NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO SANS CLASSIFICATION

20 novembre 2020

DOCUMENT
C-M(2002)49-REV1

LA SÉCURITÉ DANS L'ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD (OTAN)

Note du secrétaire général

Révision 1 du C-M(2002)49, du 17 juin 2002

Référence : C-M(2002)49-COR1 à COR12 (version consolidée), du 17 juin 2002

1. Le présent document, qui a été approuvé par le Comité de sécurité, est le résultat d'une revue complète et approfondie de la politique de sécurité de l'OTAN (C-M(2002)49) et de ses directives complémentaires.

2. Les modifications apportées dans ce C-M(2002)49-REV1, qui remplace le document cité en référence, ont porté à la fois sur la structure et sur le contenu.

3. Pour ce qui est de la structure, on notera l'ajout d'une pièce jointe « H » spécifiquement consacrée à la question de la sécurité concernant les entités non OTAN. Cette question est traitée plus en détail dans la nouvelle directive pour l'OTAN sur la sécurité liée aux entités non OTAN (AC/35-D/2006) et dans la version révisée du document complémentaire pour les entités non OTAN sur la sécurité liée à l'OTAN (AC/35-D/1038-REV3).

4. En ce qui concerne le contenu, les révisions ont porté sur les principes de base, les normes minimales et les responsabilités (pièce jointe « B »), ainsi que sur les dispositions relatives à la sécurité concernant le personnel, à la sécurité physique, à la sécurité des informations et à la sécurité concernant les entités non OTAN (pièces jointes « B », « C », « D », « E » et « H »). Les pièces jointes « F » et « G » au C-M(2002)49 n'ont pas été examinées dans le cadre de cette revue.

(signé) Jens Stoltenberg

1 annexe
Pièces jointes A, B, C, D, E, F, G, H
1 glossaire

Original : anglais

ANNEXE 1
C-M(2002)49-REV1

LA SÉCURITÉ DANS L'ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD (OTAN)

INTRODUCTION

1. Le présent C-M, intitulé « La sécurité dans l'Organisation du Traité de l'Atlantique Nord (OTAN) », énonce les principes de base et normes minimales de sécurité qui doivent être appliqués par les pays et les organismes civils et militaires de l'OTAN afin d'assurer aux informations classifiées un degré de protection commun. Les procédures de sécurité de l'OTAN ne sont pleinement efficaces que si elles peuvent s'appuyer sur un système de sécurité national ayant des caractéristiques équivalentes/conformes à celles décrites dans la présente politique. En outre, celle-ci traite également des rôles, fonctions et responsabilités en matière de sécurité à l'OTAN.

2. La présente politique comprend, en pièce jointe « A », l'accord de sécurité, intitulé « Accord sur la sécurité des informations entre les Parties au Traité de l'Atlantique Nord », ainsi que les pièces jointes suivantes :

(a) Pièce jointe « A » – Accord sur la sécurité des informations entre les Parties au Traité de l'Atlantique Nord

(b) Pièce jointe « B » – Principes de base, normes minimales et responsabilités

(c) Pièce jointe « C » – Sécurité concernant le personnel

(d) Pièce jointe « D » – Sécurité physique

(e) Pièce jointe « E » – Sécurité des informations OTAN classifiées

(f) Pièce jointe « F » – Sécurité des systèmes d'information et de communication

(g) Pièce jointe « G » – Sécurité industrielle et sécurité des projets classifiés

(h) Pièce jointe « H » – Sécurité concernant les entités non OTAN

3. Le présent document vient à l'appui de la politique de gestion de l'information OTAN (C-M(2007)0118). La politique relative à la gestion des informations OTAN non classifiées (C-M(2002)60) fixe en outre les principes de base et les normes à appliquer dans les organismes civils et militaires et les pays de l'OTAN pour la protection des informations OTAN non classifiées (informations NATO SANS CLASSIFICATION et informations communicables au public).

BUTS ET OBJECTIFS

4. Les pays et les organismes civils et militaires de l'OTAN veillent à ce que les principes de base et les normes minimales de sécurité énoncés dans le présent C-M soient appliqués afin de protéger les informations OTAN classifiées contre toute perte de confidentialité, d'intégrité et de disponibilité.

5. Les pays et les organismes civils et militaires de l'OTAN établissent des programmes de sécurité conformes à ces principes de base et à ces normes minimales afin d'assurer un degré commun de protection des informations OTAN classifiées.

APPLICABILITÉ

6. Ces principes de base et ces normes minimales s'appliquent :

(a) aux informations classifiées produites par l'OTAN ;

(b) aux informations classifiées produites par un pays de l'OTAN et communiquées à l'OTAN ou à un autre pays de l'OTAN à l'appui d'un programme, projet ou contrat OTAN ;

(c) aux informations classifiées échangées entre l'OTAN et des entités non OTAN (NNE)[1] ;

(d) aux informations classifiées confiées à des personnes et à des organismes extérieurs à un gouvernement (ou à un organisme civil ou militaire de l'OTAN), par exemple des consultants, des entreprises ou des universités.

7. L'accès aux informations ATOMAL et leur protection sont régis par l'Accord entre les États Parties au Traité de l'Atlantique Nord relatif à la coopération dans le domaine des renseignements atomiques (C-M(64)39). L'accès à ces informations, leur manipulation et leur protection doivent obéir aux dispositions administratives d'application de l'Accord entre les États Parties au Traité de l'Atlantique Nord pour la coopération dans le domaine des informations ATOMAL (C-M(68)41).

8. L'accès aux informations US-SIOP et leur protection sont régis par les dispositions du C-M(71)27(révisé), « Procédures spéciales de protection au sein de l'OTAN des renseignements relatifs au plan opérationnel unique intégré des États-Unis (US-SIOP) ».

9. Le caractère sensible des informations, des opérations, des sources et des méthodes ROEM (renseignement d'origine électromagnétique) impose la mise en œuvre de règles et procédures de sécurité rigoureuses allant souvent au-delà de celles qui sont décrites dans le présent C-M. C'est pourquoi l'accès et la protection des informations, des opérations, des sources et des méthodes ROEM sont soumis aux réglementations nationales ainsi qu'aux dispositions du MC 101 (Politique de l'OTAN en matière de renseignement d'origine électromagnétique), de la publication interalliée interarmées (AJP) qui s'y rapporte et du guide pour l'administration et les procédures ROEM établi par le Comité consultatif OTAN sur le renseignement d'origine électromagnétique (NACSI).

ORGANE D'APPROBATION

10. Le Conseil de l'Atlantique Nord a approuvé le présent document, qui met en œuvre l'Accord sur la sécurité des informations entre les Parties au Traité de l'Atlantique Nord (texte reproduit en pièce jointe « A ») et qui énonce donc la politique de sécurité de l'OTAN[2].

---

1 Pays non OTAN et autres entités non OTAN (par exemple organisations internationales), y compris les individus qui représentent ces pays ou entités.

2 Comme indiqué dans le mandat du Comité de sécurité (C-M(2015)0002), la politique de sécurité de l'OTAN comprend les C-M(2002)49 et C-M(2002)50.

PIÈCE JOINTE « A »

ACCORD SUR LA SÉCURITÉ DES INFORMATIONS ENTRE LES PARTIES AU TRAITÉ DE L'ATLANTIQUE NORD

Les Parties au Traité de l'Atlantique Nord, signé à Washington le 4 avril 1949 ;

Réaffirmant que l'efficacité de la consultation politique, de la coopération et de l'établissement de plans de défense au service des objectifs du Traité exige l'échange d'informations classifiées entre les Parties ;

Considérant que des dispositions sont nécessaires entre les Gouvernements des Parties au Traité de l'Atlantique Nord pour la protection et la sauvegarde réciproques des informations classifiées échangées entre eux ;

Considérant qu'un cadre général pour les normes et les procédures de sécurité est nécessaire ;

Agissant en leur nom propre et au nom de l'Organisation du Traité de l'Atlantique Nord, sont convenues de ce qui suit :

ARTICLE 1

Les Parties :

(i) veillent à la protection et à la sauvegarde :

  (a) des informations classifiées (voir annexe 1), identifiées comme telles, qui émanent de l'OTAN (voir annexe 2) ou qui sont soumises à l'OTAN par un État membre ;

  (b) des informations classifiées, identifiées comme telles, soumises par un État membre à un autre État membre à l'appui d'un programme, projet ou contrat de l'OTAN ;

(ii) conservent la classification de sécurité des informations visées à l'alinéa (i) ci-dessus et mettent tout en œuvre pour assurer leur protection en conséquence ;

(iii) s'abstiennent d'exploiter les informations classifiées visées à l'alinéa (i) ci-dessus à des fins autres que celles prévues par le Traité de l'Atlantique Nord ou les décisions et résolutions qui s'y rapportent ;

(iv) s'abstiennent de communiquer les informations visées à l'alinéa (i) ci-dessus à des Parties non OTAN sans l'accord de l'originateur.

ARTICLE 2

En application de l'Article 1 du présent Accord, les Parties veillent à la création d'une autorité nationale de sécurité pour les activités de l'OTAN, autorité qui met en œuvre des systèmes

de sécurité préventive. Les Parties établissent et appliquent des normes de sécurité qui garantissent un même degré de protection des informations classifiées.

ARTICLE 3

(1) Les Parties s'assurent que tout ressortissant qui, dans l'accomplissement de ses fonctions officielles, aurait besoin d'accéder à des informations classifiées CONFIDENTIEL et au-dessus ou pourrait avoir accès à de telles informations, possède une habilitation de sécurité appropriée avant sa prise de fonctions.

(2) Les procédures d'habilitation de sécurité doivent avoir pour but de déterminer si une personne peut, compte tenu de sa loyauté et de sa fiabilité, avoir accès à des informations classifiées sans constituer un risque inacceptable pour la sécurité.

(3) Sur demande, les Parties coopèrent avec les autres Parties en vue de l'exécution de leurs procédures d'habilitation de sécurité respectives.

ARTICLE 4

Le Secrétaire général s'assure que les dispositions du présent Accord qui la concernent sont appliquées par l'OTAN (voir annexe 3).

ARTICLE 5

Le présent Accord n'empêche nullement les Parties de conclure d'autres accords portant sur l'échange d'informations classifiées qui émanent d'elles et qui n'ont aucun rapport avec l'objet du présent Accord.

ARTICLE 6

(a) Le présent Accord sera ouvert à la signature des Parties au Traité de l'Atlantique Nord et sera sujet à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation seront déposés auprès du Gouvernement des États-Unis d'Amérique.

(b) Le présent Accord entrera en vigueur trente jours après la date du dépôt, par deux États signataires, de leurs instruments de ratification, d'acceptation ou d'approbation. Pour chacun des autres États signataires, il entrera en vigueur trente jours après le dépôt de leur propre instrument de ratification, d'acceptation ou d'approbation.

(c) S'agissant des Parties pour lesquelles il sera entré en vigueur, le présent Accord annulera et remplacera la « Convention sur la sécurité entre les États signataires du Traité de l'Atlantique Nord » approuvée par le Conseil de l'Atlantique Nord dans l'annexe A (paragraphe 1) à l'appendice à la pièce jointe au D.C. 2/7, du 19 avril 1952, puis incorporée à la pièce jointe « A » (paragraphe 1) au C-M(55)15(définitif), approuvée par le Conseil de l'Atlantique Nord le 2 mars 1955.

ARTICLE 7

Le présent Accord reste ouvert à l'adhésion de tout nouvel État partie au Traité de l'Alliance Nord conformément à sa propre procédure constitutionnelle. Son instrument d'adhésion devra être

déposé auprès du Gouvernement des États-Unis d'Amérique. Le présent Accord entrera en vigueur pour chacun des États y adhérant trente jours après la date du dépôt de son instrument d'adhésion.

ARTICLE 8

Le Gouvernement des États-Unis d'Amérique informera les Gouvernements des autres Parties du dépôt de chaque instrument de ratification, d'acceptation, d'approbation ou d'adhésion.

ARTICLE 9

Le présent Accord pourra être dénoncé par chaque Partie au moyen d'une notification écrite de dénonciation adressée au dépositaire, qui informera toutes les autres Parties de cette notification. La dénonciation prendra effet un an après réception de la notification par le dépositaire. Toutefois, elle n'affectera pas les obligations contractées ni les droits ou facultés acquis antérieurement par les Parties en vertu des dispositions du présent Accord.

En foi de quoi les Représentants ci-dessous, dûment autorisés à cet effet par leurs Gouvernements respectifs, ont signé le présent Accord.

Fait à Bruxelles, le .. .. XXXX, en un seul exemplaire, en langues anglaise et française, chaque texte faisant également foi, qui sera versé aux archives du Gouvernement des États-Unis d'Amérique, qui en transmettra des copies certifiées conformes à chacun des autres signataires.

ANNEXE 1

Cette annexe fait partie intégrante de l'Accord.

Les informations classifiées OTAN sont définies comme suit :

(a) le terme « informations » désigne toute connaissance pouvant être communiquée sous quelque forme que ce soit ;

(b) les termes « informations classifiées » désignent des informations ou des matériels qu'il faut protéger contre une divulgation non autorisée, conformément à leur classification de sécurité ;

(c) le terme « matériel » englobe le document et tout élément de machine, d'équipement ou d'arme, fabriqué ou en cours de fabrication ;

(d) le terme « document » désigne toute information enregistrée, quelles qu'en soient la forme ou les caractéristiques physiques, y compris – sans aucune restriction – les écrits et les imprimés, les cartes et les bandes perforées, les cartes géographiques, les graphiques, les photographies, les peintures, les dessins, les gravures, les croquis, les notes et documents de travail, les carbones et les rubans encreurs, ou les reproductions effectuées par quelque moyen ou procédé que ce soit, ainsi que les données sonores, la voix, toute forme d'enregistrements magnétiques, électroniques, optiques ou vidéo, de même que l'équipement informatique portatif avec support de mémoire fixe et amovible.

ANNEXE 2

Cette annexe fait partie intégrante de l'Accord.

Pour le but du présent Accord, le mot « OTAN » signifie l'Organisation du Traité de l'Atlantique Nord, et les organismes régis soit par la Convention sur le statut de l'Organisation du Traité de l'Atlantique Nord, des représentants nationaux et du personnel international signé à Ottawa le 20 septembre 1951, soit par le Protocole sur le statut des quartiers généraux militaires internationaux crées en vertu du Traité de l'Atlantique Nord signé à Paris le 28 août 1952.

ANNEXE 3

Cette annexe fait partie intégrante de l'Accord.

Afin de respecter leurs prérogatives, des consultations se déroulent avec les commandants militaires.

PIÈCE JOINTE « B »

PRINCIPES DE BASE, NORMES MINIMALES ET RESPONSABILITÉS

PRINCIPES DE BASE

1. Les principes de base énoncés ci-dessous sont à appliquer :

   (a) les pays et les organismes civils et militaires de l'OTAN veillent à ce que les normes minimales agréées énoncées dans le présent C-M soient appliquées afin d'assurer un degré commun de protection des informations classifiées échangées entre les parties ;

   (b) compte tenu de la responsabilité de partager, les informations classifiées sont diffusées uniquement sur la base du besoin d'en connaître[1] à des personnes qui ont été informées des procédures de sécurité applicables ;

   (c) seules les personnes dûment habilitées ont accès aux informations classifiées NATO CONFIDENTIEL ou d'un niveau de classification supérieur ;

   (d) la délivrance d'une habilitation de sécurité n'est pas considérée comme l'étape finale du processus d'évaluation du droit d'une personne à avoir accès à des informations classifiées, étant donné que des procédures continues de sécurité concernant le personnel, dites d'« accompagnement », sont mises en place pour gérer la menace intérieure[2] ;

   (e) le Bureau de sécurité de l'OTAN (NOS) coordonne la gestion de la menace intérieure, en collaboration avec les autorités nationales compétentes et les organismes civils et militaires de l'OTAN ;

   (f) la gestion des risques de sécurité[3] est obligatoire dans les organismes civils et militaires de l'OTAN, conformément au processus OTAN de gestion des risques de sécurité (AC/35-D/1035). Son application dans les pays de l'OTAN est facultative. La gestion des risques ne doit pas servir à contourner la politique de sécurité ;

---

1 Principe selon lequel il est établi avec certitude qu'un destinataire potentiel a besoin d'accéder à des informations, d'en prendre connaissance ou d'entrer en leur possession, pour accomplir des tâches ou fournir des services officiels.

2 La « menace intérieure » provient de membres du personnel qui, de par leur rôle au sein de l'Organisation, ont un accès privilégié aux informations OTAN classifiées et/ou aux biens de l'OTAN, et qui abusent ensuite de cet accès pour détruire, endommager, supprimer ou divulguer des informations OTAN classifiées et/ou des biens de l'OTAN, que ce soit intentionnellement ou par négligence.

3 Approche systématique visant à déterminer quelles contre-mesures de sécurité sont requises pour protéger les informations ainsi que les services et ressources connexes sur la base d'une évaluation des menaces et des vulnérabilités. La gestion des risques suppose qu'il y ait une planification, une organisation, une orientation et un contrôle des ressources propres à garantir que les risques restent dans des limites acceptables.

(g) les pays et les organismes civils et militaires de l'OTAN établissent au sein de leurs services des programmes de formation et de sensibilisation à la sécurité qui concernent tous les aspects de sécurité décrits à l'alinéa (l) ci-après ;

(h) tous les cas suspectés de violation de sécurité et de compromission d'informations classifiées sont signalés immédiatement à l'autorité de sécurité compétente ;

(i) les originateurs communiquent des informations classifiées à l'OTAN et à des pays de l'OTAN à l'appui d'un programme, projet ou contrat OTAN à condition que celles-ci soient gérées et protégées conformément à la politique de gestion de l'information OTAN (NIMP) et à la politique de sécurité de l'OTAN ;

(j) les informations classifiées font l'objet d'un contrôle de l'originateur[4] ;

(k) la communication d'informations OTAN classifiées se fait selon les procédures et critères correspondants en vigueur, et dans tous les cas, un degré de protection au moins égal à celui qui est spécifié dans le présent C-M et les directives complémentaires est requis pour toute information OTAN classifiée qui serait communiquée ;

(l) les informations classifiées sont protégées par un ensemble équilibré de mesures de sécurité qui concernent les sujets suivants : sécurité concernant le personnel, sécurité physique, sécurité des informations et sécurité des systèmes d'information et de communication (SIC). Les informations classifiées transmises à des contractants et communiquées à des entités non OTAN (NNE) sont également protégées grâce à l'application des procédures prévues par la présente politique. Ces prescriptions s'étendent à toutes les personnes ayant accès à des informations classifiées, aux supports contenant des informations classifiées et aux locaux où sont conservées de telles informations ;

(m) les établissements qui détiennent des informations OTAN classifiées mettent en place des mécanismes et des processus pour garantir le respect des prescriptions de la politique de sécurité de l'OTAN lorsque les conditions opérationnelles sont dégradées, y compris en cas d'incident occasionnant une interruption de service. Ces mécanismes et processus sont définis dans un plan de continuité d'activité ou dans un plan de reprise d'activité, selon la nature de l'incident.

PROTECTION DES INFORMATIONS RELATIVES AUX POINTS SENSIBLES

2. La publication d'informations sur des installations civiles critiques (matériels de défense, approvisionnement énergétique) revêtant une importance du point de vue militaire en période de tension ou de guerre peut faciliter la mise en œuvre d'une attaque cinétique ou d'un acte de sabotage en permettant à des ennemis potentiels ou à des terroristes de dresser une liste des points sensibles et de l'utiliser pour déterminer les éléments qui pourraient être vulnérables à une attaque. Il convient de prendre les mesures qui s'imposent pour s'assurer que ces informations ne sont pas disponibles librement dans le domaine public, et ce afin d'éviter que des ennemis les utilisent à des fins hostiles. Par ailleurs, les propriétaires et les opérateurs d'installations doivent être pleinement conscients du risque qui pèse sur eux et prendre les mesures nécessaires pour protéger ces informations.

[4] Principe selon lequel le pays, l'OTAN ou l'entité sous l'autorité duquel/de laquelle l'information a été créée, produite ou introduite à l'OTAN fixe les règles et les normes applicables à l'emploi de cette information et a toute latitude pour y apporter toutes modifications au cours du cycle de vie de ladite information.

RESPONSABILITÉS EN MATIÈRE DE SÉCURITÉ

Autorité nationale de sécurité (ANS)

3. Chaque pays de l'OTAN met en place une autorité nationale de sécurité (ANS) à laquelle il confie la sécurité des informations OTAN classifiées. L'ANS est le point de contact principal du NOS pour toute question concernant la sécurité à l'OTAN. Par la suite, l'ANS peut orienter le NOS vers l'autorité de sécurité désignée (ASD) appropriée ou une autre autorité de sécurité compétente.

4. L'ANS a pour tâche :

(a) d'assurer la sécurité des informations OTAN classifiées dans les organismes et services nationaux militaires ou civils, dans le pays ou à l'étranger ;

(b) de veiller à ce que l'on procède à des inspections périodiques et appropriées des dispositions de sécurité prises pour assurer la protection des informations OTAN classifiées dans tous les organismes nationaux, à tous les niveaux, tant militaires que civils, afin de vérifier que les informations OTAN classifiées bénéficient d'une protection adéquate conformément aux règles de sécurité en vigueur à l'OTAN. Dans le cas d'organismes détenant des informations COSMIC TRÈS SECRET (CTS) ou ATOMAL, des inspections de sécurité sont réalisées au moins une fois tous les 24 mois, sauf si, pendant cette période, elles sont effectuées par le NOS ;

(c) de s'assurer qu'une habilitation de sécurité du personnel (PSC) est délivrée à tous les ressortissants appelés à avoir accès à des informations classifiées NATO CONFIDENTIEL ou d'un niveau de classification supérieur, conformément à la politique de sécurité de l'OTAN ;

(d) de s'assurer que des plans de sécurité en cas d'urgence sont en place pour éviter que des informations OTAN classifiées ne tombent entre les mains de personnes non autorisées ou ennemies ;

(e) d'autoriser la création (ou la fermeture) de bureaux d'ordre centraux COSMIC nationaux. La création (ou la suppression) d'un bureau d'ordre COSMIC est signalée au NOS.

Autorité de sécurité désignée (ASD)

5. L'ASD est l'autorité chargée d'informer l'industrie de la politique nationale couvrant tous les aspects de la politique de sécurité industrielle de l'OTAN, et de fournir les orientations et l'assistance nécessaires pour que cette politique soit appliquée. Dans certains pays, la fonction d'ASD peut être remplie par l'ANS.

Comité de sécurité

6. Le Comité de sécurité est établi par le Conseil de l'Atlantique Nord ; il se compose de représentants des ANS/ASD de chacun des pays de l'OTAN, auxquels sont adjoints, en cas de besoin, d'autres responsables de la sécurité de ces pays. Des représentants de l'État-major militaire international (EMI), des commandements stratégiques et du Bureau des C3 (consultation, commandement et contrôle) participent aux réunions du Comité de sécurité. Des représentants des organismes civils et militaires de l'OTAN peuvent également y assister lorsque les questions traitées les intéressent. La présidence du Comité de sécurité au niveau des représentants principaux (AC/35), en configuration Politique de sécurité (AC/35(SP)) et en configuration Sécurité des SIC (AC/35(CISS)) est assurée par le NOS.

7. Le Comité de sécurité relève directement du Conseil pour ce qui concerne :

(a) la revue de la politique de sécurité de l'OTAN (énoncée dans les C-M(2002)49 et C-M(2002)50) et la formulation de recommandations au Conseil sur la modification de cette politique et son approbation ;

(b) l'étude des questions concernant la politique de sécurité de l'OTAN ;

(c) la revue et l'approbation des directives complémentaires et des documents d'orientation publiés pour les besoins de la politique de sécurité de l'OTAN[5] ;

(d) l'étude des questions de sécurité qui lui sont soumises par le Conseil, un pays de l'OTAN, le secrétaire général, le Comité militaire, le Bureau des C3 ou les chefs des organismes civils et militaires de l'OTAN, et la formulation de recommandations appropriées concernant ces questions.

Bureau de sécurité de l'OTAN (NOS)

8. Le NOS est établi au sein du Secrétariat international de l'OTAN, où il fait partie de la Division civilo-militaire Renseignement et sécurité. Il se compose de personnes ayant l'expérience des questions de sécurité aussi bien dans le domaine civil que dans le domaine militaire. Il se tient en liaison étroite avec les ANS*/*ASD des pays de l'OTAN, ainsi qu'avec les organismes civils et militaires de l'OTAN. Le NOS peut également, selon les besoins, demander aux pays et aux organismes civils et militaires de l'OTAN de lui fournir d'autres spécialistes en matière de sécurité pour l'aider pendant des périodes limitées, lorsque le renforcement du Bureau par du personnel à plein temps ne se justifie pas.

9. Le NOS est chargé :

(a) d'examiner toute question touchant à la sécurité de l'OTAN ;

(b) de trouver des moyens d'améliorer la sécurité à l'OTAN ;

(c) de coordonner globalement la sécurité de l'OTAN entre les pays de l'Alliance et les organismes civils et militaires de l'OTAN ;

(d) d'assurer l'exécution et la supervision de la politique de sécurité de l'OTAN, et notamment de donner aux pays et aux organismes civils et militaires de l'OTAN les conseils dont ils peuvent avoir besoin, soit pour l'application des principes de base et des normes de sécurité définis dans la présente pièce jointe, soit pour la mise en œuvre des impératifs de sécurité spécifiques ;

(e) d'informer, lorsqu'il y a lieu, le Comité de sécurité, le secrétaire général et le président du Comité militaire des conditions de sécurité au sein de l'OTAN et des progrès accomplis dans l'exécution des décisions du Conseil en matière de sécurité ;

[5] Un pays de l'OTAN peut demander qu'une directive complémentaire soit également approuvée par le Conseil.

(f) de procéder à des inspections périodiques des systèmes de sécurité en vigueur pour la protection des informations OTAN classifiées dans les pays de l'OTAN, dans les organismes civils de l'OTAN ainsi qu'au SHAPE et au QG du SACT[6] ;

(g) d'effectuer des visites de sécurité dans les NNE avec lesquelles l'OTAN a signé un accord de sécurité à des fins de certification dans un premier temps, puis régulièrement pour veiller au respect de la politique de sécurité de l'OTAN ;

(h) de coordonner les enquêtes avec les ANS/ASD et les organismes civils et militaires de l'OTAN, en cas de perte ou de compromission avérée ou présumée d'informations OTAN classifiées ;

(i) de communiquer aux ANS**/**ASD toute information défavorable qui aurait été recueillie au sujet de ressortissants de leur pays, le cas échéant ;

(j) d'arrêter les mesures de sécurité à prendre pour la protection du siège de l'OTAN et d'en assurer l'application correcte ;

(k) sous la direction et au nom du secrétaire général, de contrôler l'application du programme de sécurité de l'OTAN à la protection des informations ATOMAL en vertu de l'Accord (C-M(64)39) et des Dispositions administratives complémentaires (C-M(68)41).

Comité militaire et organismes militaires de l'OTAN

10. En tant que plus haute autorité militaire de l'OTAN, le Comité militaire est responsable de la conduite générale des affaires militaires. Il est par conséquent chargé de toutes les questions de sécurité qui se posent dans le cadre de la structure militaire de l'OTAN, et notamment de la détermination globale et centralisée des mesures nécessaires pour assurer l'adéquation des techniques et matériels cryptographiques utilisés pour la transmission d'informations OTAN classifiées, ce qui inclut l'approbation, du point de vue de la sécurité, des équipements cryptographiques financés par l'OTAN, tels que définis dans la pièce jointe « F ». Conformément à la politique agréée antérieurement et aux paragraphes 8 et 9 plus haut, le NOS assure l'exécution des mesures de sécurité entrant dans le cadre de la structure militaire de l'OTAN et veille à informer le président du Comité militaire

11. Les chefs des organismes militaires de l'OTAN mis en place sous l'égide du Comité militaire sont compétents pour toutes les questions de sécurité qui se posent dans leurs établissements. Il leur incombe donc, entre autres, de veiller à la mise sur pied de structures de sécurité, à la conception des mesures et des procédures de sécurité appropriées et à leur exécution conformément à la politique de sécurité de l'OTAN, ainsi qu'à l'inspection périodique, à chaque niveau de commandement, des dispositions prises. Dans le cas d'organismes détenant des informations CTS ou ATOMAL, des inspections de sécurité doivent être effectuées au moins une fois tous les 24 mois, sauf si, pendant cette période, le NOS s'en est chargé.

[6] Sur demande du NOS, les pays de l'OTAN peuvent participer aux inspections que le NOS réalise dans les organismes civils et militaires de l'OTAN en qualité d'observateurs ou de membres actifs de l'équipe d'inspection. Ceci ne s'applique toutefois pas aux organismes civils au sein desquels tous les pays de l'OTAN ne sont pas représentés.

Organismes civils de l'OTAN

12. Le Secrétariat international et les organismes civils de l'OTAN sont responsables envers le Conseil du maintien de la sécurité en leur sein. Il leur incombe donc, entre autres, de veiller à la mise sur pied de structures de sécurité, à l'établissement des programmes de sécurité et à leur exécution conformément à la politique de sécurité de l'OTAN, ainsi qu'à l'inspection périodique, à chaque niveau de commandement, des dispositions prises. Dans le cas d'organismes détenant des informations CTS ou ATOMAL, des inspections de sécurité doivent être effectuées au moins une fois tous les 24 mois, sauf si, pendant cette période, le NOS s'en est chargé.

SUPERVISION DE LA SÉCURITÉ DES CENTRES D'EXCELLENCE[7]/ORGANISMES RÉGIS PAR UN MÉMORANDUM D'ENTENTE

13. La supervision de la sécurité est définie comme la fonction de surveillance visant à garantir que tout organisme qui manipule des informations OTAN classifiées applique correctement la politique de sécurité de l'OTAN relative à leur protection. Pour les organismes qui se trouvent en dehors de la structure de commandement de l'OTAN (NCS), la supervision des mesures de sécurité concernant la protection des informations OTAN classifiées sera assurée comme suit.

(a) Les pays participants sont responsables de la sécurité au sein de leurs organismes militaires de l'OTAN et doivent prendre les dispositions qui s'imposent pour l'assurer. Les pays dans lesquels se trouvent un ou plusieurs de ces éléments – à savoir les pays hôtes – doivent prendre en charge la supervision de leur sécurité, sauf si des dispositions spécifiques ont été agréées à cet égard.

(b) Les centres d'excellence/organismes régis par un mémorandum d'entente (MOU) peuvent être activés en tant qu'organismes militaires de l'OTAN, si le Conseil en prend la décision. Dans ce cas, la politique de sécurité de l'OTAN s'applique, et le chef du centre d'excellence/de l'organisme régi par un MOU est responsable de toutes les questions de sécurité au sein de son établissement. Les pays participants sont responsables de la sécurité au sein de tout centre d'excellence/organisme régi par un MOU, et doivent prendre les dispositions qui s'imposent. Le pays hôte prend en charge la supervision de la sécurité, sauf si les pays participants se sont mis d'accord sur d'autres dispositions.

(c) Si un centre d'excellence/organisme régi par un MOU n'est pas activé en tant qu'organisme militaire de l'OTAN (et, par conséquent, ne se voit pas accorder un statut international par le Conseil) mais est homologué en tant que centre d'excellence/organisme régi par un MOU de l'OTAN, la politique de sécurité de l'OTAN s'applique. Bien que les pays participants soient responsables de toutes les questions de sécurité dans le centre d'excellence/l'organisme régi par un MOU, le pays hôte prend en charge la supervision de la sécurité, sauf si les pays participants se sont mis d'accord sur d'autres dispositions. Tout MOU fondateur doit contenir une description des modalités de mise en œuvre de cette supervision au sein du centre d'excellence/de l'organisme régi par un MOU.

(d) Si une entité multinationale implantée dans l'un des pays de l'OTAN n'est ni homologuée en tant que centre d'excellence, ni activée en tant qu'organisme militaire de l'OTAN, mais utilise des informations OTAN classifiées, la politique de sécurité de l'OTAN s'applique et

[7] Centres d'excellence dont l'existence a été approuvée par le Conseil conformément au PO(2020)0038 (INV).

les pays participants restent responsables des questions de sécurité. En cas de participation d'un pays non OTAN, un accord de sécurité avec celui-ci doit être conclu avant que des informations classifiées puissent être échangées. Dans ce cas, le pays hôte prend en charge la supervision de la sécurité, sauf si les pays participants se sont mis d'accord sur d'autres dispositions. Tout MOU fondateur doit contenir une description des modalités de mise en œuvre de cette supervision au sein de l'entité multinationale.

COORDINATION DE LA SÉCURITÉ

14. Tout problème de sécurité entre les ANS*/*ASD des pays de l'OTAN et les organismes civils et militaires de l'OTAN ne pouvant être réglé, ou tout problème concernant la mise en application ou l'interprétation de la politique de sécurité de l'OTAN est soumis au NOS. Lorsque ce sont les autorités militaires qui soumettent un tel problème, celles-ci passent par la chaîne de commandement. Le NOS soumet à l'examen du Comité de sécurité toute divergence non résolue.

MODIFICATIONS DE LA POLITIQUE DE SÉCURITÉ

15. Toute proposition de pays ou d'organismes civils ou militaires de l'OTAN visant à modifier la politique de sécurité de l'OTAN doit être soumise en premier lieu au NOS. Toute proposition formulée par les autorités militaires est transmise via la chaîne de commandement. Les propositions sont examinées par le NOS et, si nécessaire, soumises au Comité de sécurité pour un examen plus approfondi. Les dispositions du présent paragraphe n'excluent pas la possibilité que les ANS*/*ASD des pays de l'OTAN fassent officiellement des propositions au Comité de sécurité si elles le souhaitent.

PIÈCE JOINTE « C »

SÉCURITÉ CONCERNANT LE PERSONNEL

INTRODUCTION

1. La présente pièce jointe énonce la politique et les normes minimales pour la sécurité concernant le personnel. Des précisions et des prescriptions supplémentaires sont données dans la directive complémentaire sur la sécurité concernant le personnel (AC/35-D/2000).

2. Des processus de sécurité concernant le personnel sont établis afin d'évaluer si une personne peut, eu égard à sa loyauté, à la confiance qui peut lui être accordée et à sa fiabilité, être autorisée à avoir accès à des informations classifiées sans que cela constitue un risque inacceptable du point de vue de la sécurité. À cet effet, toute personne[1], civil ou militaire, dont les tâches ou fonctions nécessitent un accès à des informations classifiées CONFIDENTIEL[2] ou d'un niveau de classification supérieur fait l'objet d'une enquête en bonne et due forme, afin qu'il puisse être déterminé avec un degré de confiance satisfaisant si un accès à ce type d'information peut lui être octroyé et, partant, si elle peut se voir délivrer une habilitation de sécurité du personnel (PSC)[3] de son pays.

3. Pour ce qui est de l'accès à des informations classifiées NATO CONFIDENTIEL (NC) ou d'un niveau de classification supérieur, il est nécessaire que la personne soit titulaire d'une PSC en cours de validité délivrée par son pays pour ce niveau de classification et que l'ANS/ASD appropriée ou autre autorité de sécurité compétente ait confirmé que ladite personne peut être autorisée à accéder à des informations OTAN classifiées.

APPLICATION DU PRINCIPE DU BESOIN D'EN CONNAÎTRE

4. Dans les pays et les organismes civils et militaires de l'OTAN, les personnes concernées ne peuvent avoir accès qu'aux informations OTAN classifiées pour lesquelles elles justifient du besoin d'en connaître. Nul n'a le droit, du seul fait de son grade ou de sa fonction, ou de sa PSC, d'accéder à des informations OTAN classifiées.

HABILITATION DE SÉCURITÉ DU PERSONNEL (PSC)

5. La politique de sécurité de l'OTAN ne requiert aucune PSC pour l'accès aux informations classifiées NATO DIFFUSION RESTREINTE (NDR)[4]. Les personnes appelées à accéder uniquement à des informations classifiées NDR doivent avoir été informées de leurs obligations

---

1 Excepté les hauts responsables gouvernementaux visés au paragraphe 7 de la présente pièce jointe.

2 En vertu de leurs lois et règlements nationaux, certains pays exigent une habilitation de sécurité du personnel pour l'accès à des informations classifiées du niveau DIFFUSION RESTREINTE ou l'équivalent national.

3 Décision positive par laquelle une ANS/ASD ou une autre autorité de sécurité compétente reconnaît officiellement le droit d'une personne d'avoir accès à des informations classifiées NC et d'un niveau de classification supérieur, eu égard à sa loyauté, à la confiance qui peut lui être accordée et à sa fiabilité.

4 En vertu de leurs lois et règlements nationaux, certains pays de l'OTAN peuvent exiger une PSC pour l'accès à des informations classifiées NDR.

pour ce qui est de la protection des informations OTAN classifiées[5], avoir déclaré être conscientes de leurs responsabilités soit par écrit, soit par un moyen équivalent assurant la non-répudiation, et pouvoir justifier du besoin d'en connaître.

6. Une PSC appropriée est requise pour toute personne appelée à avoir accès à des informations classifiées NC ou d'un niveau de classification supérieur ou susceptible d'avoir accès à de telles informations dans l'exercice de ses fonctions. De plus, les personnes concernées doivent :

(a) avoir le besoin d'en connaître ;

(b) avoir été informées de leurs obligations pour ce qui est de la protection des informations OTAN classifiées ;

(c) avoir déclaré être conscientes de leurs responsabilités, soit par écrit, soit par une méthode équivalente assurant la non-répudiation.

7. En dérogation aux dispositions énoncées aux paragraphes 5 et 6 ci-dessus, l'accès de hauts responsables gouvernementaux (chefs d'État et de gouvernement, ministres, parlementaires et membres du pouvoir judiciaire, par exemple) à des informations OTAN classifiées est régi par les lois et règlements nationaux. Ces hauts responsables doivent être informés de leurs obligations en matière de sécurité et avoir le besoin d'en connaître.

8. Le type de PSC requis et, partant, l'étendue des procédures d'habilitation de sécurité mises en œuvre sont déterminés par le niveau de classification des informations OTAN classifiées auxquelles la personne doit avoir accès. Il doit exister une norme agréée de confiance s'agissant de l'admissibilité des personnes qui se sont vu autoriser l'accès à des informations OTAN classifiées ou dont les tâches ou les fonctions peuvent leur donner accès à de telles informations.

9. La délivrance d'une PSC n'est pas considérée comme l'étape finale du processus : il faut s'assurer qu'une personne reste admissible à l'accès à des informations OTAN classifiées. Cela se fait par une interaction et une évaluation régulière de la part des autorités de sécurité et des gestionnaires, notamment par l'évaluation de tout changement de circonstance ou de comportement qui pourrait avoir un impact sur la sécurité. En outre, il convient de faire un usage judicieux des programmes de formation et de sensibilisation à la sécurité pour rappeler aux intéressés leurs responsabilités en matière de sécurité ainsi que la nécessité de signaler à leurs gestionnaires et aux responsables de la sécurité toute information pouvant modifier leur situation sur le plan de la sécurité.

Circonstances exceptionnelles

10. Des circonstances peuvent survenir où, en raison de l'urgence de la mission, par exemple, certaines des conditions indiquées au paragraphe 6 ne pourraient pas être remplies. Des précisions relatives aux nominations provisoires, à l'accès à titre temporaire et à l'accès en cas d'urgence sont données dans la directive complémentaire sur la sécurité concernant le personnel.

Responsabilités

11. Il incombe au pays de l'OTAN dont ressortit la personne de traiter les demandes de PSC, ce qui implique de veiller à ce que, dans le cadre de la procédure de délivrance des PSC, les prescriptions et les critères minimums en matière d'enquête soient dûment respectés lorsqu'il s'agit

[5] Les pays peuvent utiliser des exposés spécifiques de l'OTAN ou leurs propres exposés si ceux-ci mettent en lumière les différences entre les prescriptions des deux cadres de sécurité.

d'évaluer si une personne est suffisamment loyale, fiable et digne de confiance pour se voir délivrer une PSC ou pour voir sa PSC renouvelée, conformément aux dispositions de la directive sur la sécurité concernant le personnel.

12. Les organismes civils et militaires de l'OTAN sont tenus de soumettre à l'ANS/l'ASD ou autre autorité de sécurité compétente les demandes de PSC et les demandes de renouvellement de PSC pour leur personnel.

13. Les responsabilités détaillées des ANS, des ASD ou autres autorités de sécurité compétentes, des pays de l'OTAN et des chefs des organismes civils et militaires de l'OTAN sont décrites dans la directive sur la sécurité concernant le personnel.

FORMATION ET SENSIBILISATION À LA SÉCURITÉ

14. Toute personne qui occupe un poste où elle peut avoir accès à des informations classifiées NDR ou qui est titulaire d'une habilitation du niveau NC ou d'un niveau de classification supérieur assiste à un exposé sur les procédures de sécurité et ses obligations en matière de sécurité. Toutes les personnes habilitées doivent attester qu'elles comprennent parfaitement leurs responsabilités et les conséquences auxquelles elles s'exposent éventuellement lorsque des informations OTAN classifiées sont transmises, volontairement ou par négligence, à des personnes non autorisées. Un registre de ces attestations de reconnaissance est tenu par le pays ou l'organisme civil ou militaire de l'OTAN qui autorise l'accès à des informations OTAN classifiées.

15. Il importe de signaler d'emblée et de rappeler périodiquement à toutes les personnes qui sont autorisées à accéder à des informations OTAN classifiées ou qui doivent les manipuler quelles sont les menaces que représentent, pour la sécurité, les éléments suivants (liste non exhaustive) :

(a) le comportement de la personne en dehors du bureau, y compris ses activités sur les réseaux sociaux ;

(b) les conversations indiscrètes avec des personnes n'ayant pas le besoin d'en connaître ;

(c) le travail en dehors du bureau et les déplacements ;

(d) les cybermenaces ;

(e) les relations avec les médias ;

(f) la menace que constituent les activités des services de renseignement qui ciblent l'OTAN et ses pays.

16. Il y a lieu de signaler immédiatement à l'autorité de sécurité compétente toute démarche ou manœuvre considérée comme suspecte ou inhabituelle.

PIÈCE JOINTE « D »

SÉCURITÉ PHYSIQUE

INTRODUCTION

1. La présente pièce jointe énonce la politique et les normes minimales relatives aux mesures de sécurité physique pour la protection des informations OTAN classifiées. Des précisions et des prescriptions supplémentaires sont données dans la directive complémentaire sur la sécurité physique (AC/35-D/2001).

2. La sécurité physique consiste à appliquer des mesures de protection physique aux sites, bâtiments, établissements ou installations contenant des informations classifiées qu'il faut protéger contre toute perte ou compromission.

3. Les pays et les organismes civils et militaires de l'OTAN établissent des programmes de sécurité physique comprenant des mesures de sécurité active et passive en vue d'assurer un degré commun de sécurité physique adapté aux menaces telles qu'évaluées, aux vulnérabilités, à la classification de sécurité et au volume des informations à protéger.

IMPÉRATIFS DE SÉCURITÉ

4. Il convient de protéger par des mesures de sécurité physique appropriées chaque local, bureau, établissement, bâtiment, site ou autre zone où des informations OTAN classifiées sont stockées, manipulées et/ou examinées. Au moment de définir le degré de sécurité physique à appliquer, il faut prendre en compte tous les facteurs pertinents, et notamment :

(a) le niveau de classification de sécurité et la catégorie des informations ;

(b) le volume et la forme (copie papier, support électronique ou les deux) des informations classifiées stockées et/ou manipulées ;

(c) le contrôle de l'accès et l'application du principe du besoin d'en connaître ;

(d) la menace émanant de services de renseignement hostiles qui ont pour cible l'OTAN et/ou ses pays membres ainsi que la menace, après évaluation locale, liée à des phénomènes tels que le terrorisme, l'espionnage, le sabotage, la subversion et la criminalité (organisée) ;

(e) le mode de stockage des informations classifiées (copie imprimée ou électronique et chiffrée).

5. Les mesures de sécurité physique sont conçues pour :

(a) empêcher toute intrusion par la ruse ou par la force ;

(b) décourager, empêcher et détecter les attaques de l'intérieur ;

(c) opérer, au niveau des personnels, une ségrégation des accès aux informations OTAN classifiées en fonction de leur niveau d'habilitation de sécurité personnelle (PSC) et de leur besoin d'en connaître ;

(d) permettre de détecter le plus tôt possible tout incident de sécurité et d'y donner suite.

PIÈCE JOINTE « D »
C-M(2002)49-REV1

IMPÉRATIFS GÉNÉRAUX EN MATIÈRE DE SÉCURITÉ PHYSIQUE

6. Les mesures de sécurité physique, qui ne représentent qu'un aspect de la sécurité de protection, doivent être étayées par de solides mesures de sécurité concernant le personnel, de sécurité des informations et de sécurité des systèmes d'information et de communication (SIC). Une gestion rationnelle des risques de sécurité implique la détermination des méthodes les plus adaptées, les plus efficaces et les plus rentables pour contrer les menaces et compenser les vulnérabilités par une combinaison de mesures de protection appartenant à chacun de ces domaines. La meilleure façon de parvenir à l'efficacité et à la rentabilité souhaitées est de définir des impératifs de sécurité physique dans le cadre de la planification et de la conception de locaux, afin d'éviter ainsi de devoir procéder à des travaux de rénovation coûteux.

7. Les programmes de sécurité physique reposent sur le principe de la défense en profondeur et font appel à différentes mesures de sécurité physique complémentaires offrant un degré de protection qui correspond aux impératifs associés au niveau de criticité et de vulnérabilité de l'organisme visé et des informations en sa possession.

8. Bien que les mesures de sécurité physique soient propres à chaque site et qu'elles soient déterminées par un certain nombre de facteurs, les principes généraux suivants s'appliquent :

(a) il faut, dans un premier temps, identifier les moyens qui exigent une protection, puis créer des mesures de sécurité sur plusieurs lignes pour permettre une « défense en profondeur » et retarder une intrusion ;

(b) les mesures de sécurité physique les plus extérieures définissent la zone protégée et sont destinées à décourager tout accès non autorisé ;

(c) les mesures de la ligne suivante détectent tout accès non autorisé ou toute tentative d'accès et alertent les services de sécurité ;

(d) les mesures mises en œuvre au niveau de la ligne la plus intérieure retardent suffisamment l'intrus pour qu'il puisse être appréhendé par les services de sécurité — il existe donc une corrélation entre le délai de réaction des services de sécurité et les mesures de sécurité physique destinées à retarder un intrus.

9. Les équipements destinés à assurer la sécurité physique (vidéosurveillance, système de détection des intrusions (IDS), armoires fortes, etc.) font l'objet d'une maintenance régulière ou liée à une raison spécifique afin de garantir des performances maximales. Il faut en outre réévaluer périodiquement l'efficacité de chacune des mesures de sécurité et de l'ensemble du système de sécurité. C'est particulièrement important si un changement intervient dans l'utilisation du site ou dans certains éléments spécifiques du système de sécurité. L'activation régulière des plans de sécurité, dans le cadre d'exercices, peut le permettre.

Zones de sécurité

10. Les zones de sécurité sont des zones fixes ou temporaires où sont conservées, manipulées et/ou examinées des informations classifiées NATO CONFIDENTIEL ou d'un niveau de classification supérieur. Elles doivent être organisées et structurées de façon à correspondre à l'une des catégories suivantes :

(a) **zone de sécurité OTAN de classe I** : zone particulièrement sensible dans laquelle des informations classifiées NC ou d'un niveau de classification supérieur sont conservées, manipulées et/ou examinées de telle façon que le fait de pénétrer dans cette zone équivaut en pratique à avoir accès à des informations OTAN classifiées

et que tout accès non autorisé constitue dès lors une violation de sécurité. Ces zones, qui peuvent par exemple comprendre les salles d'opérations, les centres de communications ou les locaux d'archives, nécessitent :

(i) d'établir de façon précise un périmètre protégé dont toutes les entrées et sorties sont contrôlées ;

(ii) de mettre en place un système de contrôle des entrées laissant pénétrer uniquement les personnes dûment habilitées et expressément autorisées[1] à y accéder ;

(iii) de déterminer le niveau de classification de sécurité et la catégorie des informations qui y sont conservées habituellement, c'est-à-dire celles auxquelles le fait d'y pénétrer donne accès ;

(iv) d'indiquer clairement que l'entrée dans les zones concernées nécessite une autorisation spéciale de l'autorité de sécurité locale. Le niveau de classification de sécurité et/ou la sensibilité de la zone concernée peut figurer sur l'indication en question.

(b) **Zone de sécurité OTAN de classe II** : zone dans laquelle des informations classifiées NC ou d'un niveau de classification supérieur sont conservées, manipulées et/ou examinées de telle façon qu'elles peuvent être protégées contre l'accès de personnes non autorisées au moyen de contrôles internes. Ces zones, qui peuvent comprendre des bureaux ou des salles de réunion dans lesquels des informations OTAN classifiées sont conservées, manipulées et/ou examinées nécessitent :

(i) d'établir de façon précise un périmètre protégé dont toutes les entrées et sorties sont contrôlées ;

(ii) de mettre en place un système de contrôle des entrées n'y laissant pénétrer sans escorte que les personnes dûment habilitées et autorisées à y accéder ;

(iii) de prévoir un dispositif d'escorte ou un mécanisme de contrôle équivalent pour les personnes qui ne satisfont pas aux critères énoncés à l'alinéa (b) (ii) ci-dessus, afin de les empêcher d'accéder à des informations OTAN classifiées et de pénétrer librement dans des zones qui ont été spécifiquement désignées comme étant des zones protégées contre les attaques techniques et les systèmes d'écoute.

Zone administrative

11. Une zone administrative est définie autour ou en amont des zones de sécurité de classe I ou II. Seules des informations classifiées NDR peuvent être conservées, manipulées et/ou examinées dans les zones administratives Ces zones nécessitent d'établir de façon visible un périmètre permettant de contrôler les personnes et les véhicules. Les visiteurs ne sont toutefois pas tenus d'être escortés.

[1] Par personne expressément autorisée, on entend un membre du personnel pour lequel il a été officiellement reconnu qu'il a le besoin d'en connaître et qu'il doit accéder aux zones concernées en raison de la nature de ses fonctions, et dont le nom figure sur les listes de contrôle d'accès, ainsi que toute personne qui a été officiellement autorisée, sur une base ad hoc, par le chef de l'organisation concernée pour remplir un rôle ou une fonction spécifique.

Zones techniquement sécurisées

12. Les zones techniquement sécurisées sont des zones fixes ou temporaires expressément reconnues comme étant à protéger contre les attaques techniques et les écoutes. Ces zones font l'objet d'inspections physiques et techniques régulières et l'accès est strictement contrôlé. Les mesures ci-après sont mises en œuvre pour assurer la protection contre les attaques techniques et les écoutes :

(a) mise en œuvre d'un contrôle d'accès reposant sur des mesures de sécurité physique et technique adaptées au risque. La responsabilité de la détermination du risque est répartie entre les spécialistes techniques compétents et l'autorité de sécurité, qui donnent des avis au propriétaire du risque pour décision/approbation ;

(b) les zones techniquement sécurisées sont verrouillées et/ou gardées lorsqu'elles ne sont pas occupées, et toutes les clés associées à celles-ci sont considérées comme des clés de sécurité. Elles font l'objet d'inspections de sécurité physique et/ou technique à intervalles réguliers, conformément aux exigences de l'autorité de sécurité compétente. Ces inspections sont conduites après toute entrée non autorisée, effective ou présumée, ainsi qu'après tout accès de personnel extérieur (par exemple, pour des travaux d'entretien ou de décoration) ;

(c) aucun objet, meuble ou matériel ne peut être introduit dans ces zones avant d'avoir subi une inspection minutieuse, effectuée par du personnel de sécurité formé à cet effet et destinée à détecter les éventuels dispositifs d'écoute. Il y a lieu de tenir un registre des objets, meubles et matériels qui y entrent ou en sortent ;

(d) la présence de systèmes ou d'appareils électroniques dotés de fonctions d'enregistrement et/ou de transmission est interdite dans ces zones ;

(e) aucun poste téléphonique ni équipement de vidéoconférence n'est en principe présent dans ces zones. Toutefois, si leur présence ne peut pas être évitée, il convient de les débrancher physiquement lorsque des discussions traitant de sujets classifiées se tiennent dans ces zones. Cette disposition ne concerne pas les dispositifs de communication dûment homologués et installés.

MESURES DE SÉCURITÉ PHYSIQUE PARTICULIÈRES

13. Diverses mesures et procédures de sécurité physique et technique particulières peuvent contribuer au cadre de sécurité d'une organisation ou d'un site, notamment : périmètre de sécurité, système de détection des intrusions (IDS), contrôle d'accès, vidéosurveillance, éclairage de sécurité, armoires fortes et mobilier de bureau verrouillable, serrures de sécurité, contrôle des clés et des combinaisons, contrôle des visiteurs, fouilles à l'entrée et à la sortie. Pour des informations détaillées sur les procédures et mesures de sécurité physique et technique particulières, consulter la directive complémentaire sur la sécurité physique.

NORMES MINIMALES POUR LE STOCKAGE DES INFORMATIONS OTAN CLASSIFIÉES

14. Les informations OTAN classifiées sont conservées dans des zones, des armoires fortes ou du mobilier de bureau verrouillable permettant de décourager et de détecter tout accès non autorisé aux informations.

15. **COSMIC TRÈS SECRET (CTS).** Les informations classifiées CTS sont conservées dans une zone de sécurité de classe I ou II, de l'une des manières suivantes :

(a) dans une armoire forte approuvée, avec l'un des contrôles supplémentaires suivants :

(i) une protection continue par un garde ou un personnel de service habilité ;

(ii) l'inspection de l'armoire forte, à intervalles variables mais inférieurs à deux heures, par un garde ou un personnel de service habilité ;

(iii) un système de détection des intrusions (IDS) approuvé, associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour enlever ou ouvrir par effraction l'armoire forte ou neutraliser les mesures de sécurité en place ;

(b) une zone de rangement ouverte construite conformément aux dispositions énoncées dans la directive complémentaire sur la sécurité physique, équipée d'un IDS associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour forcer l'entrée ;

(c) une chambre forte équipée d'un IDS associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour forcer l'entrée.

16. **NATO SECRET (NS).** Les informations classifiées NS sont conservées dans une zone de sécurité de classe I ou II, de l'une des manières suivantes :

(a) de la même manière que celle prescrite pour les informations classifiées CTS ;

(b) dans une armoire ou une chambre forte approuvée, sans contrôles supplémentaires ;

(c) dans une zone de rangement ouverte, auquel cas l'un des contrôles supplémentaires ci-après est nécessaire :

(i) l'endroit où se trouve la zone de rangement ouverte fait l'objet d'une protection continue assurée par un garde ou un personnel de service habilité ;

(ii) un garde ou un personnel de service habilité inspecte la zone de rangement ouverte toutes les quatre heures au minimum ;

(iii) un IDS associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour forcer l'entrée.

17. **NATO CONFIDENTIEL (NC).** Les informations classifiées NC sont conservées dans une zone de sécurité de classe I ou II, dans une armoire forte approuvée.

18. **NATO DIFFUSION RESTREINTE (NDR).** Les informations classifiées NDR sont conservées dans un meuble fermé à clé (p. ex. tiroir) situé dans une zone administrative ou dans une zone de sécurité de classe I ou II. Ces mêmes informations peuvent également être conservées dans un meuble fermé à clé, une chambre forte ou une zone de rangement ouverte dont l'usage est approuvé pour des informations classifiées NC ou d'un niveau de classification supérieur.

19. Des précisions et des prescriptions supplémentaires pour la conservation des informations OTAN classifiées sont énoncées dans la directive complémentaire sur la sécurité physique.

PROTECTION PHYSIQUE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (SIC)

20. Les zones dans lesquelles des informations OTAN classifiées sont présentées ou manipulées par des moyens informatiques, ou dans lesquelles l'accès à de telles informations est possible, sont établies de façon que l'exigence globale de confidentialité, d'intégrité et de disponibilité soit satisfaite.

21. Les zones dans lesquelles des SIC sont utilisés pour afficher, stocker, traiter ou transmettre des informations classifiées NC ou d'un niveau de classification supérieur, ou dans lesquelles l'accès à de telles informations est virtuellement possible, sont déclarées zones de sécurité OTAN de classe I ou II, ou l'équivalent national. Les zones dans lesquelles des SIC sont utilisés pour afficher, stocker, traiter ou transmettre des informations classifiées NDR, ou dans lesquelles l'accès à de telles informations est virtuellement possible, sont déclarées zones administratives.

22. L'accès aux zones où sont hébergés ou gérés des composants SIC critiques fait l'objet d'un contrôle spécifique et est limité aux seules personnes autorisées appartenant aux services de sécurité ou aux services d'administration des systèmes, des réseaux ou des équipements cryptographiques.

PROTECTION CONTRE LES ATTAQUES TECHNIQUES

23. Les bureaux ou les zones dans lesquels se tiennent régulièrement des discussions faisant intervenir des informations classifiées NS ou d'un niveau de classification supérieur sont protégés contre les systèmes d'écoute passive et active, au moyen de mesures de sécurité physique et de contrôles d'accès appropriés, quand le risque le justifie. La question de savoir à qui incombe la responsabilité de déterminer le risque fait l'objet d'une coordination avec les spécialistes des questions techniques et est réglée par l'autorité de sécurité compétente. Pour des informations détaillées sur la protection contre les systèmes d'écoute passive et active, consulter la directive complémentaire sur la sécurité physique.

ÉQUIPEMENTS APPROUVÉS

24. Les pays de l'OTAN n'utilisent que des équipements approuvés, par une autorité de sécurité compétente, pour la protection des informations OTAN classifiées. Les organismes civils et militaires de l'OTAN s'assurent que tout équipement acheté a été préalablement approuvé par l'un des pays de l'OTAN pour une utilisation dans des conditions similaires. Ils peuvent également acheter des équipements dont l'utilisation a été approuvée par une autorité de sécurité compétente sur la base d'une évaluation des risques réalisée en vue de réduire ou d'atténuer un ou plusieurs risques identifiés.

PIÈCE JOINTE « E »

SÉCURITÉ DES INFORMATIONS OTAN CLASSIFIÉES

INTRODUCTION

1. La présente pièce jointe énonce la politique et les normes minimales pour la sécurité des informations OTAN classifiées. Des précisions et des prescriptions supplémentaires sont données dans la directive complémentaire sur la sécurité des informations OTAN classifiées (AC/35-D/2002).

2. La sécurité des informations consiste à appliquer des mesures et procédures de protection générale pour prévenir ou déceler la perte ou la compromission d'informations classifiées ou pour y remédier. Les informations classifiées font l'objet tout au long de leur cycle de vie d'une protection d'un niveau correspondant à leur classification de sécurité. Elles sont gérées de façon à être classifiées comme il convient, à être clairement identifiées comme étant classifiées et à ne rester classifiées qu'aussi longtemps qu'il le faut. La sécurité des informations est complétée par la sécurité concernant le personnel, la sécurité physique et la sécurité des SIC, afin d'offrir un ensemble équilibré de mesures pour la protection des informations OTAN classifiées.

CLASSIFICATIONS DE SÉCURITÉ OTAN, INDICATEURS DE CATÉGORIE SPÉCIALE, MARQUES ET PRINCIPES GÉNÉRAUX

3. Il incombe à l'originateur de déterminer la classification de sécurité et les modalités de la diffusion initiale des informations classifiées.

4. La classification de sécurité ne peut pas être modifiée, abaissée ou supprimée sans le consentement de l'originateur. Au moment de leur création, celui-ci indique, chaque fois que possible, si ses informations classifiées peuvent être déclassées ou déclassifiées à une certaine date ou à un moment déterminé.

5. La classification de sécurité attribuée aux informations détermine les mesures de sécurité physique et de sécurité des SIC qui leur sont associées lors de leur conservation, de leur transfert et de leur transmission, ainsi que les conditions de leur diffusion et de leur destruction et l'habilitation de sécurité (PSC) nécessaire pour y accéder. Une surclassification et une sous-classification sont donc toutes deux à éviter si l'on veut établir une sécurité effective et obtenir l'efficience voulue.

6. Des classifications de sécurité sont appliquées aux informations classifiées afin de donner une indication concernant les dommages que pourrait subir la sécurité de l'OTAN et/ou de ses pays membres si ces informations faisaient l'objet d'une communication non autorisée. Il appartient à l'originateur des informations classifiées de déterminer ou de modifier la classification de sécurité. Les classifications de sécurité OTAN sont énumérées ci-après, avec indication des cas auxquels elles s'appliquent :

(a) COSMIC TRÈS SECRET (CTS) – une communication non autorisée causerait un dommage d'une gravité exceptionnelle à l'OTAN ;

(b) NATO SECRET (NS) – une communication non autorisée causerait un dommage grave à l'OTAN ;

(c) NATO CONFIDENTIEL (NC) – une communication non autorisée serait dommageable pour l'OTAN ;

(d) NATO DIFFUSION RESTREINTE (NDR) – une communication non autorisée porterait préjudice aux intérêts ou à l'efficacité de l'OTAN.

7. Les classifications de sécurité de l'OTAN indiquent la sensibilité des informations OTAN classifiées. Elles sont utilisées pour appeler l'attention des destinataires sur la nécessité d'assurer une protection proportionnelle au dommage que causerait un accès ou une divulgation sans autorisation.

8. Les informations OTAN classifiées et les informations communicables au public sont protégées et manipulées conformément à la Politique de gestion de l'information OTAN (C-M(2007)0118) et au document intitulé « La gestion des informations OTAN non classifiées » (C-M(2002)60).

9. La planification, la préparation, l'exécution et le soutien d'activités de l'OTAN telles que les opérations, l'entraînement, les exercices, la transformation et la coopération (OTETC) peuvent nécessiter l'examen d'aspects supplémentaires relatifs à la sécurité. Le document complémentaire sur le partage des informations et du renseignement avec des entités non OTAN (NNE) contient des dispositions et des orientations de sécurité applicables dans ces circonstances.

10. Les pays et les organismes civils et militaires de l'OTAN prennent des mesures propres à garantir que les informations classifiées qui sont créées par l'OTAN ou qui lui sont fournies recevront la classification de sécurité correcte et seront protégées conformément aux prescriptions de la directive complémentaire sur la sécurité des informations OTAN classifiées.

11. Chaque organisme civil ou militaire de l'OTAN met en place un système propre à garantir que les informations CTS qui en émanent seront examinées au moins tous les cinq ans et les informations NS au moins tous les dix ans pour déterminer si la classification de sécurité se justifie toujours. Cet examen n'est pas indispensable dans le cas d'informations OTAN classifiées spécifiques pour lesquelles l'originateur a prévu une procédure de déclassement automatique à l'issue d'une période prédéfinie et qui portent des indications dans ce sens.

12. La classification de sécurité globale d'un document est au moins égale à celle de la partie ayant le niveau de classification le plus élevé. Les documents de couverture portent la classification de sécurité OTAN générale des informations classifiées auxquelles ils sont joints. Dans la mesure du possible, l'originateur doit attribuer une classification de sécurité adéquate aux différentes parties d'un document classifié NDR ou d'un niveau de classification supérieur (par exemple paragraphes, pièces jointes, annexes, etc.) afin de faciliter la décision concernant une diffusion ultérieure.

13. Lorsqu'un volume important d'informations OTAN classifiées sont compilées, il convient de conserver les marques de classification de sécurité initiales et d'évaluer la classification de ces informations compilées en fonction de l'impact que leur perte ou leur compromission aurait sur l'Organisation. Si cet impact est jugé globalement plus grave que celui correspondant à la classification de sécurité de chacun des documents compilés, il conviendra d'envisager de manipuler et de protéger ces informations à un niveau de classification supérieur, selon l'estimation de l'impact qu'aurait leur perte ou leur compromission.

Marques qualificatives

14. « COSMIC » et « NATO » sont des marques qualificatives qui, lorsqu'elles sont appliquées à des informations OTAN classifiées, signifient que ces informations doivent être protégées conformément à la politique de sécurité de l'OTAN.

Marques désignant une catégorie spéciale

15. « ATOMAL » est une marque appliquée à des informations de catégorie spéciale et signifiant que ces informations sont à protéger comme le prévoient l'Accord entre les États parties au Traité de l'Atlantique Nord relatif à la coopération dans le domaine des renseignements atomiques (C-M(64)39) et les Dispositions administratives complémentaires (C-M(68)41).

16. « US-SIOP » est une marque appliquée à des informations de catégorie spéciale et signifiant que ces informations sont à protéger comme le prévoient les « Procédures spéciales de protection au sein de l'OTAN des renseignements relatifs au plan opérationnel unique intégré des États-Unis (US-SIOP) (C-M(71)27(révisé) ».

17. « CRYPTO » est une marque désignant une catégorie spéciale et identifiant tous les matériels de chiffrement COMSEC utilisés pour protéger ou authentifier les télécommunications porteuses d'informations OTAN en rapport avec la sécurité cryptographique. Elle signifie que ces informations sont à protéger conformément aux politiques et directives appropriées concernant la sécurité cryptographique.

18. « BOHEMIA » est une marque appliquée à des informations de catégorie spéciale provenant ou relevant du renseignement transmissions (COMINT). Toutes les informations portant la marque COSMIC TRÈS SECRET-BOHEMIA seront protégées dans le strict respect du MC 101 (Politique de l'OTAN en matière de renseignement d'origine électromagnétique), de la publication interalliée interarmées (AJP) qui s'y rapporte et qui concerne la doctrine, et du guide du NACSI pour l'administration et les procédures ROEM.

Marques de limitation de la diffusion

19. Pour limiter encore la diffusion d'informations OTAN classifiées, une marque supplémentaire de limitation de la diffusion peut être appliquée par l'originateur.

CONTRÔLE ET MANIPULATION

Objectifs de la comptabilisation

20. L'objectif principal de la comptabilisation est l'obtention de données suffisantes pour permettre d'enquêter sur une perte ou une compromission volontaire ou accidentelle d'informations comptabilisables, ainsi que d'évaluer les dommages en résultant. L'obligation de comptabilisation sert à imposer une discipline pour la manipulation des informations comptabilisables et le contrôle de l'accès à ces informations.

21. Les objectifs secondaires sont les suivants :

(a) permettre de suivre les accès aux informations comptabilisables (qui a eu ou a pu avoir accès à des informations comptabilisables ; qui a tenté d'avoir accès à des informations comptabilisables) ;

(b) permettre de localiser les informations comptabilisables ;

(c) permettre de suivre le mouvement des informations comptabilisables à l'intérieur des domaines OTAN et nationaux ;

(d) permettre d'enregistrer les informations comptabilisables qui ont été communiquées aux NNE.

22. Les informations classifiées CTS, NS et ATOMAL sont comptabilisables et elles sont contrôlées et manipulées conformément aux prescriptions de la présente pièce jointe et de la directive complémentaire sur la sécurité des informations OTAN classifiées. Lorsque les lois et règlements nationaux l'exigent, des informations portant d'autres marques de classification ou de catégorie spéciale peuvent être considérées comme des informations comptabilisables.

Le système de bureaux d'ordre

23. Les procédures de sécurité et les prescriptions du système de bureaux d'ordre s'appliquent de la même manière dans les domaines physique et électronique. Des précisions et prescriptions supplémentaires concernant le domaine électronique figurent dans la pièce jointe « F » au présent document et dans ses directives complémentaires.

24. Il doit exister un système de bureaux d'ordre responsable de la réception, de la comptabilisation, de la manipulation, de la diffusion et de la destruction des informations comptabilisables. Une telle responsabilité peut être exercée soit au sein d'un système de bureaux d'ordre unique, auquel cas un strict compartimentage des informations classifiées CTS et des informations de catégorie spéciale est maintenu en permanence, soit par des bureaux d'ordre et des points de contrôle séparés.

25. Chaque pays ou organisme civil ou militaire de l'OTAN, selon le cas, établit un bureau d'ordre central pour les informations classifiées CTS, qui fait fonction de principale autorité responsable de la réception et de l'expédition pour le pays ou l'organisme dans lequel il a été établi ; Le ou les bureaux d'ordre centraux peuvent également remplir ces fonctions pour d'autres informations comptabilisables.

26. Les bureaux d'ordre et les points de contrôle sont responsables de la distribution interne des informations classifiées CTS et NS et de la tenue de registres pour tous les documents comptabilisables dont ils ont la charge ; ils peuvent être établis au niveau d'un ministère, d'un département ou d'un commandement. Les informations NC et NDR n'ont pas à passer par le système de bureaux d'ordre, sauf spécification contraire dans les lois et règlements nationaux.

27. En ce qui concerne les informations OTAN comptabilisables, les bureaux d'ordre et les points de contrôle doivent être à même à tout moment de déterminer où elles se trouvent. Un accès peu fréquent et temporaire à de telles informations n'entraîne pas nécessairement l'obligation d'établir un bureau d'ordre ou un point de contrôle, pourvu que des procédures soient en place pour faire en sorte que les informations restent sous le contrôle du système de bureaux d'ordre.

28. La diffusion des informations classifiées CTS s'opère par la voie des bureaux d'ordre COSMIC. Une fois par an au moins, chaque bureau d'ordre établit un inventaire de toutes les informations classifiées CTS dont il est comptable, conformément aux prescriptions de la directive complémentaire sur la sécurité des informations OTAN classifiées. Quel que soit le type d'organisation des bureaux d'ordre, ceux qui manipulent des informations classifiées CTS nomment un « responsable du contrôle COSMIC » (CCO).

29. La directive complémentaire sur la sécurité des informations OTAN classifiées décrit, entre autres, les responsabilités du CCO, les processus détaillés de manipulation des informations classifiées CTS et NS par le système de bureaux d'ordre, la procédure à suivre pour les reproductions, les traductions et les extraits, les exigences concernant la diffusion et le transfert, et celles relatives à l'élimination et à la destruction des informations OTAN classifiées.

30. Le Comité militaire a établi un système séparé pour la comptabilisation, le contrôle et la diffusion des matériels cryptographiques. Les matériels transférés par ce système ne doivent pas être comptabilisés par le système de bureaux d'ordre.

PLANS DE CIRCONSTANCE

31. Les pays et les organismes civils et militaires de l'OTAN établissent des plans de circonstance pour la protection ou la destruction, dans des situations d'urgence, des informations OTAN classifiées, afin d'éviter tout accès non autorisé à ces informations et la divulgation de celles-ci, ainsi que toute perte de disponibilité. Ces plans se basent sur des évaluations de la menace revues de façon périodique et donnent la plus haute priorité aux informations les plus sensibles et à celles qui sont les plus importantes pour l'exécution d'une mission ou pour lesquelles le facteur temps est déterminant.

INCIDENTS DE SÉCURITÉ

32. Un incident de sécurité est un événement ou tout autre fait qui est susceptible de porter atteinte à la sécurité des informations OTAN classifiées et qui requiert un complément d'enquête pour établir avec précision s'il constitue une violation ou une infraction de sécurité.

Violation de sécurité

33. Une violation de sécurité est un acte ou une omission, à caractère délibéré ou accidentel, contraire aux règles de sécurité énoncées dans la présente politique, qui peut entraîner la compromission effective ou possible d'informations OTAN classifiées ou de services et ressources connexes.

Compromission

34. Il y a compromission lorsqu'à la suite d'une violation de sécurité ou d'une activité à caractère hostile, des informations OTAN classifiées ont perdu leur confidentialité, leur intégrité ou leur disponibilité, ou les services et ressources connexes ont perdu leur intégrité ou leur disponibilité. Cela inclut la perte, la communication à des personnes non autorisées, la modification non autorisée, la destruction d'une manière non autorisée, et le déni de service.

Infraction

35. Une infraction est un acte ou une omission, à caractère délibéré ou accidentel, contraire aux règles de sécurité énoncées dans la présente politique, qui ne donne pas lieu à une compromission effective ou possible d'informations OTAN classifiées.

36. Toute violation de sécurité, réelle ou potentielle, est immédiatement signalée à l'autorité de sécurité compétente. Chaque violation signalée fait l'objet d'une enquête menée par des personnes possédant l'expérience nécessaire en matière de sécurité, d'investigation et, s'il y a lieu, de contre-ingérence, et qui sont indépendantes de celles qui sont directement concernées par la violation. Pour plus de précisions sur les mesures à prendre en cas de découverte d'une violation

de sécurité ou d'une infraction, consulter la directive complémentaire sur la sécurité des informations OTAN classifiées.

SIGNALEMENT

37. Le but essentiel du signalement des violations de sécurité et des compromissions d'informations OTAN classifiées est de permettre au service de l'OTAN qui est à l'origine des informations d'évaluer les dommages qui en résultent pour l'OTAN et de prendre toute mesure souhaitable ou réalisable pour les atténuer. Des rapports sur l'évaluation des dommages et sur les mesures prises pour les atténuer sont transmis au NOS par l'ANS/ASD ou le chef de l'organisme civil ou militaire de l'OTAN concerné.

38. Si possible, l'autorité dont émane le rapport informe le service de l'OTAN qui est à l'origine des informations, en même temps que le NOS, mais elle peut demander à ce dernier de s'en charger lorsque l'auteur est difficile à identifier. Le moment où les rapports doivent être transmis au NOS dépend de la sensibilité des informations en cause et des circonstances.

39. Le NOS peut, au nom du secrétaire général de l'OTAN, demander aux autorités compétentes de mener une enquête supplémentaire et de lui rendre compte de ses conclusions. En fonction des circonstances et de la gravité de la compromission, le NOS peut en informer le Comité de sécurité.

40. La directive complémentaire sur la sécurité des informations OTAN classifiées décrit en détail les mesures à prendre, les registres à tenir et les informations à fournir en cas de violations de sécurité et de compromissions.

41. Les dispositions relatives à la compromission de matériels cryptographiques ont été communiquées séparément par le Comité militaire aux autorités de sécurité des télécommunications des pays et des organismes civils et militaires de l'OTAN.

PIÈCE JOINTE « F »

SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

1. INTRODUCTION

1.1 La présente pièce jointe énonce la politique et les normes minimales à appliquer pour la protection des informations OTAN classifiées et des services et ressources système connexes[1] dans les systèmes d'information et de communication et autres systèmes électroniques qui stockent, traitent ou transmettent des informations OTAN classifiées.

1.2 La présente pièce jointe complète la politique de gestion de l'information OTAN ainsi que la politique relative à la gestion des informations OTAN non classifiées, qui fixe les principes de base et les règles à appliquer dans les organismes civils et militaires de l'OTAN et dans les pays membres de l'OTAN pour la protection des informations OTAN non classifiées.

1.3 La sécurité des systèmes d'information et de communication (sécurité des SIC) est l'une des composantes de l'assurance de l'information (voir figure 1) qui se définit comme l'application de mesures de sécurité pour la protection des systèmes de communication et d'information et d'autres systèmes électroniques[2] ainsi que des informations stockées dans ces systèmes ou traitées ou transmises au moyen de ceux-ci[3], pour ce qui est de leur confidentialité, de leur intégrité, de leur disponibilité, de leur authentification et de leur non-répudiation.

1.4 Pour atteindre les objectifs de sécurité que sont la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation[4] des informations classifiées manipulées par ces SIC, il convient d'appliquer un ensemble équilibré de mesures de sécurité (relevant de la sécurité physique, de la sécurité concernant le personnel, de la sécurité des informations et de la sécurité des SIC), afin de créer un environnement sûr pour l'exploitation d'un SIC. Lorsque des informations classifiées sont manipulées par l'industrie dans le cadre de contrats, des mesures spécifiques supplémentaires de sécurité industrielle sont appliquées conformément à la pièce jointe « G » au présent C-M et à la directive complémentaire sur la sécurité industrielle.

---

1 Services et ressources système connexes - services et ressources nécessaires pour faire en sorte que les objectifs de sécurité des SIC soient atteints ; cela comprend, par exemple, les produits et mécanismes cryptographiques, les matériels COMSEC, les services d'annuaire, et les installations et contrôles environnementaux.

2 Dénommés « SIC » dans la présente pièce jointe.

3 Le verbe « manipuler » est utilisé à cet effet dans la présente pièce jointe.

4 Dénommés « objectifs de sécurité » dans la présente pièce jointe.

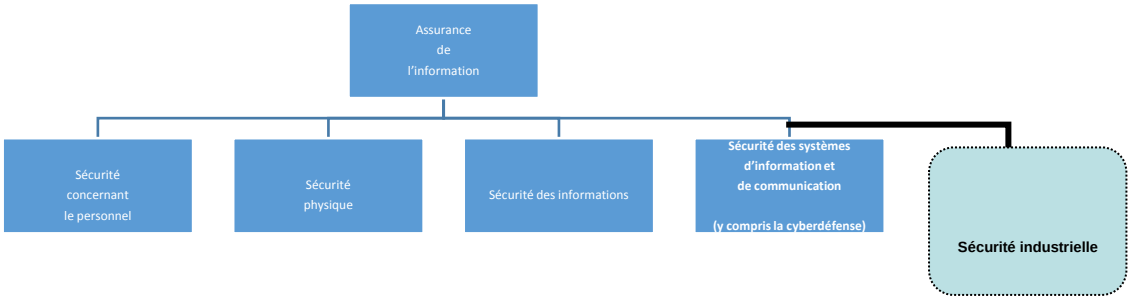

Figure 1 – Liens entre l'assurance de l'information et la sécurité des SIC

1.5 Les activités relevant de la sécurité des SIC à mener pendant le cycle de vie des SIC et les responsabilités des comités ainsi que des organismes civils et militaires de l'OTAN en matière de sécurité des SIC sont décrites dans la « Directive principale concernant la sécurité des SIC », qui est publiée par le Comité de sécurité et le C3B à l'appui de la présente politique. La « Directive principale concernant la sécurité des SIC » est complétée par des directives portant sur la gestion de la sécurité des SIC (y compris la gestion des risques de sécurité, l'homologation de sécurité, la documentation relative à la sécurité et l'examen/l'inspection de sécurité) et sur les aspects techniques et de la mise en œuvre de la sécurité des SIC (y compris la sécurité des ordinateurs et des réseaux locaux (LAN), la sécurité de l'interconnexion de réseaux, la sécurité cryptographique, la sécurité des transmissions et la sécurité des émissions).

2. OBJECTIFS DE SÉCURITÉ

2.1 Afin d'assurer une protection adéquate des informations OTAN classifiées manipulées dans des SIC, un ensemble équilibré de mesures de sécurité (relevant de la sécurité physique, de la sécurité concernant le personnel, de la sécurité des informations et de la sécurité des SIC) est établi et mis en œuvre, de manière à créer un environnement sûr pour le fonctionnement des SIC et à répondre aux objectifs de sécurité suivants :

(a) maintien de la confidentialité des informations par le contrôle de la communication d'informations OTAN classifiées ainsi que des services et ressources système connexes, et par le contrôle de l'accès dont ils font l'objet ;

(b) maintien de l'intégrité des informations OTAN classifiées ainsi que des services et ressources système connexes ;

(c) maintien de la disponibilité des informations OTAN classifiées ainsi que des services et ressources système connexes ;

(d) maintien de moyens d'identifier et d'authentifier de manière sûre les personnes, les dispositifs et les services qui ont accès à des SIC manipulant des informations OTAN classifiées ;

(e) maintien de mesures appropriées de non-répudiation des personnes et des entités ayant traité les informations.

2.2 Les informations OTAN classifiées ainsi que les services et ressources système connexes sont protégés par un ensemble minimum de mesures visant à assurer une protection générale contre les problèmes couramment rencontrés (qu'ils soient d'origine accidentelle ou délibérément provoqués) et connus comme affectant tous les systèmes ainsi que tous les services et ressources système connexes. Des mesures supplémentaires adaptées aux circonstances sont prises lorsqu'une évaluation des risques de sécurité a montré que des informations OTAN classifiées et/ou

des services et ressources système connexes sont exposés à des risques accrus découlant de menaces et de vulnérabilités spécifiques.

2.3 Quelle que soit la classification de sécurité des informations OTAN qui sont manipulées, les autorités de sécurité de l'OTAN évaluent les risques et l'ampleur des dommages pour l'OTAN si les mesures destinées à atteindre les objectifs de sécurité autres que celui de confidentialité échouent. L'ensemble minimum de ces mesures relatives aux services non liés à la confidentialité est déterminé conformément aux directives à l'appui de la présente politique.

3. HOMOLOGATION DE SÉCURITÉ

3.1 Lors de la définition des impératifs de sécurité, on détermine la mesure dans laquelle les objectifs de sécurité doivent être atteints et le degré de confiance qui peut être accordé aux mesures de sécurité des SIC pour la protection des informations OTAN classifiées ainsi que des services et ressources système connexes. Le processus d'homologation de sécurité assure qu'un niveau de protection suffisant a été atteint et qu'il est maintenu.

3.2 Tous les SIC manipulant des informations OTAN classifiées sont soumis à un processus d'homologation de sécurité axé sur les objectifs de sécurité.

4. SÉCURITÉ CONCERNANT LE PERSONNEL

4.1 Les personnes autorisées à accéder aux informations OTAN classifiées, quelle qu'en soit la forme, doivent être habilitées, le cas échéant, en fonction de leur responsabilité globale pour ce qui est d'atteindre les objectifs de sécurité des informations ainsi que des services et ressources système connexes. Cela inclut les personnes qui ont reçu l'accès aux services et ressources système connexes ou qui sont responsables de leur protection, même si elles ne sont pas autorisées à accéder aux informations manipulées par le système.

5. SÉCURITÉ PHYSIQUE

5.1 Les zones dans lesquelles des informations OTAN classifiées sont présentées ou manipulées par des moyens informatiques, ou dans lesquelles l'accès à de telles informations est possible, sont établies de telle façon que l'exigence globale des objectifs de sécurité soit satisfaite.

6. SÉCURITÉ DES INFORMATIONS

6.1 Tous les supports de mémoire d'ordinateur classifiés doivent être dûment identifiés, conservés et protégés d'une manière compatible avec le plus haut niveau de classification des informations stockées.

6.2 Les informations OTAN classifiées enregistrées sur des supports de mémoire d'ordinateur réutilisables ne sont effacées que selon les procédures approuvées par l'autorité de sécurité compétente.

6.3 Les mesures de sécurité approuvées (liées ou non à la confidentialité), mises en œuvre conformément aux directives à l'appui de la présente politique, peuvent servir à protéger des informations OTAN classifiées sur des supports de mémoire d'ordinateur, de manière à assouplir les exigences de sécurité physique lorsque le niveau de classification est moins élevé.

7. SÉCURITÉ INDUSTRIELLE

7.1 Les installations d'un contractant qui sont utilisées dans le cadre de contrats et dans lesquelles des informations OTAN classifiées sont manipulées sur des SIC sont établies de telle façon que l'exigence globale des objectifs de sécurité soit satisfaite.

7.2 Un ensemble cohérent de mesures de sécurité des SIC est décrit dans les contrats, les avenants « sécurité » (SAL) et/ou les instructions de sécurité applicables aux projets (PSI) et/ou les accords sur les niveaux de service (SLA), selon les cas, et est mis en place par les contractants pour atteindre les objectifs de sécurité des SIC de l'OTAN et pour protéger les informations OTAN classifiées ainsi que les services connexes.

8. MESURES DE SÉCURITÉ

8.1 Pour tous les SIC manipulant des informations OTAN classifiées, un ensemble cohérent de mesures de sécurité est mis en place pour atteindre les objectifs de sécurité, de manière à protéger les informations ainsi que les services et ressources système connexes. Les mesures de sécurité comprennent, le cas échéant :

(a) un moyen d'obtenir des données suffisantes pour pouvoir enquêter sur une compromission volontaire ou accidentelle ou sur une tentative de compromission des objectifs de sécurité d'informations classifiées ainsi que de services et ressources système connexes, en fonction des dommages qui seraient occasionnés ;

(b) un moyen d'identifier et d'authentifier de manière sûre les personnes, les dispositifs et les services autorisées à avoir accès à un SIC. Les informations et le matériel servant à contrôler l'accès à un SIC sont eux-mêmes contrôlés et protégés par des dispositifs adaptés aux informations auxquelles l'accès peut être donné. Sur les SIC de l'OTAN, des mécanismes d'authentification forte des personnes sont employés ;

(c) un moyen de contrôler la communication d'informations OTAN classifiées et l'accès à celles-ci ainsi qu'aux services et ressources système connexes, sur la base du principe du besoin d'en connaître ;

(d) un moyen de vérifier l'intégrité et l'origine des informations OTAN classifiées ainsi que des services et ressources système connexes ;

(e) un moyen de maintenir l'intégrité des informations OTAN classifiées ainsi que des services et ressources système connexes ;

(f) un moyen de maintenir la disponibilité des informations OTAN classifiées ainsi que des services et ressources système connexes ;

(g) un moyen de contrôler le raccordement des SIC qui manipulent des informations OTAN classifiées ;

(h) une mesure de la confiance qui peut être placée dans les mécanismes de protection de la sécurité des SIC ;

(i) un moyen d'évaluer et de vérifier le bon fonctionnement des mécanismes de protection de la sécurité des SIC pendant le cycle de vie du SIC ;

(j) un moyen d'enquêter sur les activités des utilisateurs et des SIC *;*

(k) un moyen de donner des assurances de non-répudiation, de sorte que l'expéditeur d'informations reçoive la preuve de la transmission de celles-ci et que le destinataire reçoive la preuve de l'identité de l'expéditeur ;

(l) un moyen de protéger des informations OTAN classifiées stockées, lorsque les mesures de sécurité physique ne respectent pas les normes minimales.

8.2 Des mécanismes et procédures de gestion de la sécurité sont mis en place pour décourager, prévenir et détecter les incidents, pour y résister ainsi que pour assurer la reprise après des incidents mettant en cause les objectifs de sécurité d'informations OTAN classifiées ainsi que de services et ressources système connexes, y compris pour l'établissement de rapports sur les incidents de sécurité.

8.3 Les mesures de sécurité sont gérées et mises en œuvre conformément aux directives à l'appui de la présente politique.

9. GESTION DES RISQUES DE SÉCURITÉ

9.1 Les SIC manipulant des informations OTAN classifiées dans les organismes civils et militaires de l'OTAN font l'objet d'une gestion des risques de sécurité, qui comprend une évaluation de ces risques, conformément aux prescriptions des directives à l'appui de la présente politique.

9.2 La gestion des risques de sécurité des SIC de l'OTAN assure une évaluation continue des vulnérabilités des systèmes et du respect des dispositions de sécurité, et s'oriente vers une gestion dynamique des risques devant permettre de faire face de manière efficace aux défis que représentent à notre époque les scénarios opérationnels complexes et les environnements de la menace aux aspects multiples.

10. TRANSMISSION ÉLECTROMAGNÉTIQUE[5] D'INFORMATIONS OTAN CLASSIFIÉES

10.1 Lors de la transmission électromagnétique d'informations OTAN classifiées, des mesures spéciales sont prises afin que les objectifs de sécurité soient atteints. Les autorités de l'OTAN déterminent les besoins concernant la protection des transmissions contre la détection, l'interception ou l'exploitation.

11. SÉCURITÉ CRYPTOGRAPHIQUE

11.1 Lorsque des produits ou mécanismes cryptographiques doivent être utilisés pour assurer une protection des informations liée ou non à leur confidentialité, que ce soit pendant leur transmission, leur traitement ou leur stockage (données au repos), ces produits ou mécanismes sont expressément approuvés à cet effet et des mesures physiques, procédurales et techniques en matière de chiffrement doivent être spécialement appliquées afin que les objectifs de sécurité voulus soient atteints.

11.2 Les données au repos sont protégées à un niveau compatible avec les objectifs de sécurité à atteindre et, lorsque des produits et mécanismes cryptographiques sont utilisés, les exigences liées à la sécurité cryptographique sont conformes aux directives pertinentes de l'OTAN sur les aspects techniques et la mise en œuvre de l'INFOSEC.

[5] L'expression « transmission électromagnétique » couvre les transmissions qui ont des caractéristiques ou des propriétés électriques et magnétiques, comprenant, entre autres, la lumière visible, les ondes radioélectriques, les hyperfréquences et le rayonnement infrarouge.

11.3 Pendant la transmission, la confidentialité des informations classifiées NATO SECRET (NS) ou d'un niveau de classification supérieur est protégée par des produits ou mécanismes cryptographiques approuvés par le Comité militaire de l'OTAN (NAMILCOM).

11.4 Pendant la transmission, la confidentialité des informations classifiées NATO CONFIDENTIEL (NC) ou NATO DIFFUSION RESTREINTE (NDR) est protégée par des produits ou mécanismes cryptographiques approuvés par le NAMILCOM ou par un pays membre de l'OTAN.

11.5 Pendant la transmission, les exigences de protection non liées à la confidentialité sont remplies conformément au besoin opérationnel du système de communication. S'agissant des mécanismes cryptographiques non liés à la confidentialité, les besoins en matière d'évaluation et l'autorité d'approbation sont déterminés et agréés en même temps que la spécification de ces mécanismes dans l'énoncé du besoin opérationnel, comme convenu dans les directives techniques.

11.6 Dans certaines circonstances opérationnelles exceptionnelles, des informations classifiées NC et NS peuvent être transmises en clair pour autant que chaque cas soit dûment signalé aux autorités supérieures. Ces circonstances exceptionnelles sont les suivantes :

(a) lors de crises, de conflits ou de situations de guerre effectifs ou imminents ;

(b) lorsque la rapidité de la transmission est d'une importance primordiale, que l'on ne dispose pas de moyens de chiffrement et que l'on estime que les informations transmises ne peuvent pas être exploitées assez rapidement pour que cela ait un effet négatif sur les opérations.

11.7 Dans certaines circonstances opérationnelles exceptionnelles, lorsque la rapidité est d'une importance primordiale, que l'on ne dispose pas de moyens de chiffrement et que l'on estime que les informations transmises ne peuvent pas être exploitées assez rapidement pour que cela ait un effet négatif sur les opérations, des informations classifiées NDR peuvent être transmises en clair.

11.8 Au cours de transmissions entre SIC OTAN et SIC de pays non membres de l'OTAN ou d'organisations internationales (NNN/IO), la confidentialité des informations classifiées NS ou d'un niveau de classification supérieur est protégée par des produits ou mécanismes cryptographiques approuvés par le NAMILCOM.

11.9 Au cours de transmissions au sein de SIC NNN/IO, la confidentialité des informations classifiées NS ou d'un niveau de classification supérieur est protégée par des produits ou mécanismes cryptographiques approuvés par le NAMILCOM.

11.10 Lorsque les prescriptions des paragraphes 11.8 et 11.9 ne peuvent pas être respectées, l'OTAN et une organisation internationale peuvent se mettre d'accord sur l'acceptation mutuelle de leurs processus respectifs d'évaluation, de sélection et d'approbation des produits ou mécanismes cryptographiques autorisés pour la protection, pendant leur transmission, des informations NS ou des informations de l'organisation internationale du niveau de classification équivalent. Les conditions relatives à cette acceptation sont énoncées plus loin au paragraphe 11.12.

11.11 Dans des circonstances exceptionnelles, afin de pouvoir répondre à des besoins opérationnels spécifiques, et lorsque les prescriptions des paragraphes 11.8 et 11.9 ne peuvent pas être respectées, l'OTAN peut approuver les processus d'évaluation, de sélection et d'approbation d'un pays non OTAN (NNN) relatifs aux produits ou mécanismes cryptographiques autorisés pour la protection, pendant leur transmission, des informations NS ou des informations du NNN du niveau

de classification équivalent. Les conditions relatives à cette approbation sont énoncées plus loin au paragraphe 11.12.

11.12 Les conditions suivantes s'appliquent dans le cadre des scénarios décrits plus haut aux paragraphes 11.10 et 11.11 :

(a) le NNN/IO a conclu un Accord de sécurité avec l'OTAN et a reçu du Bureau de sécurité de l'OTAN (NOS) une certification de son aptitude à protéger de manière appropriée les informations OTAN classifiées communiquées ;

(b) chaque NNN/IO est considéré cas par cas et le fondement de toute acceptation/approbation est exposé dans les dispositions de sécurité à l'appui de l'Accord de sécurité entre l'OTAN et le NNN/IO ;

(c) les dispositions de toute acceptation/approbation de ce type sont approuvées par le NAMILCOM sur la base d'une évaluation objective menée par le NOS, en collaboration avec le Bureau de sécurité et d'évaluation des systèmes de communication et d'information (SECAN) du NAMILCOM, la Commission capacitaire Assurance de l'information et cyberdéfense du C3B et le Secrétariat des C3 du siège de l'OTAN, et portant sur l'aptitude du NNN/IO à réaliser des évaluations cryptographiques qui répondent à des exigences équivalentes à celles imposées à l'OTAN pour la protection cryptographique des informations NS ;

(d) le NOS, conjointement avec le SECAN et le Secrétariat des C3 du siège de l'OTAN, s'assure, au moyen d'une vérification et de vérifications ultérieures périodiques, que le NNN/IO a mis en place des structures, règles et procédures appropriées pour l'évaluation, la sélection, l'approbation et le contrôle des produits et mécanismes cryptographiques, et que ces structures, règles et procédures sont mises en application efficacement et en toute sécurité.

11.13 Lorsqu'une acceptation/approbation intervient selon les conditions énoncées plus haut au paragraphe 11.12, la confidentialité des informations classifiées NS peut être protégée par des produits ou mécanismes cryptographiques approuvés par le NAMILCOM ou par des produits ou mécanismes cryptographiques approuvés par la NCSA (ou l'autorité équivalente) du NNN/IO pour la protection d'informations d'un niveau de classification équivalent.

11.14 Au cours de transmissions entre SIC OTAN et SIC NNN/IO et au sein de SIC NNN/IO, la confidentialité des informations classifiées NC ou NDR est protégée par des produits ou mécanismes cryptographiques évalués et approuvés par une autorité compétente. L'autorité compétente peut être le NAMILCOM, la NCSA d'un pays membre de l'OTAN ou l'autorité équivalente du NNN/IO, à condition que celui-ci ait mis en place des structures, règles et procédures appropriées pour l'évaluation, la sélection, l'approbation et le contrôle de ces produits ou mécanismes, et que ces structures, règles et procédures soient mises en application efficacement et en toute sécurité. Ces structures, règles et procédures font l'objet d'un accord entre le NAMILCOM et le NNN/IO.

11.15 Le caractère sensible du matériel cryptographique utilisé pour protéger les informations OTAN classifiées rend nécessaire l'application de mesures de sécurité spéciales en plus de celles qu'exige la protection des autres informations OTAN classifiées.

11.16 La protection qui est assurée au matériel cryptographique est fonction du dommage qui pourrait être causé en cas d'échec de cette protection. Il faut disposer de moyens sûrs pour évaluer et vérifier la protection et le bon fonctionnement des produits et mécanismes cryptographiques, ainsi

que la protection et le contrôle des informations cryptographiques (p.ex. des modalités détaillées d'application et la documentation qui y est associée).

11.17 Étant donné le caractère particulièrement sensible des informations cryptographiques, il doit y avoir au sein de l'OTAN et dans chaque pays membre un organisme spécial et une réglementation spéciale régissant la réception et le contrôle des informations cryptographiques OTAN ainsi que leur transmission à des personnes ayant fait l'objet d'une certification spéciale.

11.18 Des procédures spéciales sont également suivies pour le partage d'informations techniques ainsi que pour le choix, la production et l'acquisition de produits et mécanismes cryptographiques.

12. SÉCURITÉ DES ÉMISSIONS

12.1 Des mesures de sécurité sont prises pour empêcher la compromission d'informations classifiées NC ou d'un niveau de classification supérieur par des émissions électromagnétiques non voulues. La nature de ces mesures est fonction du risque d'exploitation et de la sensibilité des informations.

13. RESPONSABILITÉS SPÉCIFIQUES EN MATIÈRE DE SÉCURITÉ DES SIC

13.1 Comité militaire de l'OTAN (NAMILCOM)

13.1.1 Les responsabilités du NAMILCOM en matière de sécurité des SIC comprennent l'approbation de sécurité et la délivrance du matériel cryptographique ainsi que la participation à l'évaluation et à la sélection des produits et mécanismes cryptographiques destinés à une utilisation courante par l'OTAN. Les quatre agences du NAMILCOM dotées en personnel par les pays (SECAN, DACAN, EUSEC et EUDAC) lui donnent des avis et lui apportent leur soutien en matière de sécurité des SIC, ainsi qu'au Comité de sécurité, au C3B et, le cas échéant, à leurs structures subordonnées, aux pays membres et à d'autres organismes de l'OTAN.

13.2 Bureau des C3 (C3B)

13.2.1 En tant que comité directeur de haut niveau dans le domaine des C3 au sein de l'OTAN, le C3B appuie le NAMILCOM et les autorités politiques de l'OTAN au cours du processus de validation des projets et capacités C3 en examinant les besoins opérationnels en matière de C3. Le C3B est chargé de la fourniture de systèmes C3 sécurisés et interopérables à l'échelle de l'OTAN. Le Secrétariat des C3 du siège de l'OTAN (NHQC3S) assure le soutien administratif du C3B.

13.3 Bureau de gestion de la cyberdéfense (CDMB) de l'OTAN

13.3.1 Le CDMB est l'organisme de coordination en matière de cyberdéfense qui établit des plans et des directives stratégiques pour la mise en œuvre de la politique de cyberdéfense et qui facilite la coopération avec les Alliés. Il fait rapport au Conseil de l'Atlantique Nord et reçoit de celui-ci des orientations politiques, via le Comité de la politique et des plans de défense en configuration renforcée (DPPC(R)). Il est supervisé par les Alliés par l'intermédiaire du C3B pour les orientations relatives aux C3 et les aspects liés à la mise en œuvre de la cyberdéfense. Il consulte des experts sur des sujets spécifiques par l'intermédiaire des comités OTAN compétents.

13.4 Autorité nationale de sécurité des SIC (NCSA)

13.4.1 Les pays membres de l'OTAN et, le cas échéant, les pays non OTAN désignent chacun une NCSA, qui peut être mise en place sous la forme d'un organisme faisant partie de la structure nationale des services de sécurité. La NCSA est chargée :

(a) de contrôler les informations techniques cryptographiques se rapportant à la protection des informations OTAN dans le pays ;

(b) de s'assurer que les systèmes, produits et mécanismes cryptographiques destinés à protéger les informations OTAN sont choisis, utilisés et entretenus de manière appropriée ;

(c) de s'assurer que les produits de sécurité des SIC destinés à protéger les informations OTAN sont choisis, utilisés et entretenus de manière appropriée dans le pays ;

(d) d'échanger des informations avec les organismes OTAN et nationaux compétents sur les questions techniques et de sécurité des communications de l'OTAN liées à la sécurité des SIC, dans les domaines civil et militaire ;

(e) de désigner s'il y a lieu une autorité nationale TEMPEST.

13.4.2 Les NCSA travaillent en coordination avec leur(s) ANS.

13.5 Autorité nationale de distribution (NDA)

13.5.1 Les pays membres de l'OTAN et, le cas échéant, les pays non membres désignent chacun une NDA, qui peut être mise en place sous la forme d'un organisme faisant partie de la structure nationale des services de sécurité et qui est responsable de la gestion du matériel cryptographique de l'OTAN à l'échelon national et s'assure que des procédures appropriées sont appliquées et des filières établies pour que l'ensemble du matériel cryptographique fasse l'objet d'une comptabilisation complète et soit manipulé, conservé, distribué et détruit dans des conditions de sécurité.

13.5.2 Les NDA travaillent en coordination avec leur(s) ANS.

13.6 Autorité(s) d'homologation de sécurité

13.6.1 Les pays membres de l'OTAN et, le cas échéant, les pays non membres désignent chacun une ou plusieurs autorité(s) d'homologation de sécurité responsable(s) de l'homologation, sur le plan de la sécurité, des systèmes suivants :

(a) SIC nationaux qui manipulent des informations OTAN classifiées ;

(b) SIC de l'OTAN qui fonctionnent au sein d'organisations/organismes nationaux, le cas échéant, dans des pays non membres de l'OTAN.

13.6.2 Lorsqu'un organisme civil ou militaire de l'OTAN est établi dans un pays de l'OTAN, les SIC de l'OTAN sont soumis à l'homologation de sécurité d'une SAA de l'OTAN. Dans ce cas, l'homologation de sécurité peut être donnée en coordination avec l'autorité d'homologation de sécurité nationale compétente.

13.7 Autorité d'homologation de sécurité de l'OTAN (SAA)

13.7.1 À l'OTAN, il y a trois SAA chargées de l'homologation de sécurité des SIC de l'OTAN qui manipulent des informations OTAN classifiées. La fonction de SAA est exercée par le directeur du Bureau de sécurité de l'OTAN et les commandants stratégiques, ou par leur(s) représentant(s) délégué(s)/désigné(s) à cet effet, en fonction du SIC à homologuer.

13.7.2 Le Bureau d'homologation de sécurité des SIC de l'OTAN (NSAB), composé des SAA de l'OTAN indiquées au paragraphe qui précède, supervise l'homologation de sécurité de tous les SIC de l'OTAN qui manipulent des informations OTAN classifiées, de manière à garantir une approche globale et cohérente de la sécurité des SIC de l'OTAN. Le mandat du NSAB est soumis à l'approbation du Comité de sécurité.

13.8 Autorité de sécurité des pays non OTAN (NNN)

13.8.1 Les NNN désignent une autorité de sécurité chargée des dispositions de sécurité de la présente pièce jointe et de la supervision des autorités des NNN ayant des responsabilités spécifiques en matière de sécurité des SIC pour les SIC des pays manipulant des informations OTAN classifiées (y compris les NCSA, NDA et SAA).

PIÈCE JOINTE « G »

SÉCURITÉ INDUSTRIELLE ET SÉCURITÉ DES PROJETS CLASSIFIÉS

INTRODUCTION

1. La présente pièce jointe énonce la politique et les normes minimales pour la sécurité des informations OTAN classifiées dans l'industrie. Des précisions et prescriptions supplémentaires sont données dans la directive complémentaire sur la sécurité industrielle et la sécurité des projets classifiés.

2. La sécurité industrielle consiste à appliquer des mesures et procédures de protection pour prévenir ou déceler la perte ou la compromission d'informations classifiées manipulées par l'industrie dans le cadre de contrats, ou pour remédier à une telle perte ou compromission. Les informations OTAN classifiées communiquées à l'industrie et produites à la suite d'un contrat passé avec l'industrie ainsi que les contrats classifiés avec l'industrie doivent être protégés conformément à la politique de sécurité de l'OTAN et à ses directives complémentaires.

3. Les ANS/ASD font en sorte d'avoir les moyens de rendre leurs règles de sécurité industrielle obligatoires pour l'industrie et d'avoir également le droit de vérifier et d'approuver les mesures prises par l'industrie pour la protection des informations OTAN classifiées.

IMPÉRATIFS DE SÉCURITÉ DES ÉTABLISSEMENTS

4. Tout contractant/sous-traitant qui exécute un contrat impliquant des informations OTAN classifiées et qui a besoin d'accéder à des informations classifiées NC ou d'un niveau de classification supérieur, ou de produire de telles informations, détient une habilitation de sécurité délivrée à un établissement (FSC) du niveau approprié, qui aura été délivrée par l'ANS/ASD compétente du pays ayant juridiction sur les installations du contractant/sous-traitant.

5. Aucune FSC n'est requise pour l'accès à des informations classifiées NATO DIFFUSION RESTREINTE (NDR) ni pour la production de telles informations.

SOUMISSION D'OFFRES, NÉGOCIATION ET ATTRIBUTION DE CONTRATS IMPLIQUANT DES INFORMATIONS OTAN CLASSIFIÉES

6. Le contrat principal relatif à un programme/projet OTAN est négocié et attribué par une agence/un bureau de programme/projet OTAN (APO/BPO). Tous les contractants associés à des contrats pour lesquels ils devront gérer ou produire dans leurs établissements des informations classifiées NATO CONFIDENTIEL (NC) ou d'un niveau de classification supérieur, ou avoir accès à de telles informations, doivent posséder une FSC. Pour les contrats classifiés NATO DIFFUSION RESTREINTE (NDR), aucune FSC n'est exigée.

7. L'APO/Le BPO ou toute autre autorité contractante qui entame une procédure contractuelle s'assure que le contractant détient pour son établissement une FSC du niveau approprié pour la phase spécifique du contrat. L'autorité contractante vérifie que le personnel du contractant qui accède à des informations classifiées NC ou d'un niveau de classification supérieur dans les locaux de l'autorité contractante est titulaire d'une PSC du niveau approprié.

8. Après la passation du contrat principal, le contractant principal peut négocier des sous-contrats avec d'autres contractants, c'est-à-dire des sous-traitants. Ces sous-traitants peuvent aussi négocier des sous-contrats avec d'autres sous-traitants. Si ces sous-contrats requièrent un accès à des informations classifiées NC ou d'un niveau de classification supérieur, les exigences de sécurité concernant les établissements et le personnel énoncées dans la section « Habilitations de sécurité industrielle pour les contrats OTAN » de la présente pièce jointe et dans la directive sur la sécurité industrielle et la sécurité des projets classifiés sont applicables. Si un sous-traitant potentiel relève de la juridiction[1] d'un pays non OTAN, la permission de négocier un sous-contrat doit être préalablement obtenue de l'APO/du BPO ou de toute autre autorité contractante. Si l'APO/le BPO a imposé des restrictions à l'attribution de contrats à des pays de l'OTAN qui ne participent pas à un programme/projet, il lui sera demandé au préalable d'envisager d'autoriser toute négociation contractuelle avec des entreprises de ces pays.

9. À la passation du contrat, l'APO/le BPO ou toute autre autorité contractante en donne notification à l'ANS/ASD du contractant, et veille à ce que l'avenant « sécurité » (SAL) et/ou les instructions de sécurité applicables au projet (PSI), selon le cas, soient communiqués au contractant principal, avec le contrat.

IMPÉRATIFS DE SÉCURITÉ POUR LES CONTRATS IMPLIQUANT DES INFORMATIONS OTAN CLASSIFIÉES

10. Le contractant principal et les sous-traitants sont tenus contractuellement, sous peine de voir le contrat résilié, de prendre toutes les mesures prescrites par les ANS/ASD pour protéger toutes les informations OTAN classifiées qui sont confiées au contractant ou dont celui-ci est l'auteur, ou qui sont incorporées à des articles fabriqués par le contractant.

(a) Les contrats relatifs à des programmes/projets de grande envergure impliquant des informations OTAN classifiées contiennent, en annexe, des PSI, dont le « Guide en matière de classification de sécurité dans le cadre du projet » fait partie. Tous les autres contrats impliquant des informations OTAN classifiées contiennent, au minimum, un SAL pouvant être considéré comme des PSI réduites. En pareil cas, le guide en matière de classification de sécurité dans le cadre du programme/projet s'appelle « Liste de contrôle des classifications de sécurité ». Les PSI donnent en complément les principes et les exigences de sécurité de l'OTAN, prévoient les procédures de sécurité spécifiques associées au programme/projet OTAN concerné et attribuent des responsabilités pour la mise en œuvre des mesures de sécurité concernant les informations classifiées.

(b) Pour les contrats impliquant uniquement des informations classifiées NDR, des règles spécifiques ont été établies dans la directive sur la sécurité industrielle et la sécurité des projets classifiés, en particulier dans l'appendice 4 intitulé « Clause contractuelle de sécurité à inclure dans les soumissions et les contrats impliquant des informations NATO DIFFUSION RESTREINTE ».

11. La classification de sécurité des informations d'un programme/projet liées à d'éventuels sous-contrats est fondée sur le guide en matière de classification de sécurité dans le cadre du programme/projet.

[1] Pouvoir d'exercer son autorité dans un domaine ou sur un territoire/une zone géographique.

CONTRATS IMPLIQUANT DES INFORMATIONS OTAN CLASSIFIÉES AVEC DES CONTRACTANTS ÉTABLIS DANS DES PAYS NON OTAN

12. L'attribution de contrats impliquant des informations OTAN classifiées à des contractants établis dans des pays non OTAN constitue une communication d'informations et doit se faire conformément à la pièce jointe « E » au présent C-M, à la directive sur la sécurité des informations OTAN classifiées et à la directive sur la sécurité industrielle et la sécurité des projets classifiés. Cette communication est toujours soumise au consentement du/des originateur(s) concerné(s).

13. Les contrats impliquant des informations OTAN classifiées avec des contractants établis dans des pays non OTAN requièrent un accord/arrangement de sécurité bilatéral entre l'OTAN ou un pays OTAN contractant/se portant garant et le pays non OTAN. Si le contrat est régi par un accord/arrangement de sécurité bilatéral entre un pays OTAN contractant/se portant garant et un pays non OTAN, le pays OTAN donne une assurance de sécurité écrite à l'OTAN confirmant que les informations OTAN classifiées communiquées entrent dans le champ d'application de l'accord/arrangement de sécurité. Une copie de cette assurance est transmise au NOS et à l'APO/au BPO compétent(e).

14. L'attribution d'un contrat à un contractant d'un pays non OTAN devra suivre les procédures établies dans la directive sur la sécurité industrielle et la sécurité des projets classifiés.

15. Pour les pays non OTAN, une ou plusieurs autorité(s) de sécurité compétente(s) exerçant des fonctions équivalentes à celles de l'ANS/ASD dans un pays de l'OTAN sera/seront désignée(s).

HABILITATIONS DE SÉCURITÉ INDUSTRIELLE POUR LES CONTRATS OTAN

Généralités

16. Les principes décrits dans les paragraphes qui suivent pour les établissements et les personnes s'appliquent aux contrats et aux sous-contrats.

Habilitations de sécurité délivrées à des établissements (FSC)

17. Il incombe à l'ANS/ASD de chaque pays de l'OTAN de s'assurer que tout établissement relevant de sa juridiction qui devra avoir accès à des informations classifiées NC ou d'un niveau de classification supérieur a pris les mesures de sécurité nécessaires pour pouvoir obtenir une FSC. Lorsqu'elles délivrent une FSC, les ANS/ASD s'assurent qu'elles sont en mesure d'être avisées de toute circonstance qui risque d'avoir une influence sur la validité de l'habilitation accordée.

18. L'évaluation à faire avant la délivrance d'une FSC doit être conforme aux prescriptions et critères exposés dans la directive complémentaire sur la sécurité industrielle et la sécurité des projets classifiés, ainsi qu'aux lois et règlements nationaux applicables. L'évaluation doit au minimum couvrir les aspects relatifs à l'intégrité et à la probité du contractant/sous-traitant, à la situation de sécurité de son personnel et d'autres personnes qui, en vertu de leurs liens avec le contractant/sous-traitant, pourraient être amenées à avoir accès à des informations OTAN classifiées, ainsi que les questions de propriété, d'influence et de contrôle étrangers.

19. Un soumissionnaire non titulaire d'une FSC appropriée telle qu'elle est demandée aux termes du contrat/sous-contrat potentiel n'est pas automatiquement exclu de l'appel d'offres. L'autorité contractante doit tout mettre en œuvre pour que le niveau de classification de sécurité des informations à fournir aux soumissionnaires soit le plus bas possible tout en permettant à

ceux-ci de répondre de façon éclairée et appropriée à l'appel d'offres. Cependant, le document d'appel d'offres mentionnera l'exigence d'une FSC du niveau approprié, et ce préalablement à l'attribution du contrat/sous-contrat.

20. Différents scénarios énonçant les exigences relatives aux FSC sont présentés dans la directive complémentaire sur la sécurité industrielle et la sécurité des projets classifiés.

21. Il n'est pas nécessaire d'être en possession d'une FSC ou d'une PSC pour les contrats classifiés NDR ou pour l'accès à des informations classifiées NDR. Un pays qui, en vertu de ses lois et règlements de sécurité nationaux, exige la possession d'une FSC pour un contrat ou un sous-contrat classifié NDR ne doit pas exercer de discrimination à l'encontre d'une entreprise dont le pays n'en exige pas, mais s'assure que l'entreprise a été informée de ses responsabilités quant à la protection des informations et obtient d'elle une reconnaissance de ces responsabilités.

Habilitations de sécurité du personnel pour les membres du personnel d'un établissement

22. Le personnel de l'établissement devant avoir accès à des informations classifiées NC ou d'un niveau de classification supérieur doit être titulaire d'une PSC du niveau approprié. Les PSC sont délivrées conformément aux dispositions de la pièce jointe « C » au présent C-M, de la directive sur la sécurité concernant le personnel et de la directive sur la sécurité industrielle et la sécurité des projets classifiés.

23. Les demandes d'habilitation de sécurité pour les membres du personnel d'un contractant sont introduites auprès de l'ANS/ASD dont relève l'établissement.

24. Si un établissement désire employer un ressortissant d'un pays non OTAN à un poste qui exige l'accès à des informations OTAN classifiées, il incombe à l'ANS/ASD du pays qui a juridiction sur l'établissement employeur d'appliquer la procédure d'habilitation de sécurité prescrite dans le présent document, et de déterminer si l'intéressé peut avoir accès à ces informations conformément aux exigences de la pièce jointe « C » au présent C-M, de la directive sur la sécurité concernant le personnel et de la directive sur la sécurité industrielle et la sécurité des projets classifiés.

COMMUNICATION D'INFORMATIONS OTAN CLASSIFIÉES À L'OCCASION DE LA PASSATION DE CONTRATS

25. Par communication d'informations OTAN classifiées à l'occasion de la passation de contrats, on entend la communication de telles informations soit à des pays non OTAN ou à des organisations internationales, soit à des destinataires de pays de l'OTAN ne participant pas au programme/projet. Cette communication se fait avec l'accord de l'APO/du BPO compétent(e) et/ou de l'originateur, selon le cas, et en conformité avec les autres pièces jointes à la politique de sécurité de l'OTAN applicables, la directive sur la sécurité des informations OTAN classifiées et la directive sur la sécurité industrielle et la sécurité des projets classifiés.

MANIPULATION DES INFORMATIONS OTAN CLASSIFIÉES DANS LES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (SIC)

26. Seuls les SIC ayant fait l'objet d'une homologation de sécurité appropriée sont utilisés pour le stockage, le traitement ou la transmission (ci-après « la manipulation ») des informations OTAN classifiées. La pièce jointe « F » au présent C-M, la « Directive principale sur la sécurité des SIC » (AC/35-D/2004), la « Directive sur la gestion de la sécurité des SIC » (AC/35-D/2005) et toutes les directives pertinentes sur les aspects techniques et la mise en œuvre de la sécurité des SIC (documents de l'AC/322) contiennent des principes et des instructions supplémentaires à respecter pour la mise en place des SIC manipulant des informations OTAN classifiées.

27. L'homologation de sécurité des SIC manipulant des informations classifiées NDR peut être déléguée à des contractants, conformément aux lois et règlements de sécurité nationaux. En cas de délégation, les ANS/ASD/SAA compétentes demeurent responsables de la protection des informations NDR que manipule le contractant, et elles conservent le droit de vérifier les mesures de sécurité prises par ce dernier.

PROCÉDURES DE CONTRÔLE DES VISITES INTERNATIONALES (IVCP)

28. Les IVCP s'appliquent aux visites internationales de représentants de pays de l'OTAN, d'organismes civils ou militaires de l'OTAN, ou de titulaires de contrats ou de sous-contrats impliquant des informations OTAN classifiées. Ces procédures peuvent aussi s'appliquer aux représentants d'un pays non OTAN, notamment aux titulaires de contrats ou de sous-contrats d'un tel pays, si ce dernier a adopté les IVCP.

29. Les visites impliquant l'accès à des informations classifiées NC ou d'un niveau de classification supérieur ou celles impliquant un accès sans escorte à des zones de sécurité sont approuvées par l'ANS/ASD. Les visites impliquant l'accès à des informations NSC[2] ou à des informations classifiées NDR peuvent être organisées directement par l'établissement qui effectue et par celui qui reçoit la visite, sans qu'il y ait d'exigence formelle.

30. Les dispositions détaillées concernant le déroulement des visites internationales figurent dans la directive sur la sécurité industrielle et la sécurité des projets classifiés.

PERSONNEL DÉTACHÉ DANS LE CADRE D'UN PROJET OU D'UN PROGRAMME OTAN

31. Lorsqu'une personne titulaire d'une habilitation lui permettant d'avoir accès à des informations OTAN classifiées doit être détachée d'un établissement auprès d'un autre dans le cadre du même programme ou projet OTAN mais dans un pays OTAN différent, l'établissement dont relève cette personne demande à son ANS/ASD de fournir pour elle une confirmation d'habilitation de sécurité du personnel à l'ANS/ASD de l'établissement auprès duquel elle doit être détachée.

TRANSMISSION ET TRANSPORT INTERNATIONAUX DE MATÉRIELS OTAN CLASSIFIÉS

Principes de sécurité applicables à tous les modes de transport

32. Au moment de l'examen des dispositions de sécurité proposées pour le transport international d'envois de matériels classifiés, il convient d'observer les principes suivants :

(a) la sécurité est assurée à tous les stades du transport et quelles que soient les circonstances, du point de départ à la destination finale ;

(b) le degré de protection accordé à un envoi sera déterminé par le plus haut niveau de classification de sécurité des matériels qu'il contient ;

(c) une FSC sera obtenue, au besoin, pour les sociétés assurant les transports. Dans ce cas, le personnel de ces sociétés manipulant l'envoi se verra délivrer une PSC, conformément aux dispositions de la présente pièce jointe ;

(d) les trajets seront effectués de point à point dans la mesure du possible, et aussi rapidement que les circonstances le permettent ;

[2] NSC n'est pas une classification de sécurité de l'OTAN.

(e) on prendra soin de fixer un itinéraire ne traversant que des pays de l'OTAN. Les itinéraires traversant des pays non OTAN ne devraient être utilisés que sur autorisation de l'ANS/ASD ayant juridiction sur l'expéditeur et conformément aux dispositions de la directive complémentaire sur la sécurité des informations OTAN classifiées.

33. Les dispositions applicables aux envois de matériels classifiés sont stipulées pour chaque programme/projet. Toutefois, ces dispositions entrent en vigueur pour réduire le risque d'accès non autorisé aux matériels classifiés.

34. Les normes de sécurité applicables au transfert international d'informations OTAN classifiées figurent dans la directive complémentaire sur la sécurité des informations OTAN classifiées. Cependant, les prescriptions détaillées relatives au convoyage de matériels OTAN classifiés, au transport de matériels classifiés par des société commerciales de messagerie ou par des gardes ou des escortes de sécurité, ainsi qu'au transport d'explosifs, de propergols ou d'autres substances dangereuses, sont exposées dans la directive complémentaire sur la sécurité industrielle et la sécurité des projets classifiés.

PIÈCE JOINTE « H »

SÉCURITÉ CONCERNANT LES ENTITÉS NON OTAN

INTRODUCTION

1. La présente pièce jointe énonce les principes et les normes minimales à appliquer pour la protection des informations OTAN classifiées qui doivent être communiquées à – ou auxquelles doivent avoir accès – des pays non OTAN ou des organismes non OTAN (par exemple des organisations internationales), y compris des personnes représentant ces pays ou organismes (ci-après dénommés « entités non OTAN » (NNE)).

2. Le partage d'informations OTAN classifiées avec des NNE se fait dans le cadre des activités de coopération de l'OTAN approuvées par le Conseil de l'Atlantique Nord. Toute demande de partage d'informations OTAN classifiées avec des NNE hors du cadre de ces activités de coopération est étudiée et approuvée au cas par cas par le Conseil ou par l'autorité déléguée compétente. Des précisions et des prescriptions supplémentaires pour la protection des informations OTAN classifiées devant être communiquées à des NNE, ou auxquelles ceux-ci doivent avoir accès, figurent dans la directive complémentaire pour l'OTAN sur la sécurité concernant les entités non OTAN.

3. Le terme « 7 pays non OTAN » (7 NNN) fait uniquement référence aux pays ci-après et à leurs ressortissants : Australie, Autriche, Finlande, Irlande, Nouvelle-Zélande, Suède et Suisse[1].

4. Les NNE mettent en place une autorité de sécurité compétente responsable de la sécurité des informations OTAN classifiées. Le document complémentaire pour les entités non OTAN sur la sécurité liée à l'OTAN offre aux NNE une vue d'ensemble des principes de base et des normes minimales de sécurité à appliquer pour la protection et la manipulation des informations OTAN classifiées, et de leurs équivalents nationaux, échangées dans le cadre d'activités de coopération de l'OTAN approuvées par le Conseil.

EXIGENCES GÉNÉRALES

5. Le partage d'informations OTAN classifiées avec une NNE peut avoir lieu dans le cadre des activités suivantes :

(a) activité de coopération approuvée par le Conseil, pour laquelle la participation de la NNE a été approuvée par le Conseil de l'Atlantique Nord ;

(b) activité de l'OTAN (par exemple programme, projet, opération ou tâche), pour laquelle la participation de la NNE et sa contribution à un aspect spécifique de l'activité sont considérés comme présentant un intérêt pour l'OTAN ;

(c) collaboration entre un pays de l'OTAN et une NNE, dans le cadre de laquelle le partage d'informations OTAN classifiées a été jugé comme présentant un intérêt pour l'OTAN.

[1] Les ANS/ASD peuvent proposer au Comité de sécurité des modifications à cette liste de pays, pour approbation.

6. Avant tout partage d'informations OTAN classifiées avec une NNE, l'entité en question et l'OTAN doivent avoir conclu un accord de sécurité, dont la mise en œuvre doit être certifiée par le Bureau de sécurité de l'OTAN (NOS). En l'absence d'un tel accord, une assurance de sécurité aura été donnée lorsqu'un impératif politique ou opérationnel nécessite de partager rapidement des informations OTAN classifiées à l'appui d'une activité de coopération approuvée par le Conseil ou, dans des circonstances exceptionnelles, en dehors d'une activité de ce type. La directive complémentaire pour l'OTAN sur la sécurité concernant les NNE décrit en détail les dispositions applicables au partage d'informations OTAN classifiées avec des NNE dans les différents cas exposés au paragraphe 5.

ACCORDS DE SÉCURITÉ ET DISPOSITIONS ADMINISTRATIVES

7. Un accord de sécurité est un instrument qui permet les échanges d'informations classifiées avec une NNE donnée. Il définit des principes stratégiques généraux agréés entre l'OTAN et la NNE, sur la base desquels des mesures de sécurité appropriées sont mises en œuvre pour protéger les informations OTAN classifiées et les informations classifiées de la NNE, le cas échéant. Avant toute communication d'informations OTAN classifiées à une NNE, la mise en œuvre de l'accord de sécurité par la NNE aura été certifiée par le NOS.

8. Les principes de sécurité définis dans l'accord de sécurité reposent sur un ensemble approprié de dispositions administratives. L'exécution d'un accord de sécurité repose sur un ensemble de dispositions administratives, qui énoncent les impératifs de sécurité fondamentaux à respecter pour garantir la protection adéquate et mutuellement acceptable des informations classifiées échangées. Une fois que les dispositions administratives ont été conclues, leur bonne mise en application est confirmée par le NOS à l'occasion d'une visite d'examen.

9. Le NOS effectue des visites d'examen périodiques, au moins une fois tous les deux ans, sur la base d'une approche de gestion des risques, auprès des organismes compétents de la NNE afin de s'assurer que celle-ci continue de respecter l'accord de sécurité et ses dispositions administratives.

ASSURANCES DE SÉCURITÉ

10. En l'absence d'accord de sécurité certifié entre l'OTAN et une NNE, on recourt à une assurance de sécurité lorsque, pour des raisons politiques ou opérationnelles, il faut impérativement partager rapidement des informations OTAN classifiées à l'appui d'une activité de coopération approuvée par le Conseil ou, dans des circonstances exceptionnelles, en dehors d'une activité de ce type. La directive complémentaire pour l'OTAN sur la sécurité concernant les NNE précise les critères à remplir lorsqu'une assurance de sécurité est utilisée.

11. Une assurance de sécurité formalise l'engagement d'une NNE à offrir aux informations OTAN classifiées reçues, quelles qu'elles soient, un niveau de protection approprié. Elle est limitée à une activité bien précise et reste valable pendant une durée bien précise.

12. Une assurance de sécurité signée par un représentant dûment mandaté par la NNE est donnée au NOS lorsqu'une telle assurance est utilisée pour permettre le partage d'informations OTAN classifiées à l'appui :

(a) d'une activité de coopération approuvée par le Conseil ;

(b) d'une activité de l'OTAN pour laquelle la participation de la NNE a été approuvée par le Conseil ou par l'autorité déléguée compétente, au cas par cas.

Rôle de garant joué par un pays de l'OTAN

13. Le partage d'informations OTAN classifiées dans le cadre d'activités autres que celles visées aux alinéas 12 (a) et (b) suite à une demande spéciale d'un pays de l'OTAN, nécessite un garant. Le rôle de garant joué par un pays de l'OTAN correspond au soutien qu'il apporte à une NNE afin de permettre le partage d'informations OTAN classifiées avec celle-ci en l'absence d'accord de sécurité certifié entre l'OTAN et cette NNE.

14. Pour qu'un pays de l'OTAN puisse jouer ce rôle de garant, il faut un cadre de sécurité approprié (par exemple un accord de sécurité ou toute autre disposition applicable) entre le garant et la NNE. Le garant est tenu de remettre au NOS une assurance de sécurité écrite et signée par un représentant dûment mandaté par la NNE. L'assurance de sécurité énonce les normes minimales que la NNE appliquera pour la protection des informations OTAN classifiées.

15. Le rôle de garant est limité à une activité bien précise et reste valable pendant une durée bien précise.

DISPOSITIONS DE SÉCURITÉ PARTICULIÈRES

16. Pour le partage d'informations OTAN classifiées avec des NNE, trois cas de figure sont envisageables s'agissant de l'accès à des installations de l'OTAN ou à des informations OTAN classifiées : accès aux installations de l'OTAN, accès aux informations OTAN classifiées, et communication d'informations OTAN classifiées. La directive complémentaire pour l'OTAN sur la sécurité concernant les NNE précise les critères ainsi que les mesures et procédures spécifiques correspondantes à appliquer pour chaque cas.

Sécurité concernant le personnel

17. Avant qu'un représentant d'une NNE puisse avoir accès à des informations classifiées NC ou d'un niveau de classification supérieur, il doit avoir fait l'objet d'une procédure favorable d'habilitation PSC qui n'est pas moins rigoureuse que celle qui s'appliquerait à un ressortissant d'un pays de l'OTAN en vertu de la politique de sécurité de l'OTAN et de ses directives complémentaires.

18. Aucune PSC n'est requise pour l'accès à des informations classifiées NATO DIFFUSION RESTREINTE (NDR). Toutefois, le représentant d'une NNE doit pouvoir justifier du besoin d'en connaître, avoir été informé de ses obligations pour ce qui est de la protection des informations OTAN classifiées, et avoir déclaré être conscient de ses responsabilités en matière de sécurité soit par écrit, soit par une méthode équivalente assurant la non-répudiation.

19. Une PSC peut être requise pour accéder à des installations de l'OTAN en fonction des critères spécifiques stipulés dans la directive complémentaire pour l'OTAN sur la sécurité concernant les NNE et des règles de sécurité locales pertinentes.

Sécurité physique

20. Les représentants de NNE qui, de par leur affectation et leurs fonctions officielles, doivent entretenir des contacts réguliers avec des services de l'OTAN peuvent obtenir une autorisation d'accès à des zones spécifiques dans lesquelles des informations classifiées NR ou d'un niveau de classification supérieur sont conservées, manipulées et/ou examinées. Ces personnes peuvent également se voir attribuer un bureau dans des zones spécifiques. L'octroi d'un accès sans escorte et/ou l'attribution de bureaux se font au cas par cas.

21. La directive complémentaire pour l'OTAN sur la sécurité concernant les NNE énonce en détail la procédure à suivre, les autorités d'approbation à contacter et les critères à remplir pour qu'un représentant d'une NNE puisse se voir octroyer un accès à une zone de sécurité de classe I ou II ou à une zone administrative.

Sécurité des informations

22. Dans le cadre d'une coopération avec des NNE, on distingue trois cas de figure dans lesquels des NNE peuvent se voir autoriser l'accès à des informations OTAN classifiées ou à des installations de l'OTAN :

(a) **Accès à des installations de l'OTAN** Un représentant d'une NNE est autorisé à avoir physiquement accès à un site spécifique de l'OTAN, à une installation ou à une zone précise à l'intérieur d'une installation. L'accès physique ne sous-entend pas automatiquement un accès à des informations OTAN classifiées.

(b) **Accès aux informations OTAN classifiées** Une personne représentant une NNE est autorisée à accéder à des informations OTAN classifiées pour accomplir sa tâche et exercer ses fonctions officielles lorsque l'accès présente un intérêt pour l'OTAN. L'accès est limité à ce seul représentant, qui n'a pas le droit de diffuser ces informations OTAN classifiées à d'autres membres de la NNE sauf si elles ont été communiquées en vertu des dispositions établies.

(c) **Communication des informations OTAN classifiées** Des informations OTAN classifiées peuvent être communiquées à une NNE.

23. La directive complémentaire pour l'OTAN sur la sécurité concernant les NNE précise les critères qui doivent être remplis dans les cas particuliers où un organisme civil ou militaire de l'OTAN, ou un pays de l'OTAN, doit octroyer un accès à des informations OTAN classifiées ou communiquer de telles informations.

24. La communication d'informations OTAN classifiées à une NNE est toujours subordonnée à l'obtention du consentement écrit préalable du ou des originateurs.

25. Des informations OTAN classifiées peuvent être communiquées dans le cadre d'une activité de coopération approuvée par le Conseil ou d'une activité de l'OTAN pour laquelle l'association de participants de NNE a été approuvée par le Conseil ou par l'autorité déléguée compétente. La directive complémentaire pour l'OTAN sur la sécurité concernant les NNE précise un ensemble de critères supplémentaires à appliquer avant toute communication d'informations.

26. Pour ce qui est des informations OTAN classifiées à communiquer sur demande spéciale d'un pays de l'OTAN (le garant) à une NNE en dehors de toute activité de coopération approuvée par le Conseil ou de toute activité de l'OTAN pour laquelle l'association de participants de NNE a été approuvée par le Conseil ou par l'autorité déléguée compétente, la directive complémentaire pour l'OTAN sur la sécurité concernant les NNE précise les critères supplémentaires à appliquer avant toute communication d'informations.

27. Lorsqu'un accord de sécurité ou une assurance de sécurité existe avec une organisation internationale, la communication d'informations OTAN classifiées aux membres non OTAN de celle-ci se fait conformément aux dispositions pertinentes de cet accord de sécurité et à d'autres règles établies dans le cadre de leur participation à des activités de l'OTAN. En l'absence d'accord de sécurité, lorsqu'il existe une assurance de sécurité avec une organisation internationale, la communication d'informations OTAN classifiées aux membres non OTAN de celle-ci se fait conformément aux dispositions pertinentes de la directive complémentaire et de cette assurance de sécurité.

28. Une NNE qui n'est pas partie à l'Accord en vigueur entre les États parties au Traité de l'Atlantique Nord sur la coopération dans le domaine des renseignements atomiques (C-M(64)39) ne peut pas se voir communiquer des informations ATOMAL, quelle qu'en soit la classification de sécurité, ni y avoir accès.

Autorité ayant le pouvoir d'autoriser la communication

29. Le Conseil de l'Atlantique Nord est l'autorité suprême pour la communication d'informations OTAN classifiées à des NNE. Ce pouvoir d'autoriser la communication est soumis au principe du consentement de l'originateur et est délégué :

(a) au comité compétent en la matière, pour les informations classifiées jusqu'au niveau NS inclus ayant pour origine ce même comité et/ou les organes qui lui sont subordonnés. Pour les informations classifiées NDR, le comité compétent en la matière peut à son tour déléguer ce pouvoir à une personne exerçant des fonctions de soutien bien déterminées ou jouant un rôle particulier au sein des services de soutien à ce comité ;

(b) au Comité militaire, pour les informations classifiées jusqu'au niveau NS inclus ayant pour origine lui-même et/ou les organismes qui lui sont subordonnés. Pour les informations classifiées NDR, le Comité militaire peut à son tour déléguer ce pouvoir à une personne exerçant des fonctions de soutien bien déterminées ou jouant un rôle particulier au sein de ses services de soutien ;

(c) au SACEUR ou au DSACEUR, pour les informations classifiées jusqu'au niveau NS inclus qui sont identifiées comme étant communicables à la mission (XFOR) ou pour les informations classifiées NATO/XFOR SECRET (Mission SECRET), sous réserve de conditions spécifiques, lesquelles sont précisées dans la directive complémentaire pour l'OTAN sur la sécurité concernant les NNE ;

(d) au SACT ou au SACT adjoint, pour les informations classifiées jusqu'au niveau NS inclus, sous réserve de conditions spécifiques, lesquelles sont précisées dans la directive complémentaire pour l'OTAN sur la sécurité concernant les NNE ;

(e) au Commandant de la mission pour une opération à laquelle sont associés des NNTCN dont la participation aura été entérinée par le Conseil, pour les informations classifiées jusqu'au niveau NS inclus et déjà désignées comme étant communicables à la mission (XFOR), sous réserve de conditions spécifiques, lesquelles sont précisées dans la directive complémentaire pour l'OTAN sur la sécurité concernant les NNE ;

(f) à l'organisation de production et de logistique de l'OTAN (OPLO), en coordination avec les pays participants, pour les informations OTAN classifiées ayant leur origine dans un ou plusieurs des pays de l'OPLO et leur appartenant.

30. Compte tenu des exceptions relatives aux informations classifiées NDR énoncées aux alinéas 29 (a) et (b), les autorités ayant reçu délégation de pouvoir pour autoriser la communication ne peuvent pas elles-mêmes déléguer leur pouvoir.

31. Le pouvoir d'autoriser la communication ne peut être délégué qu'à un comité compétent en la matière au sein duquel l'originateur/les originateurs est/sont représenté(s). Si l'on ne peut identifier l'originateur/les originateurs, le comité compétent en la matière assume la responsabilité d'originateur.

32. Les instructions d'application pour le partage du renseignement entre l'OTAN et les NNE (DSG(2015)0307-REV1) et le document complémentaire sur le partage des informations et du renseignement avec des entités non OTAN (AC/35-D/1040) déterminent l'autorité ayant le pouvoir d'autoriser la communication dans des environnements tels que les opérations, l'entraînement, les exercices, la transformation ou la coopération.

Registre des informations communiquées

33. Les organismes civils et militaires de l'OTAN tiennent des registres de toutes les informations classifiées NC ou d'un niveau de classification supérieur qu'ils ont décidé de communiquer à une NNE et ils transmettent, au minimum tous les six mois, au Bureau d'ordre central de l'OTAN, à Bruxelles, le numéro de référence, le titre et la date de communication des documents concernés, sauf instructions contraires émanant de l'autorité de sécurité compétente.

Sécurité des systèmes d'information et de communication

34. La directive complémentaire pour l'OTAN sur la sécurité concernant les NNE énonce les conditions spécifiques qui doivent être réunies pour octroyer un accès à un systèmes d'information et de communication (CIS) de l'OTAN à une NNE.

35. L'interconnexion de SIC de l'OTAN avec le SIC d'une NNE doit faire l'objet d'une homologation de sécurité conforme aux dispositions de la politique de sécurité de l'OTAN et de ses directives complémentaires.

INCIDENTS DE SÉCURITÉ

36. Les incidents de sécurité qui impliquent des informations classifiées d'une NNE en possession de l'OTAN sont régis par les dispositions de la directive sur la sécurité des informations OTAN classifiées (AC/35-D/2002) et par toute disposition supplémentaire stipulée dans l'accord de sécurité, et ses dispositions administratives, conclu avec la NNE ou dans l'assurance de sécurité qui aura été donnée.

37. Les incidents de sécurité qui impliquent des informations classifiées d'une NNE sont signalés immédiatement au NOS. Le NOS doit informer rapidement l'autorité de sécurité compétente de la NNE de tout incident de sécurité impliquant des informations classifiées de la NNE, conformément à l'accord de sécurité et à ses dispositions administratives d'application, ou à l'assurance de sécurité.

GLOSSAIRE

Accès à des informations	Autorisation accordée à une ou plusieurs personnes d'être exposées à des informations, moyennant le respect des paramètres de sécurité requis pour l'exécution de leurs tâches, clairement définies et dûment autorisées. Dans ces circonstances, l'accès est autorisé uniquement à la personne concernée, qui n'est pas autorisée à transmettre ces informations.
Accès aux locaux	Autorisation d'accès physique à des installations données accordée à une ou plusieurs personnes choisies, avec ou sans escorte désignée, en fonction des impératifs de sécurité en vigueur et des habilitations de sécurité requises.
Agence de gestion de projet de l'OTAN	Organe exécutif d'une OPLO.
Assurance de l'information	Les informations sont protégées selon le principe de l'assurance de l'information, qui se définit comme l'ensemble des mesures visant à atteindre un degré donné de confiance dans la protection des systèmes d'information et de communication – électroniques et non électroniques – ainsi que dans les informations stockées dans ces systèmes ou traitées ou transmises au moyen de ceux-ci, pour ce qui est de leur confidentialité, de leur intégrité, de leur disponibilité, de leur non-répudiation et de leur authentification.
Authentification	Action de vérifier l'identité déclarée d'une entité.
Autorité de sécurité compétente	Autorité désignée par l'ANS qui est autorisée à exécuter des tâches spécifiques en matière de sécurité, y compris celles liées à la délivrance des habilitations de sécurité du personnel pour donner aux ressortissants de son pays l'accès aux informations OTAN classifiées.
Assurance de sécurité	Assurance donnée à l'OTAN, soit directement soit par l'intermédiaire d'un pays ou d'un organisme civil ou militaire de l'OTAN autorisant la communication, qu'un destinataire non OTAN d'informations OTAN classifiées assurera le même degré de protection que celui qu'exige la politique de sécurité de l'OTAN.
Autorité de sécurité désignée (ASD)	Autorité chargée d'informer l'industrie de la politique nationale couvrant tous les aspects de la politique de sécurité industrielle de l'OTAN, et de fournir les orientations et l'assistance nécessaires pour que cette politique soit appliquée. Dans certains pays, les fonctions d'ASD peuvent être remplies par l'ANS.
Autorité nationale de sécurité (ANS)	Autorité chargée d'assurer la sécurité des informations OTAN classifiées dans les organismes et services nationaux, militaires ou civils, dans le pays ou à l'étranger.

Avenant « sécurité » (SAL)	Document délivré par l'autorité compétente dans le cadre d'un contrat ou sous-contrat OTAN classifié ne portant pas sur un programme/projet de grande envergure, pour énoncer les impératifs de sécurité ou indiquer les éléments de ce contrat ou sous-contrat qui exigent une
Besoin d'en connaître	Principe selon lequel il est établi avec certitude qu'un destinataire potentiel a besoin d'accéder à des informations, d'en prendre connaissance ou d'entrer en leur possession, pour accomplir des tâches ou fournir des services officiels.
Centre de communication	Organisme responsable du traitement et du contrôle des communications, qui comporte normalement un centre de traitement des messages, un centre de cryptographie et des installations d'émission et de réception.
Clés de sûreté	Dispositifs permettant d'actionner les serrures montées sur les armoires fortes destinées à la conservation de matériels classifiés, sur les portes des pièces ou des zones sécurisées, sur les portes des pièces ou des zones sécurisées qui ont été soumises à des inspections de sécurité technique, et sur les coffrets de sécurité destinés au transport de documents classifiés.
Comité militaire	La plus haute autorité militaire de l'OTAN, responsable de la conduite globale des affaires militaires. Le Comité militaire est chargé d'aviser et de classer par ordre de priorité, d'un point de vue opérationnel, les besoins des utilisateurs soumis par les commandants stratégiques.
Communication d'informations	Fait d'autoriser une entité destinataire à recevoir des informations, étant entendu que ces informations seront mises à la disposition de l'ensemble de l'entité concernée. La communication des informations peut être facilitée par une personne représentant l'entité en question.
Compromission	Il y a compromission lorsque, à la suite d'une violation de sécurité ou d'une activité à caractère hostile (par exemple, espionnage, actes de terrorisme, sabotage ou vol), des informations OTAN classifiées ont perdu leur confidentialité, leur intégrité ou leur disponibilité, ou les services et ressources connexes ont perdu leur intégrité ou leur disponibilité. Cela inclut la perte, la communication à des personnes non autorisées (par exemple aux médias ou encore en cas d'espionnage), la modification non autorisée, la destruction d'une manière non autorisée, et le déni de service.
Confidentialité	Propriété d'une information qui n'est ni mise à la disposition, ni divulguée à des personnes ou entités non autorisées.
Contractant	Entité industrielle, commerciale ou autre qui s'engage à fournir des biens ou services.
Contractant principal	Entité industrielle, commerciale ou autre d'un pays membre qui a passé contrat avec une agence/un bureau de gestion de projet de l'OTAN pour la fourniture d'un service ou la fabrication d'un produit dans le cadre d'un projet de l'OTAN et qui peut elle-même passer contrat avec des sous-traitants potentiels, après approbation.
Contrat	Accord sur la fourniture de biens ou services ayant force exécutoire.

Contrat OTAN classifié	Contrat établi par un organisme civil ou militaire ou par un pays de l'OTAN dans le cadre d'un programme/projet financé ou administré par l'OTAN qui nécessitera l'accès à des informations OTAN classifiées ou qui entraînera la création de telles informations.
Contrat principal	Contrat initial passé par une agence/un bureau de gestion de projet de l'OTAN pour un programme/ projet.
Contrôle de l'originateur	Principe selon lequel le pays, l'OTAN ou l'entité sous l'autorité duquel/de laquelle des informations ont été créées, produites ou introduites à l'OTAN fixe les règles et normes applicables à l'emploi de ces informations et a toute latitude pour y apporter toutes modifications au cours du cycle de vie de ces informations.
Courrier	Personne officiellement affectée au transport de matériel.
Cycle de vie	Le cycle de vie des informations englobe les stades de la planification, du recueil, de la création ou de la production des informations, leur organisation, leur récupération, leur utilisation, leur accessibilité et leur transmission, leur stockage et leur protection, et, enfin, leur liquidation par leur transfert aux archives ou leur destruction.
Destinataire	Contractant, établissement ou autre organisme qui reçoit du matériel de l'expéditeur.
Disponibilité	Propriété des informations et matériels qui sont accessibles et utilisables, sur demande, par une personne ou entité autorisée.
Document	Toute information enregistrée, quelles qu'en soient sa forme ou ses caractéristiques physiques, notamment : textes écrits ou imprimés, cartes et bandes de traitement de données, cartes géographiques, graphiques, photographies, peintures, dessins, gravures, esquisses, notes et documents de travail, copies carbone ou rubans à encre, reproductions par quelque moyen ou selon quelque procédé que ce soit, enregistrements, sous quelque forme ce soit, de sons ou de voix sur support magnétique, électronique, optique ou vidéo, matériel informatique portable avec mémoire résidente ou amovible.
Envoi recommandé	Service de courrier qui offre à l'expéditeur la possibilité de suivre l'envoi jusqu'à sa destination et qui lui permet d'avoir une preuve de livraison.
Escorte	Personnel, armé ou non armé, appartenant à la police nationale, à des formations militaires ou à d'autres services officiels. Ce personnel a pour fonction de faciliter le transport sécurisé des matériels, mais il n'a pas de responsabilité directe en matière de protection du matériel proprement dit.
Établissement	Installation, usine, fabrique, laboratoire, bureau, université ou autre institut d'enseignement, ou entreprise commerciale, y compris les dépôts, entrepôts, viabilités et éléments qui en dépendent et qui, par leur fonction et leur implantation, forment un ensemble d'exploitation.
Expéditeur	Contractant, établissement ou autre organisme responsable de l'organisation de l'expédition de matériel.

Garant	Pays ou organisme civil ou militaire de l'OTAN qui se porte garant qu'une NNE qui a accès à des informations OTAN classifiées va leur accorder la protection requise conformément aux principes et aux spécifications de base définis dans la politique de sécurité de l'OTAN et ses directives complémentaires.
Garde	Personnel civil (appartenant aux services officiels ou faisant partie du personnel du contractant participant) ou militaire, armé ou non armé. Il peut être affecté exclusivement à des tâches de garde de sécurité ou combiner ces tâches avec d'autres fonctions.
Gestion dynamique des risques	Capacité de gérer les risques d'une manière telle que le risque lié à l'utilisation d'un SIC soit évalué en permanence, que tout changement intervenant dans le contexte opérationnel du SIC soit pris en compte de façon dynamique dans la signature de risque, et que les contre-mesures de sécurité les plus adaptées à la situation soient appliquées en temps opportun.
Gestion des risques	Approche systématique visant à déterminer quelles contre-mesures de sécurité sont requises pour protéger les informations ainsi que les services et ressources connexes sur la base d'une évaluation des menaces et des vulnérabilités. La gestion des risques suppose qu'il y ait une planification, une organisation, une orientation et un contrôle des ressources propres à garantir que les risques restent dans des limites acceptables.
Guide en matière de classification de sécurité dans le cadre du programme/projet	Partie des instructions de sécurité (PSI) relatives au programme (projet) qui indique quels éléments du programme sont classifiés, en précisant les niveaux de classification de sécurité. Ce guide peut être développé tout au long de la durée d'existence du programme, et les éléments d'information peuvent être reclassifiés ou déclassés.
Habilitation de sécurité délivrée à un établissement (FSC)	Détermination administrative, par une ANS/ASD, du fait que, sur le plan de la sécurité, un établissement est apte à assurer la protection adéquate d'informations OTAN classifiées ayant un niveau de classification de sécurité donné ou un niveau inférieur, et que les membres de son personnel qui doivent avoir accès à des informations OTAN classifiées possèdent l'habilitation de sécurité appropriée et ont été informés des règles de sécurité de l'OTAN à respecter pour l'exécution des contrats OTAN classifiés.
Habilitation de sécurité du personnel (PSC)	Décision positive par laquelle une ANS/ASD reconnaît officiellement le droit d'un individu d'avoir accès à des informations classifiées NC et d'un niveau de classification supérieur, eu égard à sa loyauté, à la confiance qui peut lui être accordée et à sa fiabilité.
Incident de sécurité	Événement ou autre fait qui est susceptible de porter atteinte à la sécurité des informations OTAN classifiées et qui requiert un complément d'enquête pour établir avec précision s'il constitue une violation ou une infraction de sécurité.
Information	Connaissance susceptible d'être communiquée sous une forme ou une autre.

Informations classifiées	Toute information (à savoir toute connaissance pouvant être communiquée, sous quelque forme que ce soit) ou tout matériel dont il a été déterminé qu'elle/il nécessite une protection contre une divulgation non autorisée et qui a été désigné(e) comme tel(le) par une classification de sécurité.
Informations comptabilisables	Toutes les informations classifiées CTS et NS et toutes les informations de catégorie spéciale (par exemple, ATOMAL).
Informations de catégorie spéciale	Informations telles que les informations ATOMAL, les informations relatives au plan opérationnel unique intégré (SIOP), les informations BOHEMIA ou les informations CRYPTO, auxquelles s'appliquent des procédures supplémentaires de manipulation/protection.
Informations OTAN	Toutes informations, classifiées ou non, diffusées au sein de l'OTAN, qu'elles proviennent d'organismes civils ou militaires de l'OTAN ou qu'elles soient transmises par des pays membres ou par des sources non OTAN.
Informations OTAN classifiées	(a) Le terme « informations » désigne toute connaissance pouvant être communiquée sous quelque forme que ce soit. (b) Les informations classifiées sont des informations ou des matériels qui nécessitent une protection contre une communication non autorisée et qui sont désignés comme tels par leur classification de sécurité. (c) Le terme « matériels » englobe le document et tout élément de machine, d'équipement ou d'arme, fabriqué ou en cours de fabrication. (d) Le terme « document » renvoie à toute information enregistrée, quelles qu'en soient sa forme ou ses caractéristiques physiques, notamment : textes écrits ou imprimés, cartes et bandes de traitement de données, cartes géographiques, graphiques, photographies, peintures, dessins, gravures, esquisses, notes et documents de travail, copies carbone ou rubans à encre, reproductions par quelque moyen ou selon quelque procédé que ce soit, enregistrements, sous quelque forme ce soit, de sons ou de voix sur support magnétique, électronique, optique ou vidéo, matériel informatique portable avec mémoire résidente ou amovible.
Infraction	Acte ou omission à caractère délibéré ou accidentel contraire à la politique de sécurité de l'OTAN et aux directives complémentaires qui n'entraîne pas la compromission effective ou possible d'informations OTAN classifiées (par exemple, informations OTAN classifiées laissées sans protection dans un établissement sécurisé où toutes les personnes présentes sont dûment habilitées, informations OTAN classifiées qui ne sont pas mises sous double enveloppe, etc.).
Instructions de sécurité applicables au programme/projet (PSI)	Ensemble de règles et de procédures de sécurité fondé sur la politique de sécurité de l'OTAN et les directives complémentaires, et appliqué à un programme/projet spécifique. Les PSI constituent également une annexe au contrat principal, et peuvent être révisées tout au long de la durée d'existence du programme. Pour les sous-contrats attribués dans le cadre du programme, les PSI constituent la base du SAL.

Intégrité	Propriété des informations (y compris les données, telles que les textes chiffrés) qui n'ont pas été modifiées ou détruites sans autorisation.
Liste de contrôle des classifications de sécurité	Partie d'un avenant « sécurité » (SAL) qui décrit les éléments d'un contrat qui sont classifiés, en précisant les niveaux de classification de sécurité. Pour les contrats attribués dans le cadre d'un programme/projet, ces éléments d'information ont leur origine dans les instructions de sécurité relatives au programme (projet) établies pour ce programme.
Matériel	Documents et machines, équipements/composants, armes ou outils fabriqués ou en cours de fabrication.
Matériel cryptographique	Comprend les algorithmes cryptographiques et les modules et produits matériels – et logiciels – cryptographiques, y compris les détails relatifs à la mise en œuvre, les documents connexes et le matériel de constitution des clés (à la fois pour les mécanismes cryptographiques symétriques et asymétriques).
Menace	Potentiel de compromission, de perte ou de vol d'informations OTAN classifiées ou de services et ressources connexes. Une menace peut être définie en fonction de sa source, de la motivation de son auteur ou de son résultat, elle peut être délibérée ou accidentelle, violente ou subreptice, externe ou interne.
Négociations	Tous les aspects de l'attribution d'un contrat ou d'un sous-contrat, depuis la « notification de l'intention de lancer un appel d'offres » jusqu'à la décision d'attribuer un contrat ou un sous-contrat.
Non-répudiation	Mesure qui permet d'assurer au destinataire que les informations ont été adressées par une personne ou une organisation particulière et à l'expéditeur que ces informations ont été reçues par les bons destinataires.
Organisation de production et de logistique de l'OTAN (OPLO)	Organisme subsidiaire, créé dans le cadre de l'OTAN pour l'exécution de tâches découlant du Traité, jouissant, par décision du Conseil de l'Atlantique Nord, d'une autonomie structurelle, administrative et financière nettement définie. Il comprend un comité de direction et un organe exécutif, composé d'un directeur général et de son personnel.
Originateur	Pays ou organisation internationale sous l'autorité duquel/de laquelle des informations ont été produites ou introduites à l'OTAN.
OTAN	Le sigle « OTAN » désigne l'Organisation du Traité de l'Atlantique Nord et les organismes régis soit par la Convention sur le statut de l'Organisation du Traité de l'Atlantique Nord, des représentants nationaux et du personnel international, signée à Ottawa le 20 septembre 1951, soit par le Protocole sur le statut des quartiers généraux militaires internationaux, adopté à la suite du Traité de l'Atlantique Nord, et signé à Paris le 28 août 1952.
Pays d'appartenance	Pays dont un individu est ressortissant.

Pays hôte	Sens général : Pays dans lequel un organisme civil ou militaire de l'OTAN est établi. Sécurité industrielle : Pays désigné par un organisme officiel de l'OTAN en tant que service gouvernemental partie au contrat pour assurer l'exécution d'un contrat principal de l'OTAN. Les pays dans lesquels sont exécutés des sous-contrats ne sont pas appelés pays hôtes.
Principe d'agrégation	Lorsqu'un volume important d'informations OTAN classifiées sont compilées, il faut conserver les marques de classification de sécurité initiales et évaluer la classification de ces informations compilées en fonction de l'impact que leur perte ou leur compromission aurait sur l'Organisation. Si cet impact est jugé globalement plus grave que celui correspondant à la classification de sécurité de chacun des documents compilés, il conviendra d'envisager de manipuler et de protéger ces informations à un niveau de classification supérieur, selon l'estimation de l'impact qu'aurait leur perte ou leur compromission.
Programme de l'OTAN	Programme approuvé par le Conseil qui est administré par une agence/un bureau de gestion de l'OTAN conformément aux règlements de l'OTAN.
Programme/projet de grande envergure	Programme ou projet d'importance majeure faisant normalement intervenir plus de deux pays et comportant l'application de mesures de sécurité qui vont au-delà des exigences de base normales décrites dans la politique de sécurité de l'OTAN.
Projet de l'OTAN	Projet approuvé par le Conseil qui est administré par une agence/un bureau de gestion de l'OTAN conformément aux règlements de
Propriétaire du risque	Personne ou organisme chargé d'évaluer les menaces, les vulnérabilités et l'impact d'un risque donné en vue de définir une propension au risque adéquate basée sur la mise en œuvre de facteurs
Ressortissants	Les ressortissants incluent les « sujets d'un royaume », les « citoyens d'un État » et les « résidents permanents au Canada ». Les « résidents permanents au Canada » ont fait l'objet d'un processus d'examen national, y compris une vérification de domicile, des casiers judiciaires et des dossiers des services de sécurité, et vont obtenir l'autorisation légale d'établir leur résidence permanente dans le pays.
Risque	Probabilité qu'une menace se concrétise par l'exploitation effective d'une vulnérabilité, entraînant une compromission de la confidentialité, de l'intégrité et/ou de la disponibilité, qui provoquerait elle-même des dommages.

Sécurité des systèmes d'information et de communication (sécurité des SIC)	Application de mesures de sécurité pour la protection des systèmes de communication et d'information et d'autres systèmes électroniques ainsi que des informations stockées dans ces systèmes ou traitées ou transmises au moyen de ceux-ci, pour ce qui est de leur confidentialité, de leur intégrité, de leur disponibilité, de leur authentification et de leur non-répudiation.
Service de courrier	Service mettant à disposition des personnes dont la mission officielle est de transporter des matériels.
Services non liés à la confidentialité	Services destinés à la sécurité des SIC et portant sur des objectifs de sécurité autres que la confidentialité, à savoir la disponibilité, l'intégrité, l'authentification et la non-répudiation.
Sous-contrat	Contrat conclu par un contractant principal avec un autre contractant (le sous-traitant) pour la fourniture de biens ou de services.
Sous-traitant	Entreprise à laquelle un contractant principal attribue un sous-contrat.
Support lisible par une machine	Support pouvant transmettre des données à un dispositif de lecture.
Transport par porteur	Transfert d'informations par une personne, qui porte physiquement ces informations.
Violation de sécurité	Acte ou omission, à caractère délibéré ou accidentel, contraire à la politique de sécurité de l'OTAN et à ses directives complémentaires qui entraîne la compromission effective ou possible d'informations OTAN classifiées ou de services et ressources connexes (ce qui inclut, par exemple, les informations classifiées perdues pendant leur transport, les informations classifiées laissées dans une zone non sécurisée à laquelle des personnes non habilitées ont accès sans escorte, un document comptabilisable qui ne peut être retrouvé, les informations classifiées qui ont l'objet d'une modification non autorisée ou qui ont été détruites d'une manière non autorisée, ou, pour les SIC, un déni de service)
Visites internationales	Visites effectuées par des personnes dépendant d'une ANS/ASD ou appartenant à un organisme de l'OTAN et se rendant dans des établissements ou organismes dépendant d'une autre ANS/ASD ou de l'OTAN, qui nécessitent ou peuvent occasionner l'accès à des informations OTAN classifiées ou au sujet desquelles, quel que soit le niveau de classification, il est prévu, par la législation nationale applicable à l'établissement ou à l'organisme visité dans le cadre d'activités approuvées par l'OTAN, qu'elles doivent être approuvées par l'ANS/ASD compétente. Tous les organismes civils et militaires de l'OTAN tombent sous la juridiction de sécurité de l'OTAN.
Vulnérabilité	Faiblesse, attribut ou absence de contrôle qui permettrait ou faciliterait la concrétisation d'une menace contre des informations OTAN classifiées ou des services et ressources connexes.
Zone administrative	Zone protégée clairement délimitée dans laquelle les personnes peuvent se déplacer sans escorte et où l'accès est soumis à autorisation.

Zone de rangement ouverte	Zone construite conformément aux impératifs de sécurité et autorisée par le chef de l'organisme civil ou militaire pour le rangement dans un espace ouvert d'informations classifiées.