

[34] Articles 8 à 11 du règlement (UE) n° 1052/2013.

3) Lien entre le NSP et l'ESP/CPIP

Le contenu du NSP et de l'ESP/CPIP peuvent se chevaucher partiellement, puisque certaines parties des tableaux de situation nationaux mis à la disposition de l'Agence et d'autres États membres font également partie de l'ESP/CPIP. Les dispositions pertinentes du règlement (UE) n° 1052/2013 (p.ex. les restrictions au partage de données à caractère personnel)[35] s'appliquent à toutes les informations des tableaux de situation nationaux qui sont intégrées à l'ESP/CPIP.

Toutes les informations contenues dans le NSP et qui ne sont pas mises à la disposition de l'Agence sont traitées conformément aux dispositions régissant les NSP. Ces dispositions s'appliquent également aux échanges d'informations entre deux ou plusieurs États membres, pour autant que ces échanges n'impliquent pas l'Agence. Les dispositions régissant l'ESP/CPIP s'appliquent automatiquement dès que l'Agence est impliquée.

Les échanges d'informations entre ces trois tableaux suivent leurs trois couches communes.

1) La *couche «événements»* inclut

- les incidents relatifs aux franchissements non autorisés des frontières, y compris les informations accessibles aux centres nationaux de coordination portant sur les incidents ayant trait à une menace pour la vie des migrants et à la criminalité transfrontalière;

- les informations sur les situations de crise;

- les informations sur les véhicules, navires et autres engins et personnes non identifiés et suspects présents aux frontières extérieures ou le long ou à proximité de celles-ci; et

- tout autre événement pouvant avoir un impact important sur le contrôle des frontières extérieures.

2) La couche «opérations» se compose des informations relatives aux ressources propres et aux autres informations opérationnelles et environnementales.

3) La couche «analyse» se compose des informations générales, rapports d'analyse, renseignements, images, géodonnées et différents types de cartes.

3.2.2 Propriété et assurance des informations et approche axée sur les services

En principe, les informations sont la propriété du centre nodal qui les a transmises (à savoir le centre national de coordination pertinent ou l'Agence). Cette propriété peut être transférée à un autre centre national de coordination ou à l'Agence, sur la base d'un accord mutuel. Ce transfert peut être décidé au cas-par-cas ou pour un groupe ou une catégorie d'informations particulier, par exemple si les informations sont transférées via un lien automatisé entre Eurosur et un autre logiciel. Il incombe à l'État membre demandant la propriété des informations de motiver sa demande.

Les centres nationaux de coordination sont tenus de fournir une explication aussi complète, exacte et rapide que possible. Les centres nationaux de coordination et l'Agence sont tenus d'assurer la disponibilité, la confidentialité et l'intégrité des informations échangées, en

[35] Article 13 du règlement (UE) n° 1052/2013.

respectant scrupuleusement les règles de sécurité, les règles de protection des données à caractère personnel et classifiées et en respectant les droits de propriété lors du traitement des informations.

Les propriétaires des informations doivent les valider avant de les publier dans le réseau de communication Eurosur (ECN). Des efforts doivent être entrepris afin d'éviter toute duplication des informations, en adoptant des procédures adéquates et des processus de validation cohérents. Il conviendra particulièrement d'éviter que les informations chargées manuellement ne soient pas des doubles des informations déjà introduites dans le système via des sources automatisées et semi-automatisées (autres systèmes connectés). Des procédures sont élaborées au niveau de l'Agence et au niveau des États membres afin de réduire ce risque.

L'Agence adopte une approche axée sur les services, reposant sur des normes acceptées au niveau international, afin de fournir informations et services à Eurosur.

3.2.3 Communautés d'intérêts[36]

Les communautés d'intérêts sont constituées des utilisateurs d'Eurosur qui ont des objectifs, des exigences ou des intérêts en commun. Ces utilisateurs peuvent former des groupes géographiques ou des groupes basés sur un thème. Par exemple, une communauté d'intérêts géographique pourrait être axée sur une zone/un type de frontière particulier ou la possession d'une frontière commune avec un pays tiers donné. Une communauté thématique pourrait avoir pour objectif de développer la couche «analyse» ou un autre service particulier d'Eurosur ou encore de participer à une opération conjointe.

Si ces communautés n'ont pas une existence officielle, elles aident à améliorer l'organisation, et, surtout, à améliorer la coopération et les synergies dans la fourniture de services et les échanges d'informations, ce qui permet d'améliorer la capacité de réaction. Les échanges d'informations et la coopération dans ces groupes sont régis par les dispositions du NSP ou de l'ESP/CPIP, en fonction de la participation ou non de l'Agence.

Vu leur caractère pluridimensionnel, les communautés d'intérêts peuvent dépasser le cadre d'Eurosur et d'autres dispositions (telles que le mandat général de l'Agence) s'appliquent alors aux éléments non couverts par Eurosur. Par exemple, si un groupe d'États membres participant à une opération conjointe constitue une communauté d'intérêts, une partie des informations collectées et traitées par l'Agence dans le cadre de cette opération peuvent sortir du cadre d'Eurosur (p.ex. des informations sur les procédures de retour, l'asile, etc.)

3.2.4 Sources d'information[37]

Catégorie	Liste non exhaustive d'exemples
A - Système national de surveillance	Système(s) de surveillance des frontières terrestres Système(s) de surveillance maritime Système(s) de surveillance des frontières aériennes
B - Capteurs fixes et mobiles	Radar: position, itinéraire, vitesse, heure, taille de l'objectif Caméras: images, vidéos, heure, direction, données traitées par l'image

[36] Voir l'annexe du règlement (UE) n° 1052/2013

[37] Article 9, paragraphe 2, du règlement (UE) n° 1052/2013.

	Caméras actives à crénelage en distance: distance de cible, identification des navires Capteurs de fréquences radio/système de contrôle de la direction: position, fréquence opérationnelle, type de radio Systèmes d'hydrophones: informations sur les mouvements des navires, identification des navires
C - Patrouilles	Missions de surveillance des frontières maritimes, terrestres et aériennes Ressources militaires appuyant une mission de maintien de l'ordre Missions de recherche et de sauvetage Missions de douane/de contrôle des pêches Missions de sécurité maritime (p.ex. détection des marées noires)
D - Centres locaux, régionaux et autres	Centres de coordination locaux et régionaux Centres de coordination des opérations de sauvetage en mer
E - Autres autorités et systèmes, y compris les officiers de liaison	Points de contact nationaux pour la prévention de l'immigration illégale/du trafic de drogues Centres opérationnels pour la coopération transfrontalière Centres nationaux pour le contrôle des pêches/la sûreté et la sécurité maritimes Points de contact entre les États membres voisins (p.ex. pour les faux documents, les frontières, les douanes ou la lutte contre la criminalité transfrontalière visant des véhicules) Ambassades, consulats et agents de liaison dans les pays tiers
F - L'Agence	Services de fusion d'Eurosur, comprenant des informations tirées de l'application commune des outils de surveillance (p.ex. service de détection des navires, imagerie satellite, informations relatives à la configuration des lieux, prévisions météorologiques) Produits d'analyse élaborés par l'unité d'analyse des risques de l'Agence (p.ex. niveaux d'impact alloués aux tronçons de frontière) Informations sur les opérations conjointes, y compris les rapports d'événements envoyés via la *Joint Operations Reporting Application* (JORA) (application de transmission d'informations sur les opérations conjointes)

	Informations sur les ressources propres de l'Agence
G - Autres centres nationaux de coordination	Tronçons de frontière adjacents: incidents, rapports d'analyse des risques au niveau tactique et, éventuellement, patrouilles Réseaux régionaux Réseau européen de patrouilles
H - Pays tiers	Réseaux régionaux Coopération bilatérale
I - Systèmes d'annonce des mouvements de bateaux	Système d'identification automatique (AIS) Système de surveillance des navires (SYSTÈME VMS) Système d'échange d'informations maritimes de l'Union, y compris SafeSeaNet (SSN) et le système d'identification et de localisation à grande distance (LRIT)

3.2.5 Couche «événements»[38]

Pour la surveillance des frontières terrestres et maritimes, les États membres doivent signaler tous les événements comme indiqué aux chapitres suivants, quel que soit leur niveau d'impact.

Si un État membre décide de signaler un incident à un point de passage frontalier ou un incident ayant trait à la surveillance des frontières aériennes, il doit:

- déclarer la portée de son signalement à l'Agence, et
- respecter pleinement cette portée lorsqu'il effectue ledit signalement.

Les problèmes ayant trait aux contrôles aux frontières et à la surveillance des frontières aériennes sont utiles pour améliorer la compréhension globale de la situation. Les États membres doivent par conséquent continuer à fournir des informations sur ces problèmes une fois qu'ils ont commencé et ne cesser que dans des situations exceptionnelles et dûment justifiées. S'ils interrompent leurs notifications, ils doivent le signaler à l'Agence.

3.2.5.1 Format de la couche «événements» du NSP

Les sous-couches de la couche «événements» ne doivent pas être considérées comme étant physiquement séparées: il s'agit de séries d'informations portant sur différents sujets, pouvant être présentées de diverses manières, dans l'objectif d'améliorer le plus possible la connaissance de la situation et la capacité de réaction. La manière dont les événements sont collectés dans le NSP devrait permettre le transfert aisé et rapide de tous les événements vers l'ESP, p.ex. par un transfert automatisé ou semi-automatisé via une interface ou un rapide encodage manuel de ces événements dans l'ESP.

[38] Voir l'article 4, paragraphes 2 et 3, l'article 9, paragraphes 3 et 4, l'article 10, paragraphe 3 et l'article 11, paragraphe 4, du règlement (UE) n°1052/2013.

3.2.5.2 Sous-couche «franchissements non autorisés des frontières»

Tous les incidents relatifs à des franchissements non autorisés des frontières détectés aux frontières extérieures de l'État membre doivent être signalés au NSP, quel que soit le nombre de personnes impliquées, leur nationalité ou le niveau d'impact de l'incident. La meilleure pratique veut que l'on inclue également les incidents relatifs aux contrôles aux frontières et à la surveillance des frontières aériennes afin de permettre une compréhension totale de la situation.

3.2.5.3 Sous-couche «criminalité transfrontalière»

Cette sous-couche désigne tous les incidents liés à des formes graves de criminalité ayant une dimension transfrontalière, commise aux frontières extérieures, ou le long ou à proximité de celles-ci

3.2.5.4 Sous-couche «situations de crise»

Cette sous-couche couvre les catastrophes d'origine naturelle ou humaine, les accidents, les crises humanitaires ou politiques ou toute autre situation grave survenant aux frontières extérieures, ou le long ou à proximité de celles-ci, susceptibles d'avoir un impact significatif sur le contrôle aux frontières. Le terme «impact significatif» doit ici être compris comme affectant les conditions à la frontière au point de nécessiter des mesures supplémentaires ou une intervention spéciale (p.ex. nécessité de renforts et d'une prise de décision et d'une intervention rapides).

3.2.5.5 Sous-couche «autres événements»

Cette sous-couche contient des informations sur les véhicules, navires et autres engins et personnes non identifiés et suspects présents aux frontières extérieures de l'État membre concerné, ou le long ou à proximité de celles-ci, et sur tout autre événement pouvant avoir un impact important sur le contrôle aux frontières extérieures.

3.2.5.6 Éléments de la couche «événements» du NSP à partager avec l'ESP

Tous les événements notifiés dans le NSP doivent également être inclus dans l'ESP. Le centre national de coordination doit veiller à ce qu'ils soient chargés et transférés vers l'ESP dans les plus brefs délais.

3.2.5.7 Affectation aux tronçons de frontière

Chaque événement est assigné à un tronçon de frontière.

3.2.5.8 Niveau d'impact pour les incidents

Lors de la maintenance de leurs NSP respectifs, les centres nationaux de coordination affectent un niveau d'impact à tous les événements qu'ils signalent, sur la base d'une évaluation nationale. L'Agence ne peut modifier les niveaux d'impact des incidents affectés par les centres nationaux de coordination.

3.2.5.9 Couche «événements» de l'ESP/CPIP

L'ESP et le CPIP sont à la disposition de tous les États membres participant à Eurosur. L'Agence doit fournir aux centres nationaux de coordination un accès illimité aux deux tableaux, via l'ECN.

Le contenu du CPIP reflète la structure présentée dans l'ESP: dès lors, les informations couvrent les mêmes domaines thématiques. Ensemble, le CPIP et l'ESP assurent une continuité géographique. Il se peut que certains incidents soient détectés dans la zone couverte par le CPIP et interceptés dans la zone couverte par l'ESP.

Tous les événements qui se produisent dans la zone opérationnelle d'une opération conjointe, d'un projet pilote ou d'une intervention rapide coordonnée par l'Agence doivent être notifiés dans l'ESP/CPIP, y compris ceux qui ont eu lieu dans la zone opérationnelle, mais pas dans le cadre de l'opération conjointe elle-même. Les zones opérationnelles du réseau européen de patrouilles et toutes les autres activités opérationnelles impliquant l'Agence relèvent de cette catégorie.

3.2.5.10 Processus de signalement et assurance qualité

Les États membres et l'Agence doivent veiller à ce que le signalement soit de qualité suffisante et qu'il n'y ait pas de doubles signalements (p.ex. d'incidents) dans le cadre d'Eurosur. Pour ce faire, les États membres mettent en place un mécanisme de validation rendant le centre national de coordination responsable de la validation finale des données transmises à l'ESP/CPIP. Le centre national de coordination doit également veiller à ce qu'aucune donnée à caractère personnel autre que celles relatives aux numéros d'identification des navires ne soit chargée dans l'ESP/CPIP.

Le point de contact national Frontex (NFPOC) informe au préalable le centre national de coordination de toute opération prévue sur son territoire.

3.2.6 Couche «opérations»[39]

3.2.6.1 NSP

La couche «opérations» inclut

- une sous-couche «ressources propres et zones opérationnelles»; et
- une sous-couche «informations environnementales» (voir le chapitre 3.2.6.5).

La sous-couche «ressources propres et zones opérationnelles» contient des informations sur les ressources nationales et les ressources humaines, tels qu'établies et maintenues au niveau national.

Les informations sur les ressources propres et les zones opérationnelles sont collectées dans les systèmes nationaux des États membres. Il peut notamment s'agir de la visualisation des zones de responsabilité des structures subordonnées sur une carte géoréférencée, de la position et de l'itinéraire des patrouilles, de la répartition et du type de ressources, d'images en temps réel fournies par des caméras vidéo, de la zone couverte par les caméras et de la position et des coordonnées des navires de patrouille sur les cours d'eau et en mer. La communication directe entre le centre national de coordination et les ressources de patrouille via des terminaux spécifiques (p.ex. le système TETRA - Trans European Trunked Radio system) améliore considérablement la capacité de réaction.

Les informations relatives aux ressources militaires appuyant une mission de maintien de l'ordre peuvent être limitées sur la base du besoin d'un connaître à la demande de l'autorité nationale qui en est responsable.

Établir des liens entre les informations fournies dans le cadre de la couche «opérations» (p.ex. sur les ressources de patrouille et les conditions météorologiques) et les informations tirées de la couche «événements» améliore considérablement la connaissance de la situation et la capacité de réaction.

[39] Voir l'article 9, paragraphes 5 et 6, l'article 9, paragraphe 9, et l'article 10, paragraphes 5 et 6, et l'article 11, paragraphe 4, du règlement (UE) n° 1052/2013.

Le tableau de situation des tronçons de frontière extérieure adjacents inclus dans la couche «opérations» peut également être partagé avec les États membres impliqués ainsi qu'avec l'Agence, sur une base volontaire.

3.2.6.2 ESP/CPIP

Cette couche inclut

- une sous-couche «ressources propres»;
- une sous-couche «opérations»;
- une sous-couche «informations environnementales» (voir le chapitre 3.2.6.5).

Les sous-couches «ressources propres» et «opérations» contiennent des informations fournies par les États membres et l'Agence, lorsque les ressources sont utilisées pour les opérations conjointes de l'Agence ou sont à la disposition de l'Agence. Les informations suivantes sont requises pour toutes les *ressources* intervenant dans les activités opérationnelles coordonnées par l'Agence:

- type de ressource;
- nom de la ressource (marque/modèle/indicatif);
- description (indications détaillées sur le type de ressource);
- propriétaire - en indiquant l'État membre (description standard, y compris le code pays à trois chiffres (norme ISO 3166-1 alpha-3) de l'autorité de l'État membre responsable du déploiement);
- situation (dernière base de déploiement);
- nom de l'opération.

Des informations sont également incluses au sujet du statut et de la position des ressources (par exemple, une ressource utilisée dans une opération conjointe envoie les informations relatives à sa position via le système de positionnement Frontex), de la déclaration de mission et des acteurs impliqués, des horaires de déploiement et de patrouille, des zones d'opération, des rapports de situation périodiques, des informations statistiques, des points focaux et de coordination et des autres activités opérationnelles coordonnées par l'Agence, telles que le réseau européen de patrouilles (EPN).

La meilleure pratique consiste à ce que les centres nationaux de coordination hébergent les activités coordonnées par l'Agence, y compris le centre de coordination international (ICC). Lorsque l'ICC est distinct du centre national de coordination, des canaux et procédures de communication adéquats doivent être mis en place pour permettre les échanges d'informations entre ces organismes sur les activités coordonnées par l'Agence.

3.2.6.3 Réseau européen de patrouilles

Tous les États membres de l'EPN se servent du cadre Eurosur pour partager les informations sur l'EPN. Les États membres de l'EPN utilisent leur centre national de coordination et l'ECN pour

- signaler tous les *incidents* en rapport avec l'immigration illégale et la criminalité transfrontalière constatés dans les zones de l'EPN dans la couche «événements» de l'ESP/CPIP. Le cas échéant, des rapports de mission standards, des vidéos et des images peuvent être joints pour fournir des détails sur l'incident;

- fournir des informations sur les *patrouilles communes* de l'EPN à la couche «opérations» de l'ESP/CPIP, y compris des informations sur les ressources de patrouille à bord des observateurs (notamment les agents de liaison);

- vérifier et mettre à jour les *zones de l'EPN*[40] dans la couche «opérations» de l'ESP/CPIP;

- mettre à jour les informations sur les éléments clés (p.ex. horaires de patrouilles de l'EPN et informations mensuelles sur les patrouilles effectuées dans les zones de l'EPN, modifications des structures de l'EPN);

les informations relatives à la coopération quotidienne entre les États membres de l'EPN doivent être clairement indiquées dans la couche «opérations» de l'ESP/Coopération.

3.2.6.4 Rôles et responsabilités

Les informations relatives aux opérations, aux projets pilotes et aux interventions rapides coordonnées par l'Agence doivent être fournies comme suit:

- L'Agence insérera des informations sur la zone d'opération pour les opérations conjointes.

- L'État membre d'accueil fournira des informations sur les ressources participant aux opérations conjointes, mais ces informations peuvent également être transmises par l'Agence, avec l'accord de l'État membre d'accueil.

- Le système de positionnement Frontex renseigne sur la position, l'heure, l'état et le type de ressources participant aux opérations conjointes, aux projets pilotes et aux interventions rapides ou celles qui sont mises à la disposition de l'Agence. Si les ressources participant à l'opération conjointe ne sont pas connectées au système de positionnement de Frontex, le centre national de coordination de l'État membre accueillant l'opération conjointe doit fournir des informations régulières sur le nombre, la position et l'état des ressources déployées.

L'Agence peut également partager, via la couche «opérations» de l'ESP/CPIP, d'autres informations sur les opérations, les projets pilotes et les interventions rapides coordonnés par l'Agence, notamment:

- les rapports de situation quotidiens/hebdomadaires pour chaque opération conjointe spécifique;

- des informations personnalisées destinées aux médias.

[40] Ces zones ont été délimitées en fonction des activités de patrouille des États membres, couvrant des zones côtières spécifiques de la mer Méditerranée, de l'océan Atlantique et de la mer Noire.

3.2.6.5 Sous-couche «informations environnementales»

Cette sous-couche donne accès à des informations sur la configuration des lieux et les conditions météorologiques. L'Agence fournit, via la couche «opérations» de l'ESP/CPIP, des observations météorologiques, des prévisions météorologiques, des informations océanographiques et des services de dérivation de modèles, qui peuvent également être utilisés pour le NSP.

3.2.7 Couche «analyse»[41]

Les couches «analyse» de l'ESP/CPIP et du NSP sont interconnectées, vu qu'elles peuvent être basées sur les mêmes données de situation et de renseignement. Les deux tableaux ci-dessous contiennent les types de produits et de services que l'on retrouve dans la couche «analyse» du NSP et de l'ESP/CPIP.

Les produits de la couche «analyse» ne sont, par défaut, pas fournis à la demande, mais sur la base de demandes internes spécifiques du centre national de coordination ou de l'Agence.

Produits	Description
Évolutions majeures	Bref rapport incluant une description succincte et une analyse des événements ou des conditions politiques, sociales, économiques ou démographiques, y compris la situation des droits fondamentaux, qui ont ou pourraient avoir une incidence sur l'immigration illégale ou la criminalité transfrontalière.
Note d'information	Un bref rapport, généralement ad hoc, analysant les problèmes spécifiques en rapport avec l'immigration illégale ou la criminalité transfrontalière. Son but principal est d'informer rapidement et efficacement les décideurs sur un problème donné.
Suivi analytique	Un rapport régulier et plus détaillé (par rapport à la note d'information) sur l'immigration illégale ou la criminalité transfrontalière, couvrant certaines régions et certains problèmes. Ce rapport va plus loin que la note d'information en proposant une analyse plus approfondie de la situation, et, si possible, des recommandations.
Rapports d'observation de la terre	Les rapports fournis par le Centre satellitaire de l'UE ou les entreprises en réponse à une demande de services d'observation de la terre, tels que des services de surveillance côtière ou de surveillance en amont des frontières.
Rapports analytiques de soutien	Cette catégorie a pour but de permettre le partage de documents analytiques ne correspondant pas aux principaux types de produits de la couche «analyse» (évolutions majeures, notes d'information et suivis analytiques) via Eurosur.

Les services de la couche «analyse» sont tous des services «à la demande», que les centres nationaux de coordination peuvent demander via les *services de fusion d'Eurosur* (voir le chapitre 3.2.8). Par défaut, ces services seront partagés avec tous les centres nationaux de coordination via l'ECN.

Services	Description

[41] Voir l'article 9, paragraphe 7, l'article 10, paragraphe 7, et l'article 11, paragraphe 4, du règlement (UE) no° 1052/2013.

Surveillance côtière	Rapports ponctuels et ad hoc, données vectorisées et images de bandes côtières (mers et ports) sélectionnées via une analyse des risques. Ces documents appuient l'évaluation opérationnelle des activités en rapport avec l'immigration illégale et la criminalité transfrontalière.
Surveillance en amont des frontières	Rapports ponctuels et ad hoc, données vectorisées et images de zones en amont des frontières sélectionnées via une analyse des risques. Ces rapports appuient l'évaluation opérationnelle des activités en rapport avec l'immigration illégale et la criminalité transfrontalière. Ce service permet la demande d'études sur la perméabilité des frontières.
Imagerie de référence/cartographie	Images satellite de très haute résolution et données vectorisées couvrant certaines zones de pays tiers sélectionnées via une analyse des risques. Cette imagerie est nécessaire pour l'analyse actuelle et future des activités en rapport avec l'immigration illégale et la criminalité transfrontalière.

Les sept étapes suivantes sont utilisées pour créer et gérer la couche «analyse»:

- Étape 1: gestion de la couche «analyse»
- Étape 2: collecte de renseignements
- Étape 3: évaluation des renseignements
- Étape 4: confrontation des renseignements
- Étape 5: analyse et interprétation
- Étape 6: création et visualisation des produits et des services
- Étape 7: diffusion

3.2.7.1 Étape 1: gestion de la couche «analyse»

Cette tâche globale vise à gérer la couche «analyse» et le cycle de renseignement qui y est associé, en définissant ou en améliorant les tâches, les procédures et les politiques.

3.2.7.2 Étape 2: collecte de renseignements

L'Agence collecte des informations et des renseignements sur la base d'exigences convenues, en s'axant sur un objectif, un comportement ou une tendance. Cette collecte suppose d'obtenir des informations provenant de diverses sources dans différents formats; dans un premier temps, elles émanent surtout de sources extérieures à Eurosur (opérations conjointes, réseaux d'agents de liaison et d'analyse des risques, agences de l'UE, missions et délégations ou agences, fonds et programmes des Nations unies). Cela évolue peu à peu en fonction de la quantité et de la qualité des renseignements fournis à Eurosur par les centres nationaux de coordination. Cette étape regroupe les types d'informations et de renseignements nécessaires à la création de la couche «analyse» de l'ESP/CPIP;

- *Imagerie et géodonnées:* informations à référence spatiale telles que des cartes topographiques, des infrastructures de transport, des cartes nautiques, des zones restreintes, des cartes thématiques et des modèles numériques d'élévation, y compris une imagerie de référence pour les principales zones d'immigration illégale et les lieux identifiés par les analyses et les renseignements.

- *Informations clés stratégiques: couvrent les études à long terme, les tendances émergentes et les évolutions de la lutte contre l'immigration illégale et la criminalité transfrontalière, les mesures potentielles d'atténuation et de prévention et les possibilités de modifications des politiques, programmes et législations.*

- *Informations opérationnelles: informations tactiques et opérationnelles telles que des données de capteurs, la détection et le pistage de navires, l'imagerie radar, les ressources de patrouille, les rapports d'incidents, l'imagerie satellite, le renseignement opérationnel et les informations sur la surveillance (renseignement par écoute des signaux, renseignement humain).*

- *Données de la base de données: la base de données contiendra une description formalisée des termes et méthodes utilisés, notamment une catégorisation des types de navires, des descriptions des scénarios typiques et des descriptions des capteurs. Elle rendra possible la collecte, l'organisation et l'extraction manuelles et semi-automatiques des connaissances.*

3.2.7.3 Étape 3: évaluation des renseignements

Cette étape consiste en deux tâches:

- *évaluation: appréciation de la fiabilité de la source et de la crédibilité des informations;*

- *validation: évaluation des données entrantes et filtrées par rapport à des critères standardisés (y compris des contrôles juridiques), afin d'améliorer la qualité des données.*

3.2.7.4 Étape 4: confrontation des renseignements

La confrontation consiste à éliminer les informations trompeuses, sans pertinence et inexactes. Il convient ensuite de réarranger les informations restantes afin de pouvoir détecter les éventuelles relations entre des éléments qui en semblent dénuées au premier abord. Elle inclut deux tâches:

- *filtrage: suppression des informations non essentielles pour répondre aux besoins immédiats d'informations;*

- *fusion: mise en commun des informations évaluées et validées afin d'obtenir un seul produit cohérent.*

3.2.7.5 Étape 5: analyse et interprétation

L'étape d'analyse transforme les informations en un produit interprété qui fournit la conclusion prospective la plus précise et la plus valide possible.

- *Le* renseignement tactique/opérationnel *contribue directement à un objectif immédiat; il est par exemple axé sur des activités criminelles spécifiques, dans le but de les neutraliser.*

- *Le* renseignement stratégique *traite des tendances existantes ou émergentes des activités d'immigration illégale et de criminalité transfrontalière. Son objectif est atteint grâce à une synthétisation et à une analyse des données collectées collectées pendant une certaine période afin de formuler des jugements informés sur des questions telles que les capacités de facilitation, les vulnérabilités, les comportements et les tendances. Il permet d'élaborer des conclusions et des prévisions qui aideront à prendre des mesures de réponse appropriées.*

- *L'*analyse de l'imagerie *est une activité importante qui permet de générer des informations, des objectifs et des renseignements stratégiques, grâce à l'exploitation des images satellite. Elle détecte et analyse les changements tout en permettant la mise en correspondance et la fusion avec les autres sources (sources ouvertes, données géospatiales, informations de développement stratégique et sources de tierces parties), les rapports analytiques et autres supports.*

Les analyses sont personnalisées en fonction des besoins des clients afin d'orienter efficacement le processus décisionnel.

3.2.7.6 Étape 6: création et visualisation des produits et des services, et Étape 7: diffusion

Lors de ces étapes, les produits de l'étape d'analyse et d'interprétation sont corrigés, concentrés, organisés et modifiés, avant la publication des documents et l'affichage des objets et des cartes. La phase finale est le chargement de tous les produits de la couche «analyse», nouveaux et mis à jour, dans le NSP ou l'ESP/CPIP. Une fois que les produits peuvent être vus dans l'ESP/CPIP, ils sont réputés avoir été diffusés.

3.2.8 Application commune des outils de surveillance[42]

3.2.8.1 Rôle de l'Agence

L'Agence coordonne l'application commune des outils de surveillance au niveau européen en fournissant des services centralisés aux États membres et à l'Agence. En tant que coordinatrice, l'Agence doit constituer le point d'entrée/de sortie unique pour l'acquisition, la fusion et la livraison de ces services.

3.2.8.2 Activation des services

Les services sont activés en fonction *des exigences* relatives à la maintenance de l'ESP et du CPIP, *à la demande* du centre national de coordination ou *d'une demande* des unités de l'Agence (p.ex. pour appyter les opérations conjointes).

3.2.8.3 Fourniture des services

1) Étendue des services: Le tableau ci-dessous présente toute la gamme de services qui peuvent être fournis:

Gamme de services	Règlement (UE) n° 1052/2013	Fourniture
Informations environnementales, y compris - informations relatives à la configuration des lieux (p.ex. cartes de base); - conditions météorologiques;	Article 10, paragraphe 5, point c)	Normale
Surveillance côtière	Article 12, paragraphe 2, point a)	Sur demande
Pistage de navires	Article 12, paragraphe 2, point b)	Sur demande
Surveillance des zones désignées situées en mer	Article 12,	Sur

[42] Article 12 du règlement (UE) n° 1052/2013.

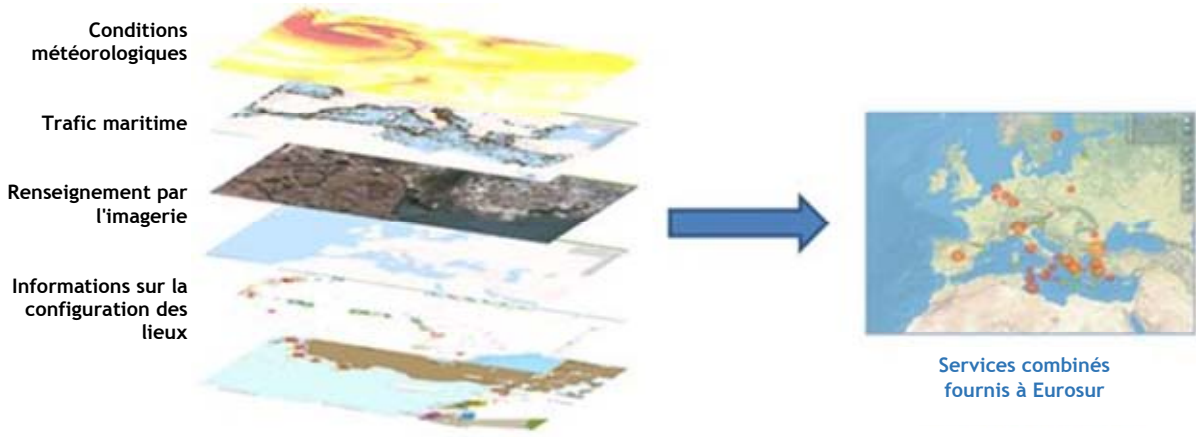
	paragraphe 2, point c)	demande
Évaluation environnementale de zones désignées	Article 12, paragraphe 2, point d)	Sur demande
Surveillance en amont des frontières	Article 12, paragraphe 2, point e)	Sur demande
Données des systèmes d'annonce des mouvements de bateaux	Article 12, paragraphe 3, point a)	Normale

2) Fusion des services

Dans le cadre des *services de fusion d'Eurosur*, l'Agence acquiert, associe et présente des services de base et combinés proposés via différents outils de surveillance et d'autres sources de l'ESP/CPIP personnalisées afin de répondre aux besoins du consommateur final. Au besoin, ces services peuvent être enrichis en fournissant une analyse de risques adéquate.

Exemples:
- service de détection des incidents;
- modèles maritimes, p.ex. dérivation de modèles (permettant le calcul de l'emplacement probable des navires, en fonction de la dernière position connue et des conditions en mer);
- détection des anomalies (permettant la détection des comportements suspicieux ou atypiques des navires);
- service de trafic maritime, y compris association des positions des navires obtenues via le système automatique d'identification (SAI) et le SAI satellite avec les données relatives aux positions des navires enregistrées par les radars terrestres et satellites.

L'illustration ci-dessous présente la combinaison entre des services distincts et séparés fournis par des fournisseurs internes et externes en un seul service combiné.



3) Liste des services

L'Agence fournira ses services soit de manière régulière, soit de manière ponctuelle, en fonction des besoins. L'Agence met à la disposition des centres nationaux de coordination et l'Agence une liste de services contenant des informations et des détails sur chacun des services fournis de manière habituelle. Lorsqu'un besoin est détecté, un nouveau service qui n'est pas encore inclus sur la liste peut être fourni.

4) Processus de services

L'Agence utilise un cycle de traitement de fourniture de services débutant avec l'introduction d'une demande et terminant par l'activation du service. Ce processus inclut toutes les étapes nécessaires pour assurer

- l'évaluation et la validation nécessaires de la demande de service sur la base d'une série de critères prédéfinis;

- des flux de travail appropriés pour fournir des services standards et concevoir et mettre en œuvre de nouveaux services; et

- la fourniture du service à l'utilisateur.

5) Critères de validation

L'Agence évalue et valide chaque demande de service avant la fourniture de ce dernier. Elle peut soit accepter de fournir le service, soit rejeter la demande pour des raisons techniques, financières ou opérationnelles. Si elle opte pour cette dernière option, elle informe le centre national de coordination compétent et motive son refus.

3.2.9 Politique relative aux données à caractère personnel[43]

3.2.9.1 NSP[44]

Les États membres traitent les données à caractère personnel dans le NSP conformément à leurs dispositions nationales. Chaque État membre traitant des données à caractère personnel dans le cadre de son NSP est notamment chargé d'assurer la sécurité de ces donnes, de fournir une formation appropriée à son personnel et de respecter les règles et exigences nationales en matière de protection des données.

Les États membres veillent à ce qu'une fois expiré le délai de conservation des données défini par la législation nationale, les données à caractère personnel soient supprimées ou rendues anonymes conformément aux dispositions du droit national. Dès que le NSP inclut des données à caractère personnel, le traitement de ces données doit être enregistré dans un journal afin de disposer d'une trace d'audit.

3.2.9.2 ESP et CPIP[45]

Le centre national de coordination doit veiller à ce qu'aucune donnée à caractère personnel autre que celles relatives aux numéros d'identification des navires ne soit chargée dans l'ESP/CPIP. Pour éviter tout risque d'inclusion involontaire de données à caractère personnel dans l'ESP/CPIP, les États membres doivent créer un mécanisme de validation au niveau de leur centre national de coordination afin de pouvoir s'assurer que les informations transmises à l'ESP/CPIP ne contiennent aucune donnée à caractère personnel lorsqu'elles quittent le NSP. Ce mécanisme de validation peut consister

- à éviter les «copier-coller» depuis les bases de données nationales, si celles-ci contiennent des données à caractère personnel;

- à relire une dernière fois le texte inséré (en particulier les champs de texte libre) avant l'envoi, en vérifiant particulièrement la présence de données à caractère personnel;

[43] Article 13 du règlement (UE) n° 1052/2013
[44] Article 13, paragraphe 1, du règlement (UE) n° 1052/2013
[45] Article 13, paragraphe 2, du règlement (UE) n° 1052/2013

- à demander aux utilisateurs de faire attention au contenu des documents qu'ils joignent à leurs objets ainsi qu'au contenu des documents indépendants, qui sont susceptibles d'inclure des données à caractère personnel.

Les mécanismes du réseau de communication d'Eurosur (ECN) devraient pouvoir empêcher le partage des données stockées dans le NSP et qualifiées de «données à caractère personnel» par le propriétaire des informations (p.ex. le centre national de coordination) avec d'autres centres nationaux de coordination, à l'exception de celles autorisées dans l'ESP/CPIP.

Si l'Agence rencontre des données à caractère personnel autre que celles ayant trait aux numéros d'identification de navires dans l'ESP/CPIP, elle doit en avertir le propriétaire/créateur des données (p.ex. le centre national de coordination) et demander leur suppression. Le propriétaire des données doit alors les supprimer de l'ESP/CPIP.

L'Agence coopère dans ce domaine avec le contrôleur européen de la protection des données (CEPD).

3.2.9.3 Échanges bilatéraux entre les États membres voisins[46]

Si des États membres voisins utilisent l'ECN pour des échanges bilatéraux d'informations, les données à caractère personnel doivent en être exclues. Cela n'empêche pas les États membres de procéder à des échanges bilatéraux de données à caractère personnel via des canaux de communication spécifiques, conformément aux règles nationales et européennes en matière de protection des données.

3.3 Capacité de réaction[47]

3.3.1 Définition et volets

La capacité de réaction est la capacité de prendre des mesures en vue de lutter contre les activités transfrontalières illégales aux frontières extérieures, ou le long ou à proximité de celles-ci, y compris les moyens disponibles et les délais nécessaires pour réagir correctement. Elle représente également l'un des facteurs clés contribuant à protéger et à sauver la vie de migrants. Les autorités nationales responsables de la surveillance des frontières extérieures doivent pouvoir réaffecter les ressources (p.ex. personnel, équipement et moyens) pour réagir rapidement à tout changement observé aux frontières extérieures terrestres et maritimes et, le cas échéant, aux points de passage frontaliers.

La capacité de réaction comporte deux volets:

- La *capacité de réaction physique* désigne la disponibilité de ressources humaines et techniques suffisantes (p.ex. du personnel formé, des systèmes et des moyens) pour permettre une réaction appropriée en cas de menace soudaine ou d'activité illégale.

Recommandation: surveiller les tronçons de frontière extérieure à l'aide d'équipements fixes et mobiles qui répondent au moins aux exigences définies pour les tronçons à faible niveau d'impact.

- La *capacité de réaction procédurale* désigne l'existence de processus et de procédures permettant aux autorités de planifier, lancer et mener des opérations visant contrer efficacement et rapidement des menaces ou des activités transfrontalières illégales.

[46] Voir l'article 9, paragraphes 9 et 10, du règlement (UE) n° 1052/2013.
[47] Voir les articles 14 à 17 du règlement (UE) n° 1052/2013.

Recommandation: pour chaque tronçon de frontière extérieure, même ceux qui présentent systématiquement un faible niveau d'impact, mettre en place une procédure ou un mécanisme d'activation de ressources supplémentaires, en cas de menace soudaine ou de hausse subite du niveau d'impact.

3.3.2 Planification de la capacité de réaction

Les centres nationaux de coordination organisent et exécutent des *simulations* de scénarios envisageables et évaluent les mesures de réaction appropriées. Cela leur permettra

- de définir, structurer et coordonner les mesures de réaction utiles incombant aux autorités nationales chargées de la surveillance des frontières sur les différents tronçons de frontière extérieure et de soutenir les mesures prises par les autres autorités nationales;

- d'évaluer la capacité globale de réaction et de recenser les éventuelles améliorations à apporter.

Recommandation: élaborer des plans pour faire face aux arrivées massives et soudaines de ressortissants de pays tiers.

La planification de la capacité de réaction peut être scindée en mesures prises au niveau local, régional, national et international. Dans la mesure du possible, le centre national de coordination doit jouer le rôle d'organisme de coordination et d'échange d'informations. Si un État membre a déjà élaboré de tels plans, il doit vérifier s'ils répondent aux exigences du présent manuel et, le cas échéant, les adapter en conséquence.

Meilleure pratique: faire en sorte que la planification de la capacité de réaction puisse couvrir tous les tronçons de frontière:

- description du tronçon de frontière extérieure (configuration des lieux, informations géopolitiques, environnementales) et aperçu de l'analyse des risques ;

- ressources disponibles au sein des autorités nationales chargées de la surveillance des frontières et des autorités de soutien (ressources humaines et techniques, localisation de celles-ci, quantité, temps de réaction, canaux de communication) ;

- autorités situées à proximité des tronçons de frontière extérieure du ou des États membres voisins et leurs ressources;

- autorités situées à proximité des tronçons de frontière du ou des États tiers voisins et leurs ressources ;

- règles d'engagement relatives à chaque réaction décidée conjointement pour faire face aux différents scénarios ;

- dispositions relatives aux mécanismes de protection des droits fondamentaux, y compris la protection internationale et la protection des groupes vulnérables en cas d'arrivées massives.

La capacité de réaction doit pouvoir être adaptée à l'évolution de la situation.

Recommandation: la capacité de réaction doit être planifiée séparément pour les niveaux d'impact faible, moyen ou élevé attribués aux tronçons de frontière extérieure, et comprendre une description des mesures à prendre en cas de modification du niveau d'impact d'un de ces tronçons. Les plans doivent également prévoir le déploiement d'équipes nationales d'intervention rapide ainsi que les activités et ressources de soutien de l'Agence.

3.3.3 Délégation des tâches au niveau local et régional[48]

Les États membres peuvent déléguer une partie des responsabilités des centres nationaux de coordination aux autorités régionales, locales, fonctionnelles ou autres qui sont à même de prendre des décisions opérationnelles assurant une capacité de réaction dans leurs domaines de compétence respectifs. Cette délégation ne doit pas affecter le rôle des centres nationaux de coordination en tant que points de contact uniques pour la coopération et l'échange d'informations avec les autres centres nationaux de coordination et l'Agence.

3.3.4 Tronçons de frontière

Chaque État membre doit diviser ses frontières extérieures terrestres et maritimes en tronçons de frontière et communiquer ceux-ci à l'Agence[49]. Il doit également signaler à l'Agence toute modification à cet égard.

La zone couverte par un tronçon de frontière correspond à la zone de responsabilité d'un centre local ou régional, ce qui permet d'assurer la gestion efficace du personnel et des ressources.

Sur demande de l'Agence, les États membres fournissent à celle-ci les informations relatives:

- aux tronçons de frontière et aux points de passage frontaliers;
- à la caractérisation des tronçons de frontière;
- aux limites des tronçons de frontière.

L'Agence doit assigner un identifiant unique à chaque tronçon de frontière nouvellement créé, puis l'inclure dans la liste des tronçons de frontière Eurosur.

3.3.5 Niveaux d'impact des tronçons de frontière

Au moment d'évaluer les niveaux d'impact Eurosur, il convient de tenir compte des trois composantes du risque (menace, vulnérabilité et impact), en utilisant le modèle CIRAM pour l'analyse des risques élaboré par l'Agence:

1) la menace doit être évaluée en termes d'impact et de probabilité qu'elle se concrétise;
2) la vulnérabilité à la menace: niveau et efficacité de la riposte;
3) l'impact: si la menace se concrétisait.

[48] Article 17 du règlement (UE) n° 1052/2013

[49] Les tronçons de frontière ainsi définis par un État membre sont sans préjudice du statut d'un territoire ou de la souveraineté d'un État sur celui-ci, de la délimitation des frontières internationales ou du nom des territoires, villes ou régions.

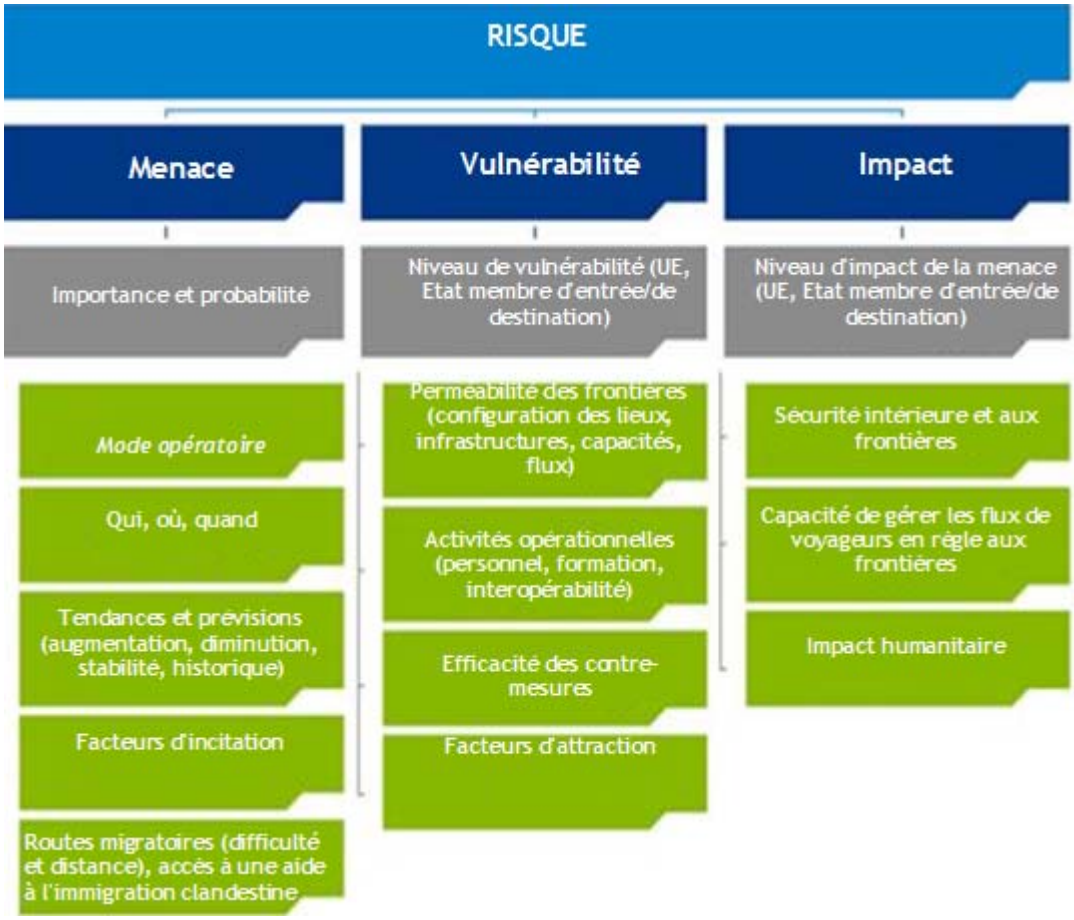


Tableau: Composantes du risque (CIRAM)

3.3.5.1 Évaluation du niveau d'impact par l'Agence

L'Agence doit procéder régulièrement à l'évaluation des niveaux d'impact Eurosur.

L'Agence évalue les variables décrivant les menaces en s'appuyant sur le modèle CIRAM. Des séries de variables sont examinées afin de déterminer le niveau de la menace pour chaque tronçon de frontière, en accordant une attention particulière aux évolutions clés affectant le *niveau de la menace*. Les principaux facteurs sont les suivants:

1) les tendances statistiques décrivant l'évolution des chiffres en rapport avec les franchissements illégaux des frontières terrestres et maritimes, compte tenu des données de référence historiques comparées avec celles de la situation actuelle;
2) les facteurs d'incitation géopolitiques et naturels facilitant les activités criminelles transfrontalières ou motivant les migrants potentiels à quitter leur pays d'origine/de transit. Il convient d'opérer une distinction entre les pays d'origine et de transit;
3) les facteurs influençant la criminalité transfrontalière et la circulation des migrants dans les pays d'origine et de transit bordant les routes migratoires qui mènent vers les États membres;
4) l'analyse de l'aide à l'immigration clandestine, y compris l'étude des activités et des caractéristiques des réseaux de passeurs le long des routes de transit et dans les pays de départ les plus récents.

Les principaux facteurs à prendre en considération au moment d'évaluer le niveau de vulnérabilité sont:

1) l'évaluation des facteurs d'incitation concernant les pays de destination et les pays de transit;
2) la capacité des autorités de contrôle aux frontières/la perméabilité des frontières;
3) les politiques européennes et nationales dans le domaine de la migration et du maintien de l'ordre;
4) la capacité des autorités à lutter contre les réseaux criminels.

Les facteurs d'impact du modèle CIRAM seront également évalués, y compris:

1) les besoins humanitaires et les questions ayant trait aux droits fondamentaux;
2) les aspects ayant une incidence sur la sécurité publique et le contrôle aux frontières.

3.3.5.2 Modification des niveaux d'impact des tronçons de frontière

Le niveau d'impact d'un tronçon de frontière peut être modifié à tout moment. Une demande d'actualisation du niveau d'impact peut émaner du ou des États membres concernés, qui la transmettent via le centre national de coordination, ou de l'Agence. En règle générale, le niveau d'impact est mis à jour lorsque les États membres et l'Agence conviennent de le faire.

L'Agence procède à l'examen et à la révision des niveaux d'impact régulièrement, ainsi que sur une base ponctuelle.

3.3.5.3 Délais

Les centres nationaux de coordination et l'Agence doivent respecter un délai limite pour transmettre leur réponse initiale aux demandes de modification du niveau d'impact. Lorsqu'aucune réponse n'a été obtenue du centre ou de l'Agence passé ce délai, un accord tacite est réputé donné. Dans ce cas, les niveaux d'impact recommandés par le centre national de coordination ou l'Agence sont attribués et inclus dans l'ESP. L'attribution des niveaux d'impact s'accompagne alors d'un avertissement indiquant clairement la nature tacite de l'accord.

Lorsque la réponse initiale à la demande de modification est négative, des négociations sont entamées en vue d'un accord bilatéral, jusqu'à l'expiration d'un deuxième délai. Si, au terme de ces discussions, un accord n'a pas pu être trouvé sur l'attribution d'un niveau d'impact à un tronçon de frontière spécifique, les niveaux d'impact recommandés par l'Agence sont attribués et inclus dans l'ESP. L'attribution des niveaux d'impact s'accompagne alors d'un avertissement indiquant clairement la position divergente.

Ces délais ont été établis afin de faire en sorte que les modifications des niveaux d'impact soient apportées dans un délai raisonnable et harmonisé, afin d'assurer l'attribution standardisée des niveaux d'impact.

3.3.6 Réactions en fonction des niveaux d'impact[50]

Il incombe aux États membres en premier lieu de garantir une réaction appropriée à la situation observée aux frontières extérieures. Ils doivent s'assurer que les actions de surveillance menées aux tronçons de frontière extérieure correspondent aux niveaux d'impact attribués. En cas d'évolution rapide et/ou inattendue de la situation, les États membres doivent avoir une réaction appropriée.

[50] Article 16 du règlement (UE) n° 1052/2013

3.3.6.1 Rôles des centres de coordination

Les États membres peuvent, en fonction de la répartition nationale des responsabilités, structurer comme suit leurs activités nationales de surveillance des frontières:

Le *centre local de coordination*, responsable d'un tronçon de frontière terrestre ou maritime, exécute les tâches suivantes:

- fournir des orientations au niveau local;
- assurer la planification détaillée et la mise en œuvre des opérations;
- collecter et traiter les informations nécessaires à la mise en œuvre des opérations;
- organiser une surveillance régulière sur la base d'une analyse des risques;
- veiller à ce que des ressources et du personnel suffisants soient maintenus dans la zone frontalière et prêts pour des actions de pistage, d'identification et d'interception;
- choisir les actions à entreprendre en temps quasi-réel pour exécuter l'opération;
- demander l'aide du centre de coordination régional/national;
- veiller à ce que la patrouille ou le centre local de coordination transmette au centre national de coordination en temps quasi-réel les informations relatives à tous les incidents survenus sur le tronçon de frontière extérieure;
- s'assurer que les informations relatives à toutes les opérations de recherche et de sauvetage le long du tronçon de frontière extérieure sont directement communiquées par la patrouille et en priorité au centre de coordination des opérations de sauvetage en mer (MRCC) et aux services d'urgence;
- lorsqu'un tronçon de frontière se voit attribuer un niveau d'impact moyen ou élevé, le centre local de coordination fournit au centre national de coordination et au centre régional de coordination un rapport hebdomadaire sur les mesures prises.

Meilleure pratique:

mettre en place des lignes de communication directes et sûres entre le centre local de coordination et les patrouilles actives sur le tronçon de frontière.

Le centre local de coordination doit disposer de suffisamment de ressources et de personnel pour assurer une surveillance régulière sur la base d'une analyse des risques. Il convient de localiser des ressources et du personnel supplémentaires qui pourront être mis à la disposition du centre en cas de relèvement à «moyen» ou «élevé» du niveau d'impact d'un tronçon de frontière.

Le *centre régional de coordination ou un autre centre fonctionnel de coordination* couvre un type de tronçon de frontière (p.ex. terrestre ou maritime), plusieurs tronçons de frontière d'une zone géographique ou une tâche spécifique dans l'ensemble des tronçons de frontière (p.ex. contrôles douaniers ou recherche et sauvetage). Il accomplit les tâches suivantes:

- fournir des orientations au niveau régional/fonctionnel;

- superviser la planification et la mise en œuvre des opérations;
- collecter et traiter les informations nécessaires à la planification des opérations;
- veiller à ce que les mesures de surveillance adéquates soient prises à chaque tronçon de frontière et avertir le centre national de coordination des mesures adoptées et de leurs résultats;
- réaffecter les ressources et le personnel (p.ex. entre les différents tronçons de frontière);
- demander l'aide du centre national de coordination;
- veiller à ce que la patrouille ou le centre local transmette en temps utile les informations sur tous les incidents survenus le long du tronçon de frontière extérieure au centre de commandement et de contrôle (s'il existe) de l'autorité nationale compétente, ainsi qu'à l'ICC, le cas échéant, en instaurant un mécanisme de notification adéquat;
- récapituler et analyser pour le centre national de coordination les informations transmises par les centres locaux de coordination;
- lorsqu'un tronçon de frontière a reçu le niveau d'impact moyen, veiller à ce que le centre local de coordination compétent reçoivent les ressources et le personnel supplémentaires dont il a besoin dans un délai de *deux semaines*.

Meilleure pratique: création de flux de travail permettant de réaffecter rapidement les ressources et le personnel d'un tronçon de frontière à un autre, y compris, si nécessaire, un flux de travail permettant au centre régional de coordination ou au centre fonctionnel de coordination de demander l'aide du centre national de coordination.

Le *centre national de coordination*, responsable de l'ensemble des tronçons de frontière, exécute les tâches suivantes:

- fournir des orientations au niveau national;
- convenir de modalités de travail et d'un dispositif de liaison avec les autorités nationales compétentes, le cas échéant;
- soutenir la planification globale des opérations nationales et surveiller leur bonne mise en œuvre;
- traiter les informations et les analyses de risques nécessaires pour appuyer la planification des opérations;
- coordonner le soutien apporté au niveau national (p.ex. par les différentes autorités nationales);

- veiller à ce que le centre national de coordination transmette à l'Agence les informations sur tous les incidents survenus aux frontières extérieures au plus tard quatre heures après les avoir reçues du centre local de coordination;

- Si un niveau d'impact élevé a été attribué à un tronçon de frontière, le centre national de coordination

- veille à ce que le centre local de coordination reçoive des ressources et du personnel supplémentaires dans un délai de trois semaines;

- demande l'aide de l'Agence; celle-ci répond (par la positive ou la négative) à la demande d'aide du centre national de coordination dans un délai de cinq jours ouvrables, en indiquant le temps que durera l'aide apportée ainsi que l'ampleur de celle-ci;

- informe régulièrement (de préférence quotidiennement) l'Agence des mesures prises et lui soumet chaque mois un rapport de synthèse sur les mesures adoptées[51]. L'Agence se servira de ces rapports pour ses évaluations régulières des tronçons de frontière.

Meilleure pratique:

mise en place de canaux de communication directs et sécurisés entre le centre national de coordination et les centres régionaux/fonctionnels/locaux de coordination et les autres autorités nationales compétentes.

Définition de règles pour les flux de travail, les échanges d'informations classifiées et non classifiées et la coopération quotidienne entre le centre national de coordination et les centres régionaux/locaux de coordination.

Le centre national de coordination dispose d'une vue d'ensemble des ressources et du personnel déployés à chaque tronçon de frontière ainsi qu'une vue d'ensemble des ressources supplémentaires et du personnel disponibles au niveau national pouvant être affectés aux tronçons de frontière ayant un niveau d'impact élevé.

Lorsque des niveaux d'impact différents ont été attribués à des tronçons de frontière extérieure adjacents, le ou les États membres concernés peuvent définir des zones potentiellement critiques à l'intérieur du tronçon de frontière et consacrer des ressources supplémentaires à la surveillance des frontières dans ces zones.

3.3.6.2 Niveau d'impact faible

Pour les tronçons de frontière à faible niveau d'impact, l'État membre doit conserver des ressources suffisantes dans la zone frontalière. Au niveau local et régional, des réserves de ressources doivent être localisées et pouvoir être utilisées sur demande.

3.3.6.3 Niveau d'impact moyen

Si un niveau d'impact moyen a été attribué à un tronçon de frontière extérieure, l'État membre doit, en plus des activités décrites ci-dessus, accroître le niveau de surveillance en adoptant des mesures supplémentaires. Dans le cadre de leurs activités, les États membres

[51] Le centre national de coordination peut, le cas échéant, combiner ces rapports avec les rapports de l'ICC.

doivent faire usage de l'analyse des risques et des outils de surveillance à leur disposition. Le centre national de coordination doit être informé de l'adoption de ces mesures de surveillance. Il peut, sur demande ou de sa propre initiative, apporter un soutien afin de renforcer les ressources sur ce tronçon de frontière.

Meilleure pratique: au niveau stratégique, le centre national de coordination assure la surveillance de la situation, effectue une analyse des risques et contribue à la gestion des ressources et du personnel, y compris à la planification des réserves.

Au niveau opérationnel et tactique, le centre régional de coordination et le centre local de coordination mettent en œuvre les mesures de surveillance supplémentaires et intensifient les activités de contrôle aux frontières, surtout dans les zones qualifiées de critiques sur le tronçon de frontière concerné.

3.3.6.4 4.5.6.4. Niveau d'impact élevé

Lorsqu'un niveau d'impact élevé est attribué à un tronçon de frontière extérieure, l'État membre doit veiller à ce que des mesures de surveillance plus strictes soient prises au niveau national.

Meilleure pratique: le centre national de coordination

- désigne un agent responsable de la surveillance et de la gestion de la situation au tronçon de frontière extérieure concerné ;
- bénéficie de renforts afin de pouvoir gérer les besoins accrus d'échanges d'informations, d'analyse des risques et de coopération au niveau national et avec les pays voisins ;
- lance, au besoin, la task-force d'urgence composée de toutes les autorités concernées
- gère la participation des autres autorités nationales ;
- évalue la situation et, au besoin, sollicite l'aide de l'Agence.
- Le niveau local/régional:
- déploie des ressources supplémentaires sous la coordination de l'autorité nationale chef de file ;
- tient le centre national de coordination informé de toutes les mesures prises et de leur impact.

L'Agence dispose de procédures distinctes pour apporter l'aide indiquée ci-dessus. Si cela se justifie, l'Agence a le droit de refuser les demandes d'aide au cas par cas.

3.3.7 Coopération avec les pays tiers voisins

Lorsqu'un niveau d'impact moyen ou élevé est attribué à un tronçon de frontière extérieure adjacent à un autre État membre ou à un pays avec lequel existent des accords ou des réseaux régionaux, le centre national de coordination prend contact avec le pays voisin et coordonne les mesures transfrontalières nécessaires. Les États membres doivent également s'efforcer de renforcer la coopération avec les pays tiers avec lesquels ils partagent une frontière à laquelle un niveau d'impact moyen ou élevé a été attribué.

La coordination entre pays voisins doit reposer sur des accords bilatéraux pertinents conformes à des normes et standards équivalents à ceux définis par le droit européen et international. Si possible, le centre national de coordination devrait informer les autres centres nationaux de coordination de l'existence de ces accords, afin que les autres États membres puissent lui demander de faciliter les échanges d'informations avec ce pays tiers en cas de

besoin opérationnel. Les moyens potentiels de renforcer la coordination entre les pays voisins consistent notamment à:

- convenir d'une langue et d'une terminologie communes;
- mettre en place des mécanismes d'échange d'information;
- échanger des tableaux de situation relatifs aux tronçons de frontière d'États membres voisins;
- effectuer régulièrement des activités conjointes - p.ex. des patrouilles communes et des opérations conjointes entre États membres;
- créer des procédures communes afin de faciliter la collaboration dans des scénarios spécifiques.

3.3.8 Évaluation

Dans ses rapports d'analyse des risques, l'Agence évaluera, avec le ou les États membres concernés, l'attribution des niveaux d'impact ainsi que les mesures prises en conséquence au niveau national et européen. Le temps de réaction constitue une mesure appropriée pour évaluer la capacité de réaction. Au niveau tactique, il s'agit du temps nécessaire pour traiter une alerte, déplacer les ressources vers le point sensible et se préparer à intervenir contre la violation des frontières; il débute au moment de la détection et se termine lorsque toutes les ressources sont mises en place et tous les préparatifs opérationnels ont été achevés.

4 Lignes directrices techniques

4.1 Réseau de communication Eurosur[52]

4.1.1 Rôles et responsabilités

Le réseau de communication Eurosur (ECN) a été créé sous la forme d'un réseau de *nœuds* échangeant des informations. Un nœud est une gamme complète de matériel et de logiciels livrés par l'Agence aux centres nationaux de coordination afin que chacun d'entre eux puisse partager ses informations avec les autres centres ainsi qu'avec l'Agence et accéder aux services d'information fournis par l'Agence. La maintenance et le support relatifs à l'ECN sont assurés par les *services de gestion technique d'Eurosur (EMTS).*

Le centre national de coordination doit assurer la fourniture, la maintenance et le support d'un liaison internet qui sert à connecter le nœud à l'ECN. La vitesse de connexion minimale requise est de 10 Mbit/s. Une bande passante plus importante peut être nécessaire en fonction du type d'utilisation et du nombre d'utilisateurs qui se servent en même temps de l'ECN dans l'État membre.

Les obligations incombant à l'Agence et aux États membres qui reçoivent le nœud sont présentées en détail dans le protocole d'accord réglementant l'utilisation opérationnelle de l'ECN, sa gestion technique et le scénario de base en matière de sécurité à mettre en œuvre. L'Agence reste propriétaire du matériel et des logiciels de l'ECN et est responsable de leur maintenance et de leur développement.

[52] Article 7 du règlement (UE) n° 1052/2013.

L’Agence prête assistance aux utilisateurs des nœuds par l'intermédiaire des administrateurs informatiques des nœuds et du point de contact technique Eurosur dans chaque centre national de coordination. L’ECN est opérationnel 24h sur 24, 7 jours sur 7, sauf lors d’éventuelles périodes de maintenance.

4.1.2 Gestion de l’application

L’application et les services Eurosur font l'objet d'un développement e d'une maintenance assurés par l’Agence conformément au protocole d’accord. Les modifications apportées à l’application respectent la procédure de gestion des modifications décrite au point 4.4. L’Agence planifie les publications des versions de l’application ainsi que leur contenu et communique les détails à tous les nœuds préalablement à ces publications. Tous les nœuds sont informés de l’état d’avancement du déploiement et des résultats. Chaque application et chaque système d’un nœud et de l’ECN doivent respecter, le cas échéant, les normes établies par:

l’Open Geospatial Consortium;

- l’Open Web Application Security Project;
- l’Open Source Security Testing Methodology Manual .

4.1.3 Services de gestion technique d’Eurosur

Les ETMS sont situés au siège de l’Agence. Cette dernière est responsable de la fourniture de ces services aux centres nationaux de coordination. Les principales responsabilités de l’Agence à cet égard sont:

1. la gestion de l’ECN et la maintenance du système;
2. le développement du matériel et des logiciels de l’ECN, en fonction des procédures de modification décrites au chapitre 4.4;
3. l’extension de l’ECN dans de nouveaux endroits;
4. la garantie de la sécurité de l’ECN;
5. l’assistance fournie au personnel du centre national de coordination (point de contact technique et administrateur informatique) et à tous les utilisateurs de l’Agence.

Les centres nationaux de coordination des États membres peuvent accéder aux ETMS 24h sur 24, 7 jours sur 7.

Les ETMS comprennent:

1) Infrastructure et application(s)

- *Assistance et résolution des problèmes*: aider à résoudre les incidents et problèmes informatiques susceptibles de survenir dans l’ECN et fournir aux centres nationaux de coordination des informations et des conseils sur les applications et l’infrastructure Eurosur.
- *Gestion des utilisateurs et des rôles*: aider les administrateurs informatiques des nœuds à créer, modifier et supprimer les comptes d’utilisateurs et à assigner des rôles Eurosur aux comptes d’utilisateurs.
- *Surveillance*: surveiller le statut et le fonctionnement du système dans l’infrastructure informatique et entre les nœuds.
- *Mises à jour*: installer les dernières mises à jour logicielles afin d’éliminer toutes les vulnérabilités et tous les virus grâce aux nouvelles versions.
- *Sauvegarde*: vérifier quotidiennement le statut de sauvegarde de l’infrastructure des ETMS et des nœuds Eurosur.

2) Sécurité

- *Cloisons pare-feu:* surveillance des évènements, résolution des problèmes, création, modification et suppression des règles du pare-feu pour l'ECN entier - à l'exception des cloisons pare-feu déployées par les centres nationaux de coordination.
- *Système de prévention des intrusions:* surveillance des évènements, signatures et mises à jour logicielles.
- *Réseau privé virtuel:* surveillance, résolution des problèmes, création, modification et suppression de VPN de site à site entre les nœuds Eurosur et entre les nœuds Eurosur et l'infrastructure des ETMS.
- *Infrastructure à clés publiques:* émission, annulation et renouvellement de certificats numériques et fourniture d'une aide aux administrateurs informatiques des centres nationaux de coordination pour l'installation des nœuds Eurosur.
- *Audits de sécurité:* réalisation d'audits de sécurité périodiques (contrôles de code et tests de pénétration) conformément aux procédures prédéfinies.
- *Documents:* création et mise à jour des documents de sécurité existants.

3) Autres services

- *Documents:* création et mise à jour des documents techniques.
- *Matériel de formation:* élaboration et mise à jour de matériel de formation et de manuels d'utilisateur.
- *Formation technique:* fourniture d'une formation technique au personnel technique des centres nationaux de coordination et de l'Agence.
- *Formation opérationnelle:* fourniture d'une formation opérationnelle au personnel opérationnel des centres nationaux de coordination et de l'Agence.

4.1.4 Administrateur informatique de nœud et tâches correspondantes

Un administrateur informatique de nœud est chargé, au sein du centre national de coordination, d'apporter un soutien technique au nœud de l'Agence, en fonction des tâches qui lui sont attribuées par l'Agence (p.ex. créer de nouveaux comptes d'utilisateur), et d'effectuer des actions techniques spécifiques selon les instructions de l'Agence (p.ex. redémarrage de services, redémarrage du matériel, etc.). Chaque centre national de coordination doit disposer d'au moins un (de préférence deux) administrateur informatique de nœud afin d'exécuter les tâches suivantes:

1) installer les certificats envoyés par l'Agence;

2) assurer la maintenance du point d'accès à l'internet utilisé pour l'ECN;

3) gérer les comptes d'accès utilisateurs;

4) gérer les comptes e-mail du domaine Eurosur;

5) aider les ETMS à exécuter les tâches impossibles à effectuer à distance;

6) demander l'aide des ETMS pour les problèmes ne pouvant être traités au niveau local;

7) surveiller le fonctionnement du nœud national de l'ECN;

8) signaler à l'Agence les dysfonctionnements et les incidents techniques;

9) analyser les éventuels incidents techniques en rapport avec le système informatique qu'il a détectés ou qui relèvent de la responsabilité de l'État membre (p.ex. panne d'un

dispositif du réseau de l'État membre empêchant certains utilisateurs d'accéder à l'ECN)[53];

10) signaler à l'Agence les problèmes qui nécessitent son intervention ou informer l'Agence de tous les problèmes affectant la connexion avec l'internet;

11) signaler tout problème de sécurité rencontré dans l'ECN à l'agent de sécurité informatique du centre national de coordination ainsi que tout problème de sécurité détecté dans le système national connecté à l'ECN et susceptible de compromettre la sécurité de l'ECN.

4.1.5 Mise en œuvre des modifications techniques

Toute modification apportée à l'ECN ou à l'infrastructure sous-jacente susceptible d'avoir une incidence sur l'ECN, le réseau d'une autre partie ou les connexions en place doit faire l'objet d'une procédure de gestion des modifications impliquant l'autre partie en tant que partie prenante. Les informations doivent être fournies par écrit à l'autre partie suffisamment à l'avance. La procédure de gestion des modifications doit être respectée comme indiqué dans le protocole d'accord, dans les procédures opérationnelles en matière de sécurité de l'ECN et dans les procédures internes de l'Agence, afin de maintenir un niveau constant de sécurité et d'homologation.

Toute modification de l'environnement technique de l'ECN ayant une incidence sur la disponibilité du système doit être annoncée au préalable par l'Agence (p.ex. pour les modifications apportées au nœud) ou par les États membres (p.ex. pour les modifications de l'infrastructure internet utilisée pour établir les liens VPN entre les nœuds, ou les modifications des interconnexions). Les changements impliquant une modification du système de l'autre partie doivent être annoncés suffisamment à l'avance, en tenant compte de l'impact de la modification apportée au système de l'autre partie et de du temps estimé nécessaire pour étudier, concevoir et mettre en œuvre ces changements.

4.1.6 Manuels de l'utilisateur

L'Agence, via les ETMS, crée, met à jour et distribue des manuels de l'utilisateur pour les applications et services utilisateurs disponibles dans l'ECN. Tous ces manuels doivent être actualisés en fonction des dernières évolutions.

4.2 Formation

Tous les utilisateurs d'Eurosur (personnels des centres nationaux de coordination et de l'Agence) doivent recevoir une formation adéquate pour pouvoir exécuter les tâches qui leur sont assignées dans le cadre d'Eurosur et ainsi assurer le fonctionnement d'Eurosur. Les catégories de formation ci-dessous tiennent compte des différents besoins des utilisateurs. Le recensement des besoins de formation et la définition des priorités de formation relèvent d'une collaboration permanente entre l'Agence et les centres nationaux de coordination. Les besoins de formation sont indiqués dans le plan de formation annuel d'Eurosur, élaboré par l'Agence. Les activités de formation sont organisées soit sur la base de ce plan de formation, soit en fonction de la demande des utilisateurs.

[53] Cette tâche peut être assignée à la fonction de soutien informatique du centre national de coordination (p.ex. le bureau d'assistance), pour autant qu'elle soit en mesure de déterminer quel système a provoqué l'incident technique (l'infrastructure informatique de l'État membre ou l'infrastructure en nœuds de l'ECN).

Catégories de formation	1. Formation des centres nationaux de coordination	2. Formation technique et informatique	3. Formation aux applications
Public cible	Personnel des centres nationaux de coordination (p.ex. cadres, opérateurs, analystes, informaticiens)	Administrateurs informatiques de l'ECN (administrateurs système, spécialistes des réseaux)	Formateurs des États membres (formateurs multiplicateurs)
Contenu	1. Gestion des affaires quotidiennes et gestion des crises, y compris respect des droits fondamentaux 2. Échange d'expériences et de bonnes pratiques 3. Amélioration de la coopération entre les centres nationaux de coordination, y compris échanges de personnel	1. Architecture de l'ECN 2. Tâches de maintenance	1. Utilisation de l'application par les différents rôles (observateur ou opérateur) 2. Gestion des applications pour les gestionnaires de l'information et les gestionnaires d'applications
Organisation et calendrier	Prévue: périodique pour tous les centres nationaux de coordination À la demande: au niveau régional/bilatéral	Prévue: périodique ou en fonction des changements (p.ex. nouvelle publication/nouveau composant) À la demande: p.ex. un problème technique spécifique est détecté ou un changement spécifique est nécessaire	Prévue: périodique ou en fonction des changements (p.ex. nouvelle publication/nouveau composant)
Dispensée par:	Certains centres nationaux de coordination accueillant la formation, en coopération avec l'Agence	L'Agence	Les formateurs nationaux des États membres et l'Agence

Catégories de formation	4. Formation opérationnelle/sur un contenu	5. Formation pour le développement des compétences	6. Formation personnalisée
Public cible	Certains utilisateurs, en fonction de certains rôles et responsabilités	Certains utilisateurs, en fonction de certains rôles et responsabilités	Certains utilisateurs, en fonction de certains rôles et responsabilités
Contenu	Couche «événements» Couche «analyse» Couche «opérations» Application commune des outils de surveillance	Contenu des services Eurosur (p.ex. analyse d'images satellites, droits fondamentaux, formation sur la sécurité des informations)	Besoin spécifique, par exemple: si des États membres rejoignent Eurosur; interconnexion du système Eurosur avec les systèmes nationaux

Organisation et calendrier	Prévue: périodique ou en fonction des changements (p.ex. déploiement de nouveaux services, nouveaux champs d'information, nouvelles exigences en matière de rapports) À la demande: à la suite de l'identification d'un thème spécifique non inclus dans le plan de formation d'Eurosur	Prévue: périodique ou en fonction des changements (p.ex. déploiement de nouveaux services, nouveaux champs d'information, nouvelles exigences en matière de rapports) À la demande: à la suite de l'identification d'un thème spécifique non inclus dans le plan de formation d'Eurosur	À la demande: p.ex. en raison de circonstances exceptionnelles
Dispensée par:	L'Agence	L'Agence (en coopération avec des partenaires, p.ex. le Centre satellitaire de l'Union européenne)	L'Agence, en coopération avec des partenaires

4.3 Politique de sécurité et gestion de la sécurité[54]

4.3.1 Objectifs de sécurité

L'ECN permet la gestion, le stockage, la transmission et le traitement en toute sécurité d'informations classifiées de l'UE (ICUE) jusqu'au niveau «RESTREINT UE/EU RESTRICTED».

4.3.1.1 Types d'information

L'Agence et les centres nationaux de coordination veillent à ce que les ICUE soient classifiées de manière appropriée, clairement identifiées en tant qu'informations classifiées, et qu'elles ne conservent leur niveau de classification qu'aussi longtemps que nécessaire. L'ECN contient les types suivants d'informations:

- informations classifiées: celles-ci incluent les informations relatives aux ressources et toutes les informations classifiées «RESTREINT UE/EU RESTRICTED» par le propriétaire;

- informations sensibles non classifiées: toutes les informations qui ne sont pas classifiées doivent être considérées comme des informations sensibles non classifiées;

- données à caractère personnel ayant trait aux numéros d'identification de navires et aux données qualifiées de données à caractère personnel par le propriétaire dans le NSP.

Les propriétaires des informations sont responsables de l'attribution, de la mise à jour et de l'abaissement des niveaux de classification de ces informations. L'artéfact relatif aux ressources propres revêt dans l'ECN le marquage «RESTREINT UE/EU RESTRICTED» même s'il n'avait pas été classifié comme tel par son créateur. Les utilisateurs ne peuvent déclasser ces artéfacts. L'autorité d'origine du document doit donner son consentement écrit préalablement au déclassement ou à la déclassification de toute autre ICUE ou à la modification/suppression des marquages.

[54] Voir l'article 7, paragraphes 3, 4 et 5, du règlement (UE) n° 1052/2013.

4.3.1.2 Protection des informations sensibles non classifiées et des informations classifiées «RESTREINT UE/EU RESTRICTED»

L'Agence doit protéger les informations non classifiées et les informations classifiées de l'Union européenne conformément à l'article 11, point d), du règlement (CE) n° 2007/2004, qui exige que l'Agence applique les règles de sécurité de la Commission[55]. Toutes les informations non classifiées dans le cadre d'Eurosur doivent être considérées comme des informations «sensibles non classifiées». Dans l'ECN, ces informations doivent, à chaque fois que cela est techniquement faisable, revêtir le marquage «LIMITÉ».

Lorsque les centres nationaux de coordination partagent avec l'ECN des informations classifiées portant un marquage national de classification de sécurité, l'Agence doit protéger ces informations conformément aux règles applicables aux ICUE à un niveau équivalent, comme indiqué dans le tableau d'équivalence des classifications de sécurité. Les centres nationaux de coordination doivent échanger, traiter et stocker des informations sensibles non classifiées et des informations classifiées dans l'ECN dans le respect des règles nationales et des procédures opérationnelles de sécurité de l'ECN.

4.3.1.3 Habilitations de sécurité du personnel

Les critères utilisés pour déterminer si une personne peut être autorisée à avoir accès à des ICUE tiennent compte de sa loyauté, de son intégrité et de sa fiabilité.

4.3.1.4 Octroi d'un accès à des informations classifiées de l'Union européenne — principes

Une personne ne peut se voir accorder l'accès à des informations classifiées qu'après:

- avoir établi qu'elle avait besoin de connaître ces informations;
- avoir été informée des règles et procédures de sécurité applicables à la protection des ICUE et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations; et
- avoir été autorisée, si les dispositions législatives et réglementaires nationales l'exigent, à accéder aux informations classifiées au niveau pertinent.

4.3.1.5 Contrôle de l'accès des utilisateurs

L'accès à l'ECN et à l'application de l'ECN est géré en fonction des principes de sécurité suivants:

- les autorisations d'accès à l'ECN et à l'application de l'ECN doivent être accordées sur la base d'une identification et d'une authentification individuelles;
- les autorisations d'accès aux utilisateurs doivent être limitées en fonction du principe du «besoin d'en connaître»;
- l'attribution et l'utilisation de comptes à privilèges doivent être minimisées;
- les systèmes informatiques doivent être configurés de telle sorte que cette politique soit techniquement applicable;
- les autorisations accordées aux utilisateurs doivent être régulièrement réexaminées sur la base d'un processus de révision formel.

Les utilisateurs recevront un accès à l'ECN à la suite d'un processus de sécurité consistant au moins à entrer et à valider un identifiant et un mot de passe, conformément aux normes de l'Agence. Cette règle s'applique également aux systèmes interconnectés, à l'exception d'une

[55] Décision (UE, Euratom) n° 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne.

interconnexion via l'interface d'intégration de nœuds d'Eurosur, pour laquelle l'authentification nationale s'applique.

L'Agence et les États membres gèrent leurs utilisateurs en créant, modifiant, verrouillant et supprimant leurs comptes et en leur octroyant les permissions d'accès à l'ECN dont ils ont besoin pour effectuer leurs tâches. Pour ce faire, ils mettent en œuvre une politique de gestion des utilisateurs de l'ECN afin de veiller à ce que la personne compétente dans ce domaine examine attentivement la création éventuelle de comptes et les permissions associées, en s'assurant que l'utilisateur possède au moins une habilitation de sécurité ou une autorisation nationale équivalente de niveau «RESTREINT UE/EU RESTRICTED» ou de niveau national équivalent et en se basant sur le principe du «besoin d'en connaître». Cette personne effectue chaque année un réexamen des utilisateurs de l'ECN et de leurs permissions. À la suite de ce réexamen, elle apporte les éventuelles modifications nécessaires au statut des comptes et à leurs permissions.

Des règles et exigences détaillées sont établies dans les documents d'homologation.

4.3.2 Mesures physiques de sécurité

Les ICUE classifiées «RESTREINT UE/EU RESTRICTED» peuvent être traitées dans les «zones administratives». L'Agence et les centres nationaux de coordination doivent s'assurer qu'une zone répond aux exigences établies avant de pouvoir être désignée comme zone administrative. Concrètement:

- un périmètre défini est établi de façon visible afin de permettre le contrôle des personnes et, dans la mesure du possible, des véhicules;
- ne peuvent y pénétrer sans escorte que les personnes dûment autorisées par l'autorité compétente; et
- toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

4.3.3 Protection des informations traitées dans les systèmes de communication et d'information

4.3.3.1 Homologation de l'ECN

L'ECN et les systèmes de communication et d'information interconnectés doivent être soumis à un processus d'homologation conformément au protocole d'accord conclu entre les États membres et l'Agence. Ce processus d'homologation permet de s'assurer que toutes les mesures de sécurité nécessaires ont été prises et que les ICUE et le système de communication et d'information ont été suffisamment protégés. La déclaration d'homologation détermine le niveau maximal de classification des informations qui peuvent être traitées dans un système de communication et d'information donné ainsi que les modalités correspondantes. Le processus d'homologation est géré par l'Agence, en qualité de autorité d'homologation, avec le soutien des États membres et conformément aux lignes directrices de la Commission européenne sur l'homologation de sécurité des systèmes informatiques.

Les modifications apportées au système devront tenir compte de la nécessité de maintenir le niveau de sécurité le plus élevé possible. Il conviendra pour cela d'évaluer les risques associés à ces modifications, de définir et de mettre en oeuvre des mesures d'atténuation appropriées et de tester régulièrement l'efficacité de ces mesures d'atténuation. Des changements importants apportés à l'ECN pourraient exiger de procéder à une nouvelle homologation intégrale de l'ECN, en fonction du résultat de l'évaluation des risques effectuée pour mesurer l'impact des modifications sur la sécurité.

4.3.3.2 Connexion d'autres systèmes au réseau

L'ECN peut être connecté à d'autres systèmes, pour autant que les conditions établies à l'article 6 et aux annexes 1 et 5 du protocole d'accord soient respectées. Dans ces cas de figure, les exigences en matière d'homologation sont définies dans le protocole d'accord.

4.3.4 Rôles et responsabilités en matière de sécurité

4.3.4.1 Rôles de sécurité au sein de l'Agence

Autorité d'homologation de sécurité	L'Agence est l'autorité d'homologation de sécurité pour l'ECN. Elle est responsable du domaine général de la sécurité ainsi que des domaines spécialisés de la sécurité de l'information, de la sécurité de la communication et de la crypto-sécurité.
Responsable de la sécurité de l'ECN	Le responsable de la sécurité de l'Agence est également le responsable de la sécurité de l'ECN. Il est chargé de superviser la protection globale des ICUE.
Agent de sécurité informatique au niveau central de l'ECN	L'agent chargé de la sécurité de l'information à l'Agence est l'agent de sécurité informatique au niveau central de l'ECN. Il est chargé de veiller au maintien du niveau de sécurité adéquat de l'ECN et de s'assurer que tous les incidents informatiques signalés soient enregistrés, analysés et résolus, en contact étroit, si nécessaire, avec les États membres.
Agent de sécurité informatique de l'Agence	L'agent de sécurité informatique de l'Agence a pour mission de superviser le contrôle des aspects de l'ECN liés à la sécurité et d'enquêter sur tous les incidents signalés.
Propriétaire des systèmes techniques	Le propriétaire des systèmes techniques est responsable de la mise en œuvre et de la réalisation des contrôles et des dispositifs de sécurité spéciaux dans l'ECN. Il définit les normes et procédures de sécurité auxquelles le fournisseur du système doit se conformer et est responsable de l'élaboration des procédures opérationnelles de sécurité.
Délégué à la protection des données	Le délégué à la protection des données s'assure que les données à caractère personnel de l'ECN sont traitées conformément aux règles et réglementations relatives à la protection des données à caractère personnel applicables à l'Agence.

4.3.4.2 Rôles de sécurité dans les États membres

Chaque État membre désignera une personne qui se verra confier les rôles suivants:

- La personne responsable de l'organisation du centre national de coordination et des mesures physiques de sécurité au sein du centre (p.ex. chef du centre national de coordination). La personne investie de ce rôle doit veiller à ce que
  - les mesures physiques de sécurité soient en place pour protéger le matériel connecté à l'ECN et pour s'assurer que seules les personnes autorisées du centre national de coordination puissent y accéder, y compris (le cas échéant) le personnel des bureaux décentralisés, ainsi qu'à tous les autres systèmes utilisés dans le centre qui sont connectés à l'ECN;
  - toutes les politiques et procédures définies dans les normes nationales, les règles nationales et le protocole d'accord — nécessaires pour protéger les informations sensibles non classifiées et les informations classifiées stockées et traitées dans l'ECN ou extraites et traitées en dehors de celui-ci — soient mises en œuvre dans le centre national de coordination et appliquées par le personnel de celui-ci (p.ex. marquage des

informations ou des documents, traitement des documents classifiés, supervision de l'application d'une procédure d'affectation du niveau adéquat de permission aux utilisateurs de l'ECN et révision périodique de celle-ci);

- des procédures soient mises en place, conformément aux règles nationales d'homologation (ou procédures équivalentes), pour les systèmes connectés à l'ECN; cela nécessitera des contacts avec toutes les autorités nationales compétentes de l'État membre.

- L'agent de sécurité informatique (ISO) du centre national de coordination

  L'ISO du centre national de coordination contrôle les aspects de sécurité des réseaux connectés à l'ECN et enquête sur tous les incidents signalés. Si nécessaire, il reçoit le soutien de l'unité informatique de l'Agence; dans ce cas, l'agent de sécurité informatique de l'Agence sert de point de contact.

En outre, chaque État membre doit charger l'une de ces personnes d'informer l'Agence des incidents de sécurité susceptibles d'affecter le nœud ECN de l'Agence ou les services de gestion technique de l'ECN, et d'informer les autres États membres concernés des incidents de sécurité pouvant avoir des répercussions sur leur nœud ECN.

4.3.4.3 Autres rôles — À l'Agence et dans les États membres

Le propriétaire de l'information: est responsable des ICUE et des autres informations traitées et produites par les systèmes techniques ou qui y sont ajoutées.

Utilisateurs: tous les utilisateurs sont tenus de respecter les politiques et procédures et de veiller à ce que leurs actions n'aient pas de conséquence négative sur la sécurité du système qu'ils utilisent.

4.3.5 Mécanismes de contrôle et procédures de signalement en cas de violation de la sécurité

Tout comportement d'un élément de l'ECN ou d'un système interconnecté laissant entendre qu'un incident de sécurité est survenu ou est en train de survenir dans l'ECN ou pourrait toucher l'ECN doit être immédiatement signalé à l'ISO du centre national de coordination et analysé par celui-ci. Si son analyse confirme un risque élevé, il doit immédiatement signaler l'incident à l'Agence, conformément aux règles et procédures établies dans les documents d'homologation.

4.4 Gestion des modifications[56]

4.4.1 Objectifs généraux et règles

L'Agence fournira une assistance en vue de développer davantage et de mettre en œuvre le cadre Eurosur dans les limites définies par les dispositions du règlement (UE) n° 1052/2013 et dans le respect de celles-ci. Les améliorations et adaptations apportées à ce cadre sont basées sur la politique de gestion des modifications définie par l'Agence, qui

- définit le cadre général du développement d'Eurosur;

- établit la méthodologie à suivre pour le déclenchement des procédures de modification et les consultations réalisées dans ce cadre;

[56] Voir les principes b), d) et e) de l'annexe du règlement (UE) n° 1052/2013.

- permet le traitement structuré des modifications;
- définit les types de modifications;
- détermine le processus décisionnel et les personnes et organisations qui en sont responsables;
- fournit des informations sur les outils techniques à utiliser pour soumettre des demandes et obtenir des retours d'information;
- garantit un cycle de développement de systèmes sûrs et sa cohérence avec l'homologation de l'ECN en matière de sécurité;
- garantit que l'approche de modification adoptée est axée sur les utilisateurs finals et leurs besoins.

Toute modification doit être conforme au règlement (UE) n° 1052/2013 et être traitée en accord avec les structures de gouvernance d'Eurosur. Le chef d'exploitation chargé d'Eurosur au sein de l'Agence est la personne investie du pouvoir de décision. Il est responsable de la totalité des processus opérationnels de l'Agence et responsable en dernier ressort de la fourniture des produits et services de l'Agence. Le chef d'exploitation est:

- conseillé par le groupe d'experts d'Eurosur (EEG);
- soutenu par les mécanismes de coordination interne de l'Agence[57];
- assisté par le conseil consultatif sur les modifications d'Eurosur.

Si des décisions stratégiques doivent être prises au sujet du développement d'Eurosur, l'avis du conseil d'administration de l'Agence peut être sollicité. Le chef d'exploitation peut déléguer une partie de son pouvoir décisionnel à d'autres entités de l'Agence, en particulier le conseil consultatif sur les modifications d'Eurosur, dont le président rend compte au chef d'exploitation et est supervisé par celui-ci.

4.4.2 Types de modifications

On entend par «modification» du cadre d'Eurosur, dans les limites et conditions établies par le règlement (UE) n° 1052/2013, tout ajout, modification ou suppression d'un composant du système, affectant sa performance. Les modifications peuvent être entreprises par un État membre ou un groupe d'États membres, par l'intermédiaire de leur centre national de coordination, ou par l'Agence.

- Les modifications majeures (qui ont une forte incidence sur les flux de travail internes, qui impliquent un grand nombre de parties prenantes, sont d'une grande complexité, qui nécessitent une interruption du flux de travail ou présentent une importance stratégique ou tactique) doivent être traitées au moyen de la structure de gestion des modifications et des mécanismes de coordination interne. Elles nécessitent l'approbation du chef d'exploitation.

[57] Les mécanismes de coordination interne de l'Agence désignent la coopération/consultation interne des unités de l'Agence et incluent les structures et procédures destinées à amorcer et à traiter les modifications à apporter à Eurosur ainsi qu'à les mettre en œuvre pour le compte de l'Agence.

- Les modifications mineures/normales (qui n'ont qu'un faible impact sur les processus en cours et la fourniture des produits/services, qui sont peu complexes ou sont de nature technique) ne nécessitent pas l'intervention de l'encadrement supérieur et devraient donc être gérées par le conseil consultatif sur les modifications. Une consultation supplémentaire, par l'intermédiaire des mécanismes de coordination interne, peut s'avérer nécessaire.

- Les modifications non standard (qui sortent du cadre des procédures standardisées) doivent être évaluées par le conseil consultatif sur les modifications et traitées en tant que modifications mineures ou majeures, en fonction de leur impact et de leur complexité. Une consultation supplémentaire, par l'intermédiaire des mécanismes de coordination interne, peut s'avérer nécessaire.

- Des solutions rapides (essentiellement d'ordre informatique) ou des modifications standards (suivant des procédures types standardisées ayant été communiquées à toutes les parties prenantes) ne nécessitent pas de réaction des structures de gouvernance et sont prises en charge par les unités compétentes de l'Agence.

Les demandes de modifications rapides, introduites en cas d'urgence, sont traitées dans le cadre d'une procédure distincte. Toute modification du cadre d'Eurosur, à l'exception des solutions rapides ou des modifications standards, nécessite le dépôt d'une demande de modification conforme aux exigences définies par l'Agence pour faciliter le processus.

4.4.3 Déclenchement d'une procédure de modification par les États membres

Les États membres peuvent lancer une procédure d'amélioration du cadre d'Eurosur par l'intermédiaire:

- du groupe d'experts d'Eurosur, ou

- du registre des modifications d'Eurosur et du système de retour d'information basé sur l'outil de retour d'information des services de gestion technique d'Eurosur.

Le *groupe d'experts d'Eurosur* fait office d'organe consultatif à l'égard du chef d'exploitation en transmettant des avis et des recommandations formulés par des utilisateurs finals. En cette qualité, il peut:

- envisager des modifications et donner son avis sur des modifications;

- formuler des propositions de modifications;

- évaluer les modifications proposées (y compris leur rapport coûts/bénéfices).

Le groupe d'experts d'Eurosur ou l'Agence peuvent décider de créer des sous-groupes spécifiques ou des task-forces chargés de préparer des demandes de modifications particulières.

Le *registre des modifications d'Eurosur et le système de retour d'information d'Eurosur* constituent ensemble un outil technique en ligne servant:

- à enregistrer toutes les demandes de modifications et à suivre leur traitement;

- à consulter/examiner la modification envisagée avant que la demande ne soit déposée;

- à signaler les problèmes et les dysfonctionnements du cadre d'Eurosur nécessitant le déclenchement de la procédure de modification;

- à soumettre des idées en vue d'améliorer le cadre d'Eurosur;

- à partager et obtenir des informations et à participer aux forums relatifs au fonctionnement du cadre d'Eurosur;

- à envoyer des retours d'information et à recevoir des contributions des autres utilisateurs finals.

L'Agence surveille le registre des modifications et le système de retour d'information d'Eurosur afin de traiter les demandes de modifications soumises au conseil consultatif sur les modifications, à l'aide des mécanismes de coordination interne de l'Agence, ou soumises au groupe d'experts d'Eurosur, pour obtenir des conseils avant de prendre une décision définitive.

4.4.4 Rôle du conseil consultatif sur les modifications d'Eurosur

Le conseil consultatif sur les modifications d'Eurosur est un forum consultatif et décisionnel géré par l'Agence et investi des missions suivantes:

- surveiller et exploiter le registre des modifications et le système de retour d'information d'Eurosur;

- collecter et enregistrer toutes les demandes de modifications opérationnelles ou techniques soumises par les parties prenantes internes et externes, en assurant le suivi du processus de demande;

- évaluer, valider chaque demande de modification et en définir le degré de priorité;

- adapter au besoin le statut de la demande de modification (p.ex. en la faisant passer de «mineure» à «standard»);

- prendre des décisions au sujet de l'application des modifications et proposer un calendrier;

- transmettre les demandes nécessitant des conseils ou des permissions supplémentaires aux structures de gestion compétentes, y compris aux mécanismes de coordination interne établis à cette fin;

- soumettre les demandes de modifications majeures au chef d'exploitation pour que celui-ci prenne une décision finale et demander un avis sur d'autres demandes de modifications au besoin;

- transmettre les problèmes au groupe d'experts d'Eurosur si leurs conseils sont nécessaires;

- effectuer des consultations supplémentaires au sein de l'Agence si l'impact ou la complexité de la modification proposée l'exige;

- communiquer les décisions et préparer une explication en cas de refus d'une demande de modification.

4.4.5 Règles appliquées aux demandes de modifications

Les demandes de modifications peuvent être acceptées ou refusées pour des raisons techniques, financières, légales ou opérationnelles. Elles peuvent également être renvoyées au demandeur pour que celui-ci les motive davantage ou fournisse de plus amples informations, notamment sur les cas d'utilisation, les coûts et l'analyse d'impact, avant qu'une décision définitive ne soit prise. Si la demande de modification est refusée, l'Agence adresse au demandeur une motivation du refus.

Le centre national de coordination représente le point de contact unique de l'Agence pour le traitement des demandes de modifications. Si la modification proposée a été formulée par le groupe d'experts d'Eurosur, son suivi est assuré par l'intermédiaire du registre des modifications et du système de retour d'information d'Eurosur. Les conclusions du centre national de coordination peuvent également déclencher une demande de modification au nom des États membres.

4.5 Gestion de la continuité des opérations[58]

La norme ISO 22301:2012 définit la continuité des opérations comme étant la capacité de l'organisation à poursuivre la fourniture de produits ou la prestation de services à des niveaux acceptables et préalablement définis après un incident perturbateur. Cette norme définit la gestion de la continuité des activités comme un «processus de management holistique

- qui identifie les menaces potentielles pour une organisation ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et

- qui fournit un cadre pour construire la résilience de l'organisation avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeur».

L'ECN étant un système décentralisé possédant un nœud dans chaque État membre et à l'Agence, la continuité des opérations doit être assurée tant au niveau national qu'au niveau européen.

Les risques et les problèmes compromettant le bon fonctionnement des différents éléments du cadre d'Eurosur doivent être détectés et évalués; par ailleurs, les centres nationaux de coordination et l'Agence doivent être prêts à prendre les mesures appropriées si ces risques se matérialisent. Les centres nationaux de coordination et l'Agence doivent empêcher, ou, à tout le moins, réduire l'impact potentiel d'une menace ou d'un risque compromettant le flux d'informations de l'ECN et perturbant l'élaboration, la maintenance et la diffusion du NSP, de l'ESP et du CPIP.

- L'Agence est chargée d'examiner les risques et les menaces auxquels l'ECN tout entier pourrait être exposé et d'assurer sa stabilité et son bon fonctionnement.

- Les centres nationaux de coordination sont chargés de garantir une utilisation efficace de leur nœud Eurosur, en enregistrant leurs données dans l'ECN, en fournissant les infrastructures nécessaires au bon fonctionnement de leur nœud ECN et en veillant à ce que les mesures de sécurité nécessaires soient prises pour protéger le nœud ECN. Les centres nationaux de coordination doivent garantir la connectivité avec leurs réseaux et

[58] Voir l'annexe du règlement (UE) n° 1052/2013.

leurs systèmes nationaux, afin de permettre l'utilisation et le transfert de données dans tout l'ECN.

Ces obligations doivent être remplies en élaborant des plans de continuité des opérations au sein de l'Agence et dans chaque centre national de coordination, comme indiqué dans le protocole d'accord et sur la base des cinq étapes clés suivantes:

4.5.1 Analyse d'impact

L'objectif de cette étape est de déterminer quels sont les processus et fonctions clés du système et quelles seraient les conséquences d'une indisponibilité de l'un d'entre eux.

L'analyse couvre les fonctions et les services fournis par l'Agence, l'ECN et les centres nationaux de coordination, répartis dans les catégories suivantes:

- *Fonctions critiques* - ne peuvent être interrompues plus d'une heure. Toute indisponibilité de ces fonctions doit être traitée immédiatement, étant donné qu'elle a une forte incidence sur le fonctionnement du cadre d'Eurosur tout entier.
- *Fonctions essentielles* - une interruption d'une journée maximum est tolérable. Toutefois, ces fonctions doivent être rétablies le plus vite possible. Idéalement, leur indisponibilité ne devrait pas dépasser quelques heures.
- *Fonctions nécessaires* - fonctions importantes pour le bon fonctionnement du cadre d'Eurosur et essentielles aux performances du centre national de coordination à long terme. Ces fonctions peuvent être interrompues pendant une semaine maximum sans perturber les éléments livrables clés, mais elles doivent néanmoins être rétablies dans les plus brefs délais.

Une analyse des risques opérationnels pour l'ECN a été réalisée dans le cadre de la procédure d'homologation.

4.5.2 Gestion des risques

Cette étape a pour but de détecter, d'analyser, de contrôler et de surveiller les risques. L'évaluation des risques doit permettre de déterminer dans quelle mesure ils sont susceptibles de se concrétiser et les conséquences qu'ils pourraient alors avoir. Parmi les risques courants figurent:

- la perte de ressources clés (siège, équipements ou infrastructures);
- la perte de membres clés du personnel (y compris leur indisponibilité);
- la perte de services externes subsidiaires (p.ex. fournisseurs contractuels externes, coupure d'électricité, d'eau ou d'autres services.

4.5.3 Élaboration d'une stratégie et d'un plan de continuité des opérations

La finalité d'une stratégie de continuité des opérations est de définir les critères d'acceptation des risques et les mesures de réduction des risques inacceptables. Toutes les fonctions critiques, essentielles et nécessaires doivent avoir un délai de rétablissement défini. Le plan de continuité des opérations décrit les procédures qui orientent les organisations afin de répondre aux problèmes, de rétablir les fonctions, de reprendre les opérations et de rétablir et reprendre le fonctionnement au niveau opérationnel prédéfini, à la suite d'une perturbation. Ces plans comportent généralement des détails sur:

- la finalité, la portée et les utilisateurs du plan;
- les documents de référence;
- les hypothèses;
- les rôles et responsabilités;

– les contacts clés;
– l'activation et la désactivation du plan;
– la communication;
– les interventions prévues en cas d'incident;
– l'ordre de rétablissement des activités;
– les plans de reprise des activités;
– le plan de reprise après une catastrophe;
– les ressources requises;
– les activités de rétablissement et de reprise.

Ces plans doivent être intégrés au plan global de continuité des opérations pour les États membres et l'Agence.

4.5.4 Communication en cas de perturbation

En cas de perturbation de la continuité des opérations de l'ECN, le centre national de coordination et l'Agence s'informent mutuellement de l'incident et de son impact potentiel en utilisant les canaux de communication décrits dans le protocole d'accord. Cette notification doit inclure une description de la perturbation et de son impact sur l'ECN et indiquer si le centre ou l'Agence a activé son plan de continuité des opérations. Si la perturbation risque d'avoir un impact plus vaste, il convient également d'informer tous les membres de l'incident et de son impact potentiel.

Si un État membre ou l'Agence effectue des tests susceptibles d'avoir un impact sur le fonctionnement global de l'ECN, ils doivent s'informer mutuellement à l'avance de ces tests ainsi que de leurs conséquences et de leur durée estimées.

4.5.5 Maintenance de la gestion de la continuité des activités

Ces plans et processus doivent être régulièrement mis à jour, ajustés et améliorés afin de faire en sorte qu'ils soient adaptés à la situation actuelle. Cela implique notamment la réalisation de tests et d'exercices réguliers, l'adoption de mesures correctives et la modification et la révision de ces plans et processus.

4.6 Communication

4.6.1 Objectifs généraux

Pour atteindre les objectifs d'Eurosur, une communication efficace doit être mise en place dans les domaines suivants:

- échanges d'informations sur le contenu d'Eurosur (NSP, ESP et CPIP);
- communication entre les centres nationaux de coordination et avec l'Agence, dans le cadre des activités quotidiennes (contacts entre opérateurs, etc.);
- résolution des éventuels problèmes techniques ou opérationnels (bogues, incidents informatiques, demandes d'accès, etc.), y compris dans les cas où la continuité des opérations est en jeu (voir le point 4.5).

Une communication efficace permet d'améliorer la qualité des informations fournies via Eurosur et ainsi d'améliorer la capacité de réaction.

4.6.2 Communication quotidienne

La communication quotidienne a lieu:

- au niveau européen — entre les centres nationaux de coordination et avec l'Agence;

- au niveau national — des canaux de communication efficaces doivent être mis en place entre toutes les autorités responsables de la surveillance des frontières, y compris au sein des autorités appartenant à la chaîne de commandement, afin d'assurer un processus décisionnel efficace et de fournir des capacités de réaction;

- à l'intérieur de l'Agence — entre les différentes unités participant à la création de l'ESP/CPIP.

La communication quotidienne peut avoir lieu:

- par l'intermédiaire de l'ECN et des applications dédiées, y compris l'application Eurosur et les dispositifs de vidéoconférence;

- par téléphone et courrier électronique, en utilisant les listes de contact (voir les points 3.1.15 et 4.6.4);

- par l'intermédiaire d'autres plateformes (p.ex. le répertoire de documents sous forme de guichet unique de Frontex, etc.)

Chaque État membre est disponible 24 heures sur 24, 7 jours sur 7, via son centre national de coordination.

4.6.3 Point de contact central de l'Agence

L'Agence possède un point de contact central situé dans l'unité responsable des échanges d'informations et du maintien de la connaissance de la situation. Cette unité constitue le point de référence central qui assure une coordination rapide et fiable, au niveau de l'Agence, de l'ensemble des informations opérationnelles entrantes et sortantes.

Cette unité fournit une approche holistique aux centres nationaux de coordination et aux unités internes de l'Agence en contrôlant et en traitant les informations opérationnelles entrantes et sortantes afin d'assurer la maintenance de l'ESP/CPIP et d'améliorer les capacités de réaction des États membres, p.ex. en coordonnant la fourniture de services relatifs à l'application commune des outils de surveillance et en facilitant si nécessaire la communication sur les réactions opérationnelles rapides.

En tant que passerelle opérationnelle de l'Agence, grâce à sa communication opérationnelle et à sa gestion des informations, ce point de contact offre des capacités pour:

- le suivi de la situation;

- la connaissance de la situation et le soutien;

- la fourniture des services de fusion d'Eurosur;

- la coordination et la facilitation des activités opérationnelles conjointes, en servant de lien opérationnel entre l'équipe de projet responsable au niveau de l'Agence et les acteurs sur le terrain;

- la gestion des urgences et des situations de crise;

- la liaison avec les centres nationaux de coordination;

- la liaison avec les unités internes de l'Agence.

4.6.4 Liste de contacts

L'Agence est chargée de tenir à jour la liste de contacts des centres nationaux de coordination, qui indique:

- la place du centre national de coordination dans les structures des États membres (nom de l'autorité, etc.);
- le nom et le titre/grade du chef du centre national de coordination;
- l'adresse et les heures d'ouverture du centre (heures de bureau/heures de permanence);
- l'adresse de courrier électronique du centre — en service 24 heures sur 24, 7 jours sur 7;
- le(s) numéro(s) de téléphone du centre — en service 24 heures sur 24, 7 jours sur 7;
- la liste des autorités représentées au sein du centre et les heures de permanence de chacune d'entre elles.

Les centres nationaux de coordination doivent informer l'Agence sans tarder de tout changement de ces coordonnées.

La liste de contacts inclut les contacts de l'Agence pour:

- les affaires d'échanges opérationnels/d'informations;
- les demandes de services ayant trait à l'utilisation commune des outils de surveillance;
- la gestion des accès;
- le bureau d'assistance technique.

4.6.5 Communication relative aux activités opérationnelles quotidiennes

Le centre national de coordination qui reçoit le premier des informations relevant du domaine d'activité d'Eurosur est tenu de les enregistrer dans l'application Eurosur et de les partager dans les plus brefs délais avec les partenaires concernés.

Les informations du terrain doivent parvenir en temps quasi-réel (notification immédiate) au centre. La notification au niveau national doit être effectuée en utilisant les modèles prédéfinis, afin d'assurer une approche unifiée de la notification. Des plans doivent être préparés à l'avance de manière à assurer la notification immédiate des cas d'urgence. Dans les situations d'urgence, les centres nationaux de coordination peuvent informer les autres centres nationaux de coordination ou l'Agence de la situation en cours via d'autres moyens de contact tels que le téléphone, la vidéoconférence, etc., en utilisant les coordonnées fournies dans la liste de contacts.

Meilleure pratique: discussion des questions opérationnelles lors de vidéoconférences mensuelles entre les chefs des centres nationaux de coordination et l'Agence.

4.6.6 Réunions officielles

Les chefs des centres nationaux de coordination, les représentants des autorités nationales compétentes et l'Agence se réunissent régulièrement au sein d'un *groupe d'experts d'Eurosur* dont les travaux sont axés sur les besoins des utilisateurs.

Le groupe d'experts d'Eurosur, auquel participent des parties prenantes internes et externes, permet l'échange des expériences acquises sur le terrain et améliore la coordination entre les acteurs internes et externes. Ce groupe a également pour but de permettre les échanges sur les questions d'ordre pratique ayant trait au cadre d'Eurosur. Le groupe prépare et prodigue des conseils sur les questions techniques et opérationnelles relatives au cadre d'Eurosur.

Des sous-groupes axés sur les aspects techniques et opérationnels peuvent être créés afin de soutenir le groupe d'experts d'Eurosur sur une base ponctuelle ou temporaire.

Exemples: groupe d'utilisateurs de la couche «analyse», groupe d'experts sur l'homologation de l'ECN, etc.

4.6.7 Eurosur et relations publiques

Les informations incluses dans Eurosur doivent être soumises aux mesures de transparence les plus strictes possibles. Toutefois, afin de ne pas compromettre la réussite des activités opérationnelles/enquêtes en cours, il convient de faire preuve de discrétion quant aux informations qui sont communiquées au public. La divulgation des informations au public doit faire l'objet d'un examen au cas par cas par les autorités compétentes.

Seules les autorités chargeant des informations dans Eurosur sont autorisées à discuter des détails d'incidents spécifiques avec la presse.

Si l'Agence est associée à des activités opérationnelles, elle se réserve le droit de faire usage des informations relatives au résultat de ces activités.

Les interviews relatives à Eurosur doivent être accordées par le personnel travaillent dans le domaine concerné et qui y est familiarisé.

4.6.8 Langue de communication

La langue de travail et de communication d'Eurosur est l'anglais. Les États membres doivent veiller à ce que toutes les communications transmises au niveau national soient claires et correctement traduites.

5 Principes de coopération interservices et de coopération externe

5.1 Coopération de l'Agence avec les autres institutions, organes et organismes de l'Union européenne et les organisations internationales[59]

Le présent chapitre propose des orientations pour des échanges d'informations et une coopération efficaces entre l'Agence et les autres institutions, organes et organismes de l'Union et organisations internationales. Les détails pratiques de ces activités sont décrits dans des documents spécifiques (p.ex. modalités de travail).

[59] Article 18 du règlement (UE) n° 1052/2013.

5.1.1 Organisations partenaires

L'Agence coordonne et échange des informations via des canaux de communication sécurisés, dans la limite de ses possibilités et selon les besoins, avec les institutions, organes et organismes de l'Union et les organisations internationales, afin d'exploiter au mieux les informations, les capacités et les systèmes disponibles. Les parties prenantes concernées sont réparties selon les catégories suivantes:

- institutions, organes et organismes de l'UE («organisations partenaires de l'UE»), et
- organisations et organismes internationaux («organisations partenaires hors UE»).

Lorsqu'elle travaille avec ces organisations partenaires, l'Agence doit veiller à ce que son mandat, son cadre juridique et son autonomie soient pleinement respectés.

5.1.2 Champ d'application

L'Agence échange des informations avec les organisations partenaires de l'UE ou hors UE aux fins suivantes:

1) fourniture de données pertinentes sur l'immigration illégale et la criminalité transfrontalière à inclure dans l'ESP/CPIP. Europol est le principal partenaire de l'Agence dans ce domaine. L'Agence peut également travailler avec d'autres organisations partenaires, telles qu'Interpol, le MAOC-N, les services de la Commission, l'agence eu-LISA, Eurojust le SEAE et d'autres. Les informations collectées dans l'ESP/CPIP sont partagées avec les organisations partenaires selon le principe du besoin d'en connaître et dans la mesure nécessaire à l'exécution de leur propre mission. Les données destinées à étayer et à mettre à jour l'ESP/CPIP fournies par les services de la Commission, le SEAE, la FRA, l'EASO (p.ex. sur la gestion des flux migratoires ou les informations sur les pays d'origine) et les organisations partenaires hors UE seront traitées et associées aux informations émanant d'autres sources, validées puis mises à disposition des centres nationaux de coordination des États membres par l'Agence via l'ESP/CPIP. Si l'Agence reçoit des informations pertinentes provenant de deux organisations partenaires ou plus, elle fusionne ces informations et les valide avant de les publier dans l'ESP/CPIP.
2) Les contributions à l'*application commune des outils de surveillance* sont fournies par l'EMSA, l'EFCA, le Centre satellitaire et les autres organisations partenaires compétentes, comme indiqué au point 3.2.8. Pour l'acquisition d'images satellites et l'utilisation de données obtenues par satellite dans ses activités quotidiennes, l'Agence exploite au mieux le programme Copernicus[60].

5.1.3 Cadre juridique

La coopération de l'Agence avec des tiers visée à l'article 18 du règlement (UE) n° 1052/2013 est définie dans les modalités de travail et autres documents réglementaires pertinents (p.ex. accords de niveau de service ou protocoles d'accord) conclus entre l'Agence et les organisations partenaires de l'UE/hors UE, conformément à l'article 13 du règlement (CE) n° 2007/2004. Ces documents peuvent inclure des instruments de coopération existants ou, le cas échéant, nouvellement élaborés. Les règles de procédure utilisées pour les échanges d'informations seront définies dans les modalités de travail.

[60] Copernicus, précédemment appelé «programme de surveillance mondiale de l'environnement et de la sécurité» (GMES), est le programme européen visant à mettre en place une capacité européenne d'observation de la Terre.

5.1.4 Canaux de communication

L'Agence constitue le point de contact unique pour les échanges d'informations et la coopération avec les organisations partenaires. L'accès à l'ESP/CPIP étant limité à l'Agence et aux centres nationaux de coordination, l'Agence crée des canaux de communication dédiés pour échanger avec les organisations partenaires.

Chaque organisation partenaire désigne l'infrastructure de communication requise ainsi qu'un point de contact. Les coordonnées (adresse de courrier électronique officielle et fonctionnelle, numéro de téléphone portable et adresse officielle) de ce point de contact doivent être communiquées à l'Agence.

Si la structure de l'organisation partenaire nécessite la désignation de plusieurs points de contact, les coordonnées de ceux-ci et la répartition de leurs responsabilités doivent être communiquées à l'Agence.

L'Agence crée et tient à jour une liste de contacts pour les organisations partenaires avec lesquelles elle coopère dans le cadre d'Eurosur.

5.1.5 Évaluation

L'Agence et les organisations partenaires analysent, conçoivent et évaluent les produits élaborés en collaborant dans le cadre d'Eurosur, dans le but de recenser les besoins et les manques et de proposer des mesures en vue d'y remédier. Ces conclusions peuvent conduire l'Agence à déclencher des procédures de modifications conformément aux règles établies au point 4.4. L'évaluation est réalisée en fonction du cadre de coopération bilatérale et à chaque fois que la situation opérationnelle le nécessite. La coopération entre l'Agence et les organisations partenaires peut être adaptée conformément à cette évaluation et aux besoins opérationnels.

5.2 Coopération des États membres avec les pays tiers voisins[61]

Un échange d'informations permanent et bien structuré avec les pays tiers voisins et une coopération entre ceux-ci et les États membres sont des éléments essentiels pour lutter contre l'immigration illégale et la criminalité transfrontalière et pour sauver la vie de migrants. Pour être durable, cette coopération doit être réciproque, basée sur une confiance mutuelle et être bénéfique à la fois pour le ou les États membres et les pays tiers. Cette coopération doit absolument se dérouler dans le plein respect de la législation relative aux droits fondamentaux.

Les États membres peuvent collaborer avec les pays tiers voisins au niveau international, multilatéral et bilatéral.

5.2.1 Coopération internationale

La coopération internationale peut comprendre, en fonction du niveau concerné:

1) des échanges d'informations avec l'Agence et une assistance de celle-ci, en étroite coordination avec le Service européen pour l'action extérieure, Europol, Eurojust, Interpol et les autres organismes concernés;

[61] Article 20 du règlement (UE) n° 1052/2013.

2) la participation d'experts de pays tiers aux programmes, projets, conférences, séminaires et groupes de travail créés par l'Agence, la Commission européenne, Interpol, les Nations unies et les organisations internationales;

3) le déploiement d'agents de liaison dans les délégations de l'UE[62] et les ambassades et consulats des États membres;

4) des activités conjointes d'analyse des risques et d'enquête avec les autorités des pays tiers;

5) des formations dispensées aux autorités des pays tiers sur les activités de contrôle aux frontières, les opérations de recherche et de sauvetage, les droits fondamentaux, etc.;

6) le renforcement des capacités des pays tiers grâce à des programmes cofinancés par des fonds de l'UE et internationaux.

5.2.2 Coopération multilatérale et bilatérale

La coopération multilatérale et bilatérale peut englober, en fonction du niveau concerné:

1) des réseaux d'agents de liaison;

2) des réseaux régionaux, servant à échanger des informations via des canaux de communication sécurisés, à échanger des agents de liaison, à organiser des formations, à renforcer les capacités de surveillance et à mettre en place des centres de coordination dans les pays tiers. Si plusieurs États membres participent à un réseau régional, ils doivent indiquer à l'Agence quel est le centre national de coordination responsable des échanges d'informations entre le réseau régional et Eurosur;

3) des activités opérationnelles conjointes (terrestres, maritimes et aériennes), y compris des patrouilles conjointes;

4) des formations dispensées aux autorités des pays tiers sur les activités de contrôle aux frontières, les opérations de recherche et de sauvetage, les droits fondamentaux, etc.;

5) le renforcement des capacités grâce à la fourniture de ressources et d'une assistance technique en vue d'améliorer les capacités de contrôle aux frontières dont disposent les pays tiers.

Parmi les réseaux régionaux figurent par exemple le réseau de coopération régionale en mer Baltique pour le contrôle aux frontières (BSRBCC) et le réseau atlantique SEAHORSE.

5.2.3 Accords

La coopération décrite ci-dessus est mise en œuvre sur la base d'accords et de modalités de travail, ou par l'intermédiaire de réseaux régionaux mis en place sur la base de ces accords. Avant de conclure un accord ou accord de collaboration de ce type, l'État membre concerné doit notifier la Commission européenne du texte ou des dispositions pertinentes. La

[62] Conformément au document intitulé «Note conceptuelle sur le déploiement d'officiers de liaison "Migration" européens» (document 13435 du Conseil du 4.11.2015 JAI 790 ASIM 130 RLEX 853).

Commission vérifiera que ces dispositions respectent celles de l'article 20 du règlement (UE) n° 1052/2013. Les États membres doivent également notifier la Commission des textes des accords conclus et la Commission en transmettra un aperçu général et une évaluation au Parlement européen, au Conseil européen et à l'Agence.

Les États membres informent l'Agence de la coopération en cours avec des pays tiers au niveau opérationnel, comme l'exige l'article 2, paragraphe 2, du règlement (CE) n° 2007/2004. Lorsqu'ils concluent des accords bilatéraux avec des pays tiers, les États membres peuvent inclure des dispositions relatives au rôle et aux responsabilités de l'Agence, après avoir au préalable consulté celle-ci.

Si les informations qui doivent être échangées avec les autorités d'un pays tiers appartiennent à un État membre (ou à l'Agence) ne faisant pas partie de l'accord de collaboration ou du réseau régional, le centre national de coordination de l'État membre souhaitant partager les informations doit faire parvenir une demande écrire au propriétaire des informations (l'État membre ou l'Agence), en indiquant le pays tiers avec lequel les informations seront partagées et en exposant les motifs du partage. Le propriétaire des informations (un État membre ou l'Agence) transmet sa réponse par écrit dans les plus brefs délais. Tout refus de partager les informations doit être motivé. L'approbation tacite n'est pas autorisée: le propriétaire des informations doit répondre par la positive ou la négative.

6 Suivi et évaluation[63]

Les mesures suivantes doivent être adoptées pour assurer le suivi du *fonctionnement technique* d'Eurosur:

- Dans son rapport dont la publication est prévue le 1er décembre 2015, puis tous les deux ans, l'Agence donne un aperçu de la mise en œuvre de l'ECN, de l'ESP (y compris concernant les tronçons de frontière et l'attribution des niveaux d'impact) et du CPIP, ainsi que de l'application commune des outils de surveillance, en décrivant les progrès accomplis et en indiquant les mesures qui restent à prendre pour respecter pleinement les dispositions du règlement (UE) n° 1052/2013.

- Au plus tard pour le 31 janvier 2016, puis chaque année à la même date, chaque État membre fournira un rapport annuel sur la création et le fonctionnement de son centre national de coordination et de son NSP, en décrivant les progrès accomplis l'année précédente et en indiquant les mesures qui restent à prendre pour respecter pleinement les dispositions du règlement (UE) n° 1052/2013. La Commission inclura un résumé dans son évaluation globale d'Eurosur, dont la publication est prévue pour le 1er décembre 2016, puis tous les quatre ans.

Les mesures suivantes doivent être adoptées pour assurer le suivi du *fonctionnement opérationnel* d'Eurosur:

- À partir de 2015, dans le rapport annuel mentionné ci-dessus, chaque État membre fournit une description des mesures prises au niveau national (en insistant sur le rôle de son centre national de coordination) en ce qui concerne les tronçons de frontière extérieure auxquels un niveau d'impact moyen ou élevé a été attribué.

- Dans son rapport dont la publication est prévue pour le 1er décembre 2015, puis tous les deux ans, l'Agence donne un aperçu des mesures prises par les États membres et l'Agence

[63] Article 22 du règlement (UE) n° 1052/2013.

en rapport avec les tronçons de frontière extérieure auxquels un niveau d'impact moyen ou élevé a été attribué. Pour ce rapport, l'Agence collaborera avec le ou les États membres concernés pour analyser et évaluer les mesures prises au niveau national et européen.

- Dans son évaluation globale dont la publication est prévue pour le 1er décembre 2016, puis tous les quatre ans, la Commission analysera la manière dont le règlement Eurosur a été appliqué dans les États membres et par l'Agence.

Les mesures suivantes devront être prises pour contrôler la manière dont les droits fondamentaux, y compris le principe de non-refoulement, ont été respectés dans le cadre d'Eurosur.

- Conformément à l'article 3, paragraphe 1, du règlement (CE) n° 2007/2004, et en annexe du rapport de l'Agence dont la publication est prévue pour le 1er décembre 2015, puis tous les deux ans, l'officier aux droits fondamentaux de l'Agence pourra présenter ses observations sur le respect, par l'Agence, de la législation relative aux droits fondamentaux. Le forum consultatif pourra transmettre des recommandations à l'Agence au sujet de son respect des droits fondamentaux lors de l'application du règlement Eurosur. Pour ce faire, l'officier aux droits fondamentaux et le forum consultatif auront accès, dans le cadre de leurs mandats respectifs, à l'ensemble des informations relatives au respect des droits fondamentaux pour toutes les activités entreprises par l'Agence dans le cadre d'Eurosur.

- Dans son évaluation globale dont la publication est prévue pour le 1er décembre 2016, puis tous les quatre ans, la Commission proposera une évaluation du respect, par l'Agence et les États membres, de la législation relative aux droits fondamentaux (y compris la protection des données à caractère personnel et le principe de non-refoulement) lors de l'application du règlement Eurosur[64].

- Dans son évaluation globale dont la publication est prévue pour le 1er décembre 2016, puis tous les quatre ans, la Commission donnera un aperçu des accords conclus entre les États membres et les pays tiers aux fins du règlement Eurosur, et analysera le respect, dans ces accords, des dispositions de l'article 20 du règlement (UE) n° 1052/2013.

7 Révision du manuel et observations finales

La Commission peut modifier le présent manuel en fonction des contributions qu'elle reçoit de l'Agence et des États membres.

L'Agence et les États membres peuvent, après consultation de la Commission européenne, approuver et classifier des documents internes (catalogues, cahiers des charges, etc.) pour préciser davantage les critères opérationnels, techniques ou autres nécessaires à la mise en œuvre et à l'utilisation quotidienne d'Eurosur. La Commission vérifie que ces documents respectent les dispositions du règlement (UE) n° 1052/2013 et du présent manuel.

[64] La Commission pourra faire appel à l'Agence des droits fondamentaux lors de la préparation de cette évaluation.

8 Liste des instruments

- Règlement (UE) n° 1052/2013 du Parlement européen et du Conseil du 22 octobre 2013 portant création du système européen de surveillance des frontières (Eurosur)

- Règlement (CE) n° 2007/2004 du Conseil du 26 octobre 2004 portant création d'une Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne

- Règlement (UE) n° 656/2014 du Parlement européen et du Conseil du 15 mai 2014 établissant des règles pour la surveillance des frontières maritimes extérieures dans le cadre de la coopération opérationnelle coordonnée par l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne

- Règlement (CE) n° 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen)

- Décision (UE, Euratom) n° 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne

- Charte des droits fondamentaux de l'Union européenne

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales

- Convention concernant le statut des réfugiés (1951) et son protocole (1967)

- Convention internationale de 1979 sur la recherche et le sauvetage en mer et autres conventions internationales relevant de l'Organisation maritime internationale

9 Liste des abréviations

Agence	Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne (Frontex)
SIA	Système d'identification automatique
BSRBCC	Réseau de coopération régionale en mer Baltique pour le contrôle aux frontières
CIRAM	Modèle d'analyse commune et intégrée des risques
CPIP	Tableau commun du renseignement en amont des frontières
EASO	Bureau européen d'appui en matière d'asile
EBGT	Équipes européennes de gardes-frontières
ECN	Réseau de communication Eurosur
CEPD	Contrôleur européen de la protection des données
SEAE	Service européen pour l'action extérieure
EEG	Groupe d'experts d'Eurosur
EFCA	Agence européenne de contrôle des pêches
AESM	Agence européenne pour la sécurité maritime
EO	Observation de la terre
EPN	Réseau européen de patrouilles
ESP	Tableau de situation européen
ETMS	Services de gestion technique d'Eurosur
UE	Union européenne
ICUE	Informations classifiées de l'Union européenne
EUROPOL	Office européen de police
Eurosur	Système européen de surveillance des frontières
FRA	Agence des droits fondamentaux
ICC	Centre de coordination internationale
INTERPOL	Organisation internationale de police criminelle
ISO	Organisation internationale de normalisation
TIC	Technologies de l'information et de la communication
JORA	Application de transmission d'informations sur les opérations conjointes
LCC	Centre local de coordination
LRIT	Système d'identification et de localisation à grande distance
MAOC-N	Maritime Analysis and Operations Centre – Narcotics (Centre d'opération et d'analyse maritime de lutte contre le trafic de drogue)
MRCC	Centre de coordination des opérations de sauvetage en mer
NCC	Centre national de coordination
NFPOC	Point de contact national Frontex
NSP	Tableau de situation national
RCC	Centre régional de coordination
SATCEN	Centre satellitaire de l'Union européenne
SAR	Recherche et sauvetage
SIRENE	Supplément d'information requis à l'entrée nationale
TETRA	Radiocommunications européennes à ressources partagées
NU	Nations unies
VHF	Très haute fréquence
VMS	Système de surveillance des navires
VPN	Réseau privé virtuel