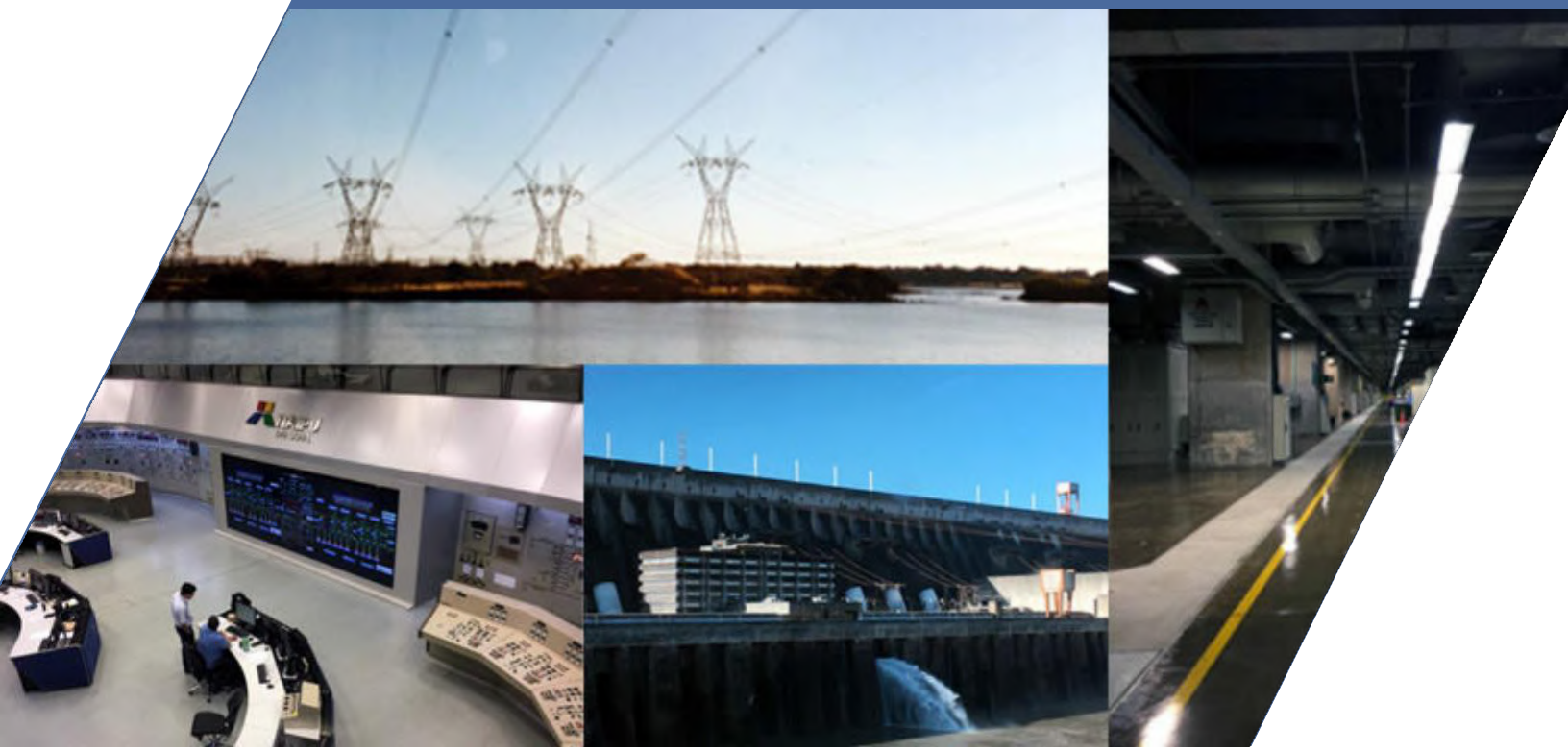
NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME
Centre de l'ONU pour la lutte contre le terrorisme

CONSEIL DE SÉCURITÉ DES NATIONS UNIES
DIRECTION EXÉCUTIVE DU
COMITÉ CONTRE LE TERRORISME (DECT)

INTERPOL

La protection des infrastructures critiques contre les attaques terroristes : Recueil de bonnes pratiques



Établi par la Direction exécutive du Comité contre le terrorisme et le Bureau de lutte contre le terrorisme en 2018

LA PROTECTION DES INFRASTRUCTURES CRITIQUES CONTRE LES ATTAQUES TERRORISTES :

RECUEIL DE BONNES PRATIQUES

Table des matières

PRÉFACE

Le 17 février 2017, le Conseil de sécurité a adopté à l'unanimité la résolution 2341 (2017) sur la protection des infrastructures critiques et le renforcement de la capacité des États de prévenir les attaques contre ces infrastructures, en priant les États Membres de lutter contre le danger que posent lesdites attaques. Dans sa résolution, le Conseil invite les États Membres à envisager éventuellement l'adoption de mesures préventives dans le cadre de l'élaboration des stratégies et des politiques nationales.

Dans la Stratégie antiterroriste mondiale des Nations Unies et au titre du pilier II relatif aux « mesures destinées à combattre et à prévenir le terrorisme », les États Membres ont décidé de « renforcer les efforts visant à améliorer la sécurité et la protection des cibles particulièrement vulnérables comme les infrastructures et les lieux publics, ainsi que les interventions en cas d'attaques terroristes et d'autres catastrophes, en particulier dans le domaine de la protection des civils, tout en reconnaissant que les États pourront avoir besoin d'une assistance à cet égard ».

Dans sa résolution 1373 (2001), le Conseil de sécurité avait déjà invité les États membres à « prendre les mesures voulues pour empêcher que des actes de terrorisme ne soient commis, notamment en assurant l'alerte rapide d'autres États par l'échange de renseignements ». Par sa résolution 1566 (2004), le Conseil de sécurité avait également appelé les États à prévenir les actes criminels perpétrés notamment contre des civils, dans le but de semer la terreur parmi la population ou chez un groupe de personnes, d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à accomplir un acte ou à s'abstenir de le faire. La protection physique des infrastructures critiques peut prévenir la commission d'attentats terroristes à fort impact. En outre, la réponse immédiate à une attaque terroriste contre des infrastructures critiques peut prévenir les effets en cascade fréquemment associés à ces attaques.

Dans sa résolution 2341 (2017), le Conseil de sécurité a demandé au Comité contre le terrorisme (CCT), agissant avec le soutien de sa Direction exécutive, « d'examiner les efforts déployés par les États Membres pour protéger les infrastructures critiques contre les attaques terroristes dans le cadre de l'application de la résolution 1373 (2001), en vue de recenser les bonnes pratiques, les lacunes et les facteurs de vulnérabilité dans ce domaine. » Dans l'exécution de ce mandat, la Direction exécutive du Comité contribue à la réalisation d'évaluations et d'analyses, y compris sur les tendances en matière de lutte contre le terrorisme, qui seront mises en commun dans le cadre de cet important projet.[1]

Dans sa résolution 1373 (2001), le Conseil a aussi encouragé l'Équipe spéciale de lutte contre le terrorisme, qui relève du Bureau de lutte contre le terrorisme, le Groupe de travail sur la protection des infrastructures critiques y compris les cibles vulnérables, Internet et la sécurité du tourisme, et le Comité contre le terrorisme (agissant avec le concours de sa Direction exécutive) à continuer de coopérer afin de faciliter l'apport d'une assistance technique en matière de protection des

[1] Le Comité contre le terrorisme a tenu deux réunions publiques d'information sur ces questions : i) l'une sur la « Protection des infrastructures critiques dans le secteur du tourisme », tenue le 12 juin 2014 ; et ii) l'autre sur le « Renforcement des interventions d'urgence à la suite d'actes terroristes », tenue le 16 juin 2015. Le 21 novembre 2016, le Conseil de sécurité a consacré une réunion, organisée selon la formule Arria, à la protection des infrastructures critiques contre les attaques terroristes ; les États Membres y ont présenté leurs préoccupations et leurs points de vue sur les principaux volets de cette question.

infrastructures critiques contre les attaques terroristes et le renforcement des capacités dans ce domaine, en faisant œuvre de sensibilisation au problème, en particulier en se concertant davantage avec les États et les organisations internationales et régionales et en collaborant, notamment par des échanges d'informations, avec les prestataires d'assistance technique.

Dans la Stratégie antiterroriste mondiale des Nations Unies et dans le cadre du pilier II portant sur les mesures visant à prévenir et combattre le terrorisme, les États Membres se sont également dits déterminés « à s'employer avec l'ONU, sans nuire à la confidentialité, dans le respect des droits de l'homme et conformément aux autres obligations prévues par le droit international, à explorer les moyens : de coordonner les efforts aux échelles internationale et régionale afin de contrer le terrorisme sous toutes ses formes et manifestations sur l'Internet ; d'utiliser l'Internet comme un outil pour faire parade à la propagation du terrorisme, tout en reconnaissant que les États pourront avoir besoin d'une assistance à cet égard. »

Sous la présidence d'INTERPOL et du Bureau de lutte contre le terrorisme, le Groupe de travail sur la protection des infrastructures critiques y compris les cibles vulnérables, Internet et la sécurité du tourisme de l'Équipe spéciale de lutte contre le terrorisme a décidé d'élaborer un recueil de bonnes pratiques en matière de protection des infrastructures critiques contre les attaques terroristes. Le recueil, qui a été élaboré dans le cadre d'une « Initiative Unité d'action des Nations Unies », contribue à mieux faire connaître les dispositions de la résolution 2341 (2017). Le recueil propose aux États Membres et aux organisations internationales et régionales des directives et un catalogue de bonnes pratiques concernant la protection des infrastructures critiques contre les attaques terroristes (assortis d'indicateurs, de normes, d'instruments d'évaluation des risques, de recommandations, de bonnes pratiques, etc.). Il fournit également aux États Membres des documents de référence sur l'élaboration de stratégies visant à réduire les risques d'attentats terroristes contre les infrastructures critiques. Tout en gardant à l'esprit les différences qui existent entre les cadres conceptuel et normatif applicables aux « cibles vulnérables » et aux Infrastructures critiques, le recueil met en lumière les synergies possibles, dans la mesure où, très souvent, les mêmes organismes publics assument des responsabilités institutionnelles et opérationnelles dans ces deux domaines. En outre, il fournit aux États membres et aux organisations internationales et régionales des directives claires concernant l'élaboration et le renforcement de ces stratégies. Le recueil comporte des références et des indicateurs concernant la prévention, la préparation, l'atténuation des effets, les enquêtes, les interventions, le relèvement et d'autres concepts intéressant la protection des infrastructures critiques.

Hormis les dispositions de la résolution 2341 (2017) du Conseil de sécurité, l'application des différents éléments figurant dans le recueil s'inscrit dans le contexte de la résolution sur le sixième examen de la Stratégie antiterroriste mondiale des Nations Unies (A/RES/72/284), dans laquelle l'Assemblée Générale « invite tous les États Membres à collaborer avec le Centre des Nations Unies pour la lutte contre le terrorisme (les entités signataires du Pacte mondial de coordination contre le terrorisme) et à contribuer à l'exécution de ses activités au sein de l'Équipe spéciale, notamment en élaborant, finançant et réalisant des projets de renforcement des capacités de façon à intensifier et à systématiser la lutte contre le terrorisme à l'échelle nationale, régionale et mondiale. »

Ce recueil a été élaboré avec le concours de M. Stefano Betti, expert principal en justice pénale et en politiques en matière de criminalité, sous la direction de la Direction exécutive du Comité contre le terrorisme. La mise en œuvre du projet a été rendue possible grâce à un don généreux du Centre des Nations Unies pour la lutte contre le terrorisme.

Vladimir Voronkov
Secrétaire général adjoint chargé du Bureau de lutte contre le terrorisme
Directeur exécutif du Centre des Nations Unies pour la lutte contre le terrorisme

Michèle Coninsx
Sous–Secrétaire générale
Directrice exécutive
Direction exécutive du Comité contre le terrorisme

LA PROTECTION DES INFRASTRUCTURES CRITIQUES CONTRE LES ATTAQUES TERRORISTES – LE POINT DE VUE D'INTERPOL

Observations liminaires d'INTERPOL – Président du Groupe de travail sur la protection des infrastructures critiques y compris les cibles vulnérables, Internet et la sécurité du tourisme (Équipe spéciale de lutte contre le terrorisme)

Les infrastructures critiques représentent la logistique vitale de notre existence quotidienne. Nos sociétés reposent sur un réseau extrêmement complexe et perfectionné de systèmes infrastructurels. Les citoyens s'en remettent à des institutions et à des services en bon état de fonctionnement pour leur santé, leur sécurité et leur bien–être économique.

Cette logistique vitale est devenue plus efficiente et plus productive en raison des avancées technologiques, des échanges liés à la mondialisation et des exigences d'une population de plus en plus urbanisée. L'avènement de La vie 3.0 – l'imbrication entre le monde numérique et le monde physique – nous permet de surveiller et même de contrôler des infrastructures de partout dans le monde.

Toutefois, cette forte dépendance vis–à–vis de la connectivité en temps réel nous rend vulnérables aux menaces. L'interdépendance de nos infrastructures à travers les différents secteurs, entre les domaines virtuel et physique et au–delà des frontières nationales, signifie qu'une attaque serait lourde de conséquences.

L'attaque d'un seul point déficient pourrait se traduire par la perturbation ou la destruction de multiples systèmes vitaux dans le pays directement touché et avoir des répercussions à l'échelle mondiale. Il s'agit là d'une cible de choix pour ceux qui ont l'intention de nous nuire. Tout comme nos villes et nos infrastructures, leurs armes évoluent.

Des tactiques auxquelles il est fait appel dans des zones de conflit, telles que les actions simultanées de plusieurs tireurs fous, l'utilisation de véhicules blindés piégés, l'usage de gilets d'explosifs artisanaux, le piratage informatique ou le recours à des systèmes de drones portables chargés d'explosifs, pourraient être mises au point et utilisées dans les rues de nos villes et contre des installations de grande importance.

Comment pouvons–nous donc assurer la protection des organes indispensables de notre logistique vitale contre cette menace en constante mutation ?

On dira, pour faire court, qu'il s'agit d'inciter tous les acteurs concernés à se préparer à ces attaques, à les prévenir et à y faire face.

Ces exigences sous–tendent l'action que mène INTERPOL pour favoriser l'échange de renseignements, le renforcement des capacités et la résilience dans certains domaines critiques

Premièrement, nous mettons l'accent sur le renforcement de la sécurité des sites critiques en nous appuyant sur les normes et les procédures de préparation aux situations d'urgence.

Par exemple, l'Équipe des cibles vulnérables d'INTERPOL coopère avec nos pays membres en Afrique de l'Ouest au renforcement de la sécurité des laboratoires contenant des agents pathogènes dangereux et à leur protection contre les attaques terroristes. Ce projet, qui bénéficie

d'un financement généreux du Gouvernement canadien, vise l'élaboration de plans d'action en matière de biosécurité, qui s'appuient sur une action conjointe inter–organisations.

Deuxièmement, nous continuons d'exhorter les pays à protéger leurs frontières et à faire échec à la mobilité des terroristes.

INTERPOL a relevé qu'entre janvier 2017 et avril 2018, le nombre de profils de combattants terroristes étrangers accessibles en temps réel par l'intermédiaire de son système de documentation criminelle avait augmenté de 200 % et les échanges d'informations entre États Membres de 750 %.

Tout simplement sans précédent dans un domaine aussi sensible, l'appel lancé par le Conseil de sécurité a marqué un tournant.

Troisièmement, il importe de faire preuve de vigilance et de s'employer plus résolument à interdire un certain nombre de matériaux et d'outils avant qu'ils ne servent à produire la prochaine arme.

Dans ce contexte, INTERPOL coopère étroitement avec l'Agence internationale de l'énergie atomique en vue de limiter le trafic illicite des matériaux radiologiques et nucléaires en formant à la surveillance et à la détection et au moyen d'opérations transfrontières.

Enfin et surtout, INTERPOL encourage la coopération inter–organisations et internationale, qui a l'avantage de démultiplier les forces. Il est essentiel d'échanger les informations, de déceler les menaces immédiates et d'adopter les meilleures pratiques concernant l'identification des vulnérabilités, des méthodologies et des enseignements tirés.

Dans le domaine du maintien de l'ordre, nous avons nettement conscience de ce paradoxe tragique : un incident terroriste constitue souvent la meilleure occasion d'apprendre et d'apporter des améliorations. Partager ces enseignements au–delà des frontières, c'est recueillir des avantages sans avoir à en payer le coût. Tout le monde y gagne.

Ensemble, nous pouvons créer un dispositif mondial de sécurité, des infrastructures et des mécanismes d'intervention en cas d'urgence, en nous appuyant sur des expériences opérationnelles concrètes. Parallèlement, nous pouvons nous mettre à l'épreuve en mettant en scène des scénarios crédibles auxquels nous pourrions avoir à faire face à l'avenir.

À cette fin, INTERPOL organise des rencontres à l'intention d'experts qui représentent toutes les parties concernées. Notre Critérium sur la sécurité informatique, que nous avons conçu avec le concours de spécialistes du secteur privé, illustrent également la collaboration que nous entretenons avec les pays membres et les donateurs afin de nous préparer aux menaces, de les prévenir et de les combattre, qu'elles soient physiques ou informatiques ou qu'elles relèvent de ces deux domaines.

Dans un monde interdépendant, nous ne réussirons pas à protéger les infrastructures nationales en agissant isolément. C'est la raison pour laquelle les initiatives mondiales appuyées par l'Organisation des Nations Unies et INTERPOL et les mesures qui seront prises par la communauté internationale sont indispensables.

LISTE DES ABRÉVIATIONS

BLT	Bureau de lutte contre le terrorisme
CBRN	CBRN = chimique, biologique, radiologique et nucléaire.
Code ISPS	Code international pour la sûreté des navires et des installations portuaires
EEI	Engin explosif improvisé
EIIL	État islamique d'Iraq et du Levant
ISO	Organisation internationale de normalisation
MANPADS	Système portable de défense antiaérienne
OACI	Organisation de l'aviation civile internationale
OIAC	Organisation pour l'interdiction des armes chimiques
OMI	Organisation maritime internationale
OSCE	Organisation pour la sécurité et la coopération en Europe
PPP	Partenariat public–privé
TIC	Technologies de l'information et des communications
UIT	Union internationale des télécommunications
UNICRI	Institut interrégional de recherche des Nations Unies sur la criminalité et la justice

Tableaux

Études de cas

CADRE, OBJECTIFS ET MÉTHODOLOGIE

Le présent recueil aborde une question dont l'étude se trouve encore, essentiellement, à un stade embryonnaire. Particulièrement dopé par les avancées considérables qu'ont enregistrées les technologies de l'information et des communications, le rythme auquel les économies modernes se sont indissociablement liées au cours des deux dernières décennies expose nos sociétés à un ensemble de menaces et de vulnérabilités sans précédent. Nombre d'entre elles émanent de groupes terroristes qui cherchent à déstabiliser les communautés et à créer des situations de panique généralisée en s'en prenant aux moyens et aux dispositifs dont dépend la survie de nos sociétés. Ces moyens et ces dispositifs sont des éléments vitaux connus sous le nom d'« infrastructures critiques ».

La prise de conscience grandissante que nous nous trouvons désormais face à un nouveau type d'environnement en matière de sécurité n'a cependant pas donné lieu à l'adoption des niveaux requis de préparation. Pourtant, en s'attaquant récemment à des systèmes de transport et en se livrant à des actes de sabotage répétés contre des barrages, des oléoducs et des ponts, notamment, Al–Qaida et l'EIIL ont de nouveau rappelé la volonté soutenue des groupes terroristes de perturber les infrastructures critiques.

C'est dans ce contexte qu'a été adoptée la résolution 2341 (2017) du Conseil de sécurité, qui constitue le tout premier instrument mondial entièrement consacré à la protection des infrastructures critiques contre les attaques terroristes. Ses dispositions témoignent de la volonté renouvelée de la communauté internationale d'élaborer et de renforcer les mécanismes dont il faut disposer pour réduire autant que possible les risques d'attaques terroristes contre les infrastructures critiques et pour intervenir et se relever en cas d'attaque.

L'outil que constitue le présent recueil a été conçu pour appuyer une large gamme d'intervenants (responsables politiques, forces de l'ordre ou parties prenantes du secteur privé), qui sont chargés de concevoir, renforcer ou appliquer des politiques et des mesures destinées à protéger les infrastructures critiques contre les attaques terroristes, conformément aux dispositions de la résolution.

Il est organisé en unités thématiques qui suivent en gros la structure de la résolution. Chaque chapitre comporte en introduction un ou plusieurs paragraphes de la résolution et une analyse générale de la question ou des questions abordées. Le lecteur n'est pas réputé être préalablement averti des notions relatives aux infrastructures critiques. Cette démarche se fonde sur le constat que la question de la protection des infrastructures critiques est une donnée relativement nouvelle dans le débat consacré, à l'échelle mondiale, aux politiques publiques.

L'examen des difficultés d'ordre pratique ou juridique sous–jacentes s'appuie sur les solutions qu'ont adoptées ou pourraient adopter un certain nombre de d'États et d'organisations. Le recueil adopte une démarche pragmatique qu'illustre la richesse des études de cas, qui fournissent des exemples concrets et différentes possibilités d'application. Un certain nombre de tableaux offrent aux pays la possibilité de comparer rapidement les mesures adoptées par d'autres pays et, à terme,

d'adopter en les adaptant à celles qui correspondent le mieux à leur propre contexte institutionnel, dans le cadre des dispositions énoncées par la résolution.

S'il donne la priorité à la protection des infrastructures critiques contre les attaques terroristes, le recueil rend également compte du fait qu'un certain nombre de pays ont choisi d'adopter des stratégies globales intégrées, qui prennent en compte la nécessité de renforcer la résilience des infrastructures critiques vis–à–vis de tous les risques, qu'ils soient d'origine humaine ou naturelle. Le recueil offre donc les outils conceptuels qui permettront aux pays d'adopter, s'ils le souhaitent, des stratégies globales portant une attention particulière à la menace terroriste, ainsi que les mécanismes appropriés d'évaluation et d'atténuation des risques.

Conformément à l'esprit de la résolution 2341 (2017), le recueil traite de la protection des infrastructures critiques, sans privilégier un type donné d'infrastructures. La démarche transversale adoptée vise à mettre en lumière les principes, les méthodes et les processus communs que les pays sont encouragés à traduire en stratégies, en plans d'action et en mesures intéressant des domaines précis. Dans le même temps, des exemples de mesures d'atténuation sectorielles sont fournis dans tout le document. Par ailleurs, on trouvera au chapitre 9 un aperçu des principales initiatives prises par de grands organismes internationaux dans certains secteurs.

Enfin, hormis les orientations qu'il propose aux pays, le recueil souscrit au principe d'une prise en compte adéquate et effective des questions relatives aux droits de l'homme dans l'ensemble des mesures et des stratégies de protection des infrastructures critiques.

1. COMPRENDRE LES DÉFIS

Résolution 2341 (2017) du Conseil de sécurité
Paragraphe 2

> *Le Conseil de sécurité [...]*
>
> *Engage tous les États à faire des efforts concertés et coordonnés, notamment par l'intermédiaire de la coopération internationale, pour mener des activités de sensibilisation et faire mieux connaître et comprendre les défis posés par les attaques terroristes, de façon à être mieux préparés en cas d'attaque contre des infrastructures critiques*.

1.1 Le terrorisme en tant que menace visant spécifiquement les infrastructures critiques

Si les infrastructures critiques sont exposées à des risques très divers, tels que les catastrophes naturelles, l'erreur humaine, les défaillances techniques et les actes délictueux pris au sens large, l'apparition du domaine d'intervention spécifique que constitue leur protection résulte directement des événements du 11 septembre.

Au cours de ces dernières décennies, les terroristes se sont manifestement intéressés aux infrastructures critiques, considérées comme des cibles potentielles pour la promotion de leurs objectifs. Déjà en 2002, il apparaissait clairement qu'Al–Qaida cherchait à exploiter les vulnérabilités des équipements collectifs publics et privés des États–Unis. La découverte, en Afghanistan, d'un ordinateur contenant des logiciels d'analyse structurale de barrages a conduit le National Infrastructure Protection Centre (Centre national de protection des infrastructures) des États–Unis à diffuser un bulletin d'avertissement (NIPC 2002).

On notera surtout que pratiquement aucun secteur n'a échappé aux activités terroristes ou, à tout le moins, à une attention soutenue de la part des groupes terroristes. Les exemples abondent. Dans le secteur des transports, on compte, parmi les événements récents, les attaques perpétrées simultanément en 2016 contre l'aéroport et le métro de Bruxelles par deux équipes de l'EIIL. En tout, 32 personnes ont été tuées et quelque 300 blessées.

Le secteur de l'énergie a été la cible d'une activité terroriste soutenue, concrétisée par des attaques perpétrées par Al–Qaida et ses associés contre les installations et le personnel de compagnies pétrolières en Algérie, en Arabie saoudite, en Iraq, au Koweït, au Pakistan et au Yémen.

D'importantes infrastructures d'eau ont particulièrement été visées par l'EIIL. Entre 2013 et 2015, l'EIIL a lancé quelque 20 attaques de grande envergure contre des cibles en Syrie et en Iraq. Outre la destruction de canalisations, de ponts et d'usines d'assainissement, l'EIIL s'est stratégiquement servi des infrastructures d'eau, par exemple en fermant des barrages et en interrompant l'approvisionnement en eau (Vishwanath 2015).

Dans certains cas, des attaques ont été tentées contre des infrastructures qui contenaient des matières dangereuses. Le 26 juin 2015, près de Lyon, un individu a précipité une voiture dans une

usine de produits chimiques contre des bonbonnes de gaz, provoquant une explosion. En 2016, deux centrales nucléaires ont été fermées en Belgique, l'EIIL ayant alors été soupçonné de vouloir attaquer, infiltrer ou saboter les installations pour se procurer des matières nucléaires ou radioactives.

Si des infrastructures critiques n'ont pas encore subi d'attaques massives entraînant des répercussions ou des défaillances en chaîne, le risque d'un tel scénario reste très présent et exige des pays qu'ils se dotent de plans de prévention et d'intervention appropriés. De fait, les actes terroristes perpétrés à ce jour ont mis à nu les vulnérabilités intrinsèques d'un certain nombre d'infrastructures critiques. Par ailleurs, ce qui se profile à l'horizon, c'est la possibilité que de nouvelles générations de terroristes se familiarisent de plus en plus avec les technologies de l'information et des communications (TIC). On peut soutenir que les cyber–attaques terroristes, qui ne se sont pas encore matérialisées, sont désormais plus susceptibles de se produire en raison de la progression des niveaux de « savoir–faire » dans le domaine des TIC. D'après le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, « le risque que les technologies de l'information et des communications soient utilisées à des fins terroristes dans le cadre d'autres activités que le recrutement, le financement, l'entraînement et l'incitation au terrorisme, notamment contre des systèmes qui utilisent ces technologies ou contre des infrastructures qui en dépendent, augmente. Si l'on ne s'attaque pas à ce problème, il pourrait menacer la paix et la sécurité internationales » (A/70/174, par. 6).

1.2 Infrastructures critiques et cibles vulnérables

La notion de « cibles vulnérables » est généralement associée à des lieux très fréquentés, tels que les musées, les cinémas, les lieux de culte ou les centres commerciaux, par opposition aux cibles dites « difficiles » qui, dans l'ensemble, bénéficient de niveaux de protection élevés, souvent en raison de la présence de gardes armés ou du fait que l'accès du public est restreint ou soumis à des contrôles stricts (c'est le cas, par exemple, des ambassades, des aéroports ou des installations militaires).

Comme l'ont montré les attaques récemment perpétrées dans des zones piétonnes à Nice et à Barcelone, au marché de Noël de Berlin et dans d'autres lieux, le caractère ouvert des cibles vulnérables et la très grande facilité d'accès à ces lieux les rendent particulièrement vulnérables aux attaques terroristes. Dans le même temps, les cibles vulnérables se prêtent d'une manière idéale à des attaques qui, sans grande planification, permettent d'infliger des pertes considérables.

Dans cet ordre d'idées, le Conseil de sécurité, par sa résolution 2396 (2017), a spécifiquement pris acte du danger que les combattants terroristes étrangers liés à l'EIIL et revenus des zones de conflit font peser en planifiant et en perpétrant des attaques contre des cibles vulnérables

Si les deux notions – infrastructures critiques et cibles vulnérables – se recoupent par endroits, leur définition et l'élaboration des stratégies de protection connexes incombant à chaque pays, elles ne sont pas substituables l'une à l'autre. La question de la « criticité » est un facteur clef de distinction. Une cible vulnérable ne revêt pas nécessairement une importance critique au regard

de la prestation de services essentiels à la société. Qui plus est, si une cible vulnérable peut consister en une infrastructure (par exemple, un stade), il n'en est pas toujours ainsi (c'est le cas d'un rassemblement de personnes dans un square, à l'occasion d'un concert en plein air). En dépit de ces différences conceptuelles, les pays sont invités, à la section 2.3.1 du Recueil, à envisager d'établir des synergies entre les deux notions, dans le cadre des politiques qu'ils élaborent pour lutter contre le terrorisme.

1.3 Menaces terroristes visant spécifiquement les infrastructures critiques

Les menaces terroristes qui visent les infrastructures critiques ont de multiples dimensions. Les sections suivantes décomposent ces menaces en fonction de leur nature (physique ou cybernétique), de leur origine (interne ou externe) et du contexte dans lequel elles surviennent (cibles isolées ou multiples). Comme on l'a vu au chapitre 2, la compréhension des différents types de menaces auxquelles sont exposées les infrastructures critiques constitue une première étape sur la voie de l'élaboration de stratégies de protection adéquates.

1.3.1 Menaces physiques et cyber–menaces

Les menaces physiques qui ciblent les infrastructures critiques peuvent prendre différentes formes. Elles ont pour caractéristique commune de chercher à détruire une infrastructure, à l'affaiblir ou à la rendre totalement ou partiellement inopérante en intervenant, par exemple, sur sa structure physique ou ses composants mécaniques.

Les menaces physiques les plus intuitives qui visent les infrastructures critiques font appel à l'utilisation d'explosifs ou d'engins incendiaires, de moyens de transport, de roquettes, de systèmes portables de défense antiaérienne (MANPADS), de grenades et même d'outils simples (par exemple, des allumettes ou des briquets utilisés pour allumer des incendies criminels), notamment, l'objectif étant de provoquer l'effondrement total ou partiel ou la destruction d'une infrastructure. Les attaques peuvent également se matérialiser par une modification ou une manipulation intentionnelle des systèmes de fonctionnement des infrastructures critiques (que sont, par exemple, la mise en marche et l'arrêt des installations, l'ouverture et la fermeture des systèmes de tuyauterie ou la suppression des systèmes de signalisation des processus, des signaux de défaillance ou des alarmes). Le déploiement d'armes ou de substances chimiques, biologiques, radiologiques ou nucléaires constitue aussi un type particulier de menace pour les infrastructures critiques. Il peut aller de la propagation d'agents pathogènes infectieux dans les chaînes d'approvisionnement alimentaire et les conduites d'eau, par exemple, à l'utilisation de gaz toxiques dans des carrefours de grande fréquentation. Il convient également de noter que l'attaque d'une installation critique contenant des matières chimiques, biologiques, radiologiques ou nucléaires pourrait aussi entraîner la libération de ces matières.

Bien que différentes de par leur nature, les cybermenaces et les menaces physiques peuvent, en définitive, produire les mêmes résultats. Les cybermenaces, qui sont variables, peuvent donner lieu à des attaques consistant, par exemple, à :

- manipuler des systèmes ou des données – c'est le cas des logiciels malveillants qui exploitent les vulnérabilités des logiciels informatiques et des composants matériels nécessaires au fonctionnement des infrastructures critiques ;
- interrompre des systèmes vitaux – cas des attaques par saturation[2] ;
- restreindre l'accès à des systèmes ou à des informations d'importance vitale – par exemple en recourant à des logiciels rançonneurs.

Comme indiqué à la section 2.4.2, si les systèmes de contrôle informatisés interconnectés et intégrés ont considérablement rationalisé le mode de fonctionnement des infrastructures critiques et dégagé des gains d'efficience sur le marché, l'extension de la connectivité peut également élargir la surface d'attaque et exposer ces infrastructures à un risque élevé de manipulation.

Dans une enquête menée en 2010 auprès de 200 cadres du secteur privé de l'électricité de 14 pays, près de la moitié des personnes interrogées ont déclaré qu'elles n'avaient jamais dû faire face à des attaques par saturation ou à des infiltrations de réseau à grande échelle. En 2011, la situation avait considérablement évolué : 80 % des personnes interrogées avaient dû affronter une attaque par saturation à grande échelle, tandis que 85 % avaient été victimes d'infiltrations de réseaux (McAfee 2011, p. 6).

Tableau 1 : les 10 principales menaces qui pèsent sur les systèmes de contrôle industriels

N°	Menace	Explication
1	Utilisation non autorisée de points d'accès de télémaintenance	Les points d'accès pour la maintenance sont des entrées externes au réseau des systèmes de contrôle industriels, intentionnellement créées et souvent insuffisamment sécurisées.
2	Attaques en ligne via les réseaux des bureaux ou des entreprises	Pour la connexion aux réseaux, les systèmes informatiques des bureaux utilisent généralement plusieurs canaux. Dans la plupart des cas, puisqu'il existe également des connexions réseau entre les bureaux et les systèmes de contrôle industriels, les auteurs des attaques peuvent se créer un accès par cette voie.
3	Attaques contre des composants standards utilisés dans les réseaux des systèmes de contrôle industriels	Les composants informatiques standards, tels que les logiciels d'exploitation, les serveurs d'applications ou les bases de données comportent souvent des failles ou des vulnérabilités qui peuvent être exploitées par les pirates. Si ces composants standards sont également utilisés dans le réseau des systèmes de contrôle industriels, le risque d'une attaque réussie contre ce réseau augmente.
4	Attaques par saturation	Les attaques par saturation peuvent nuire aux connexions réseau et aux ressources vitales et provoquer des pannes de systèmes, l'objectif consistant, par exemple, à perturber le fonctionnement d'un système de contrôle industriel.

[2] L'attaque perpétrée, le 14 mai 2018, contre la billetterie des chemins de fer danois est un exemple récent d'attaque par saturation visant des infrastructures critiques.

5	Erreur humaine et sabotage	Les actes intentionnels – qu'ils soient le fait d'acteurs internes ou externes– constituent une menace considérable pour touts les objectifs des mesures de protection. La négligence et l'erreur humaine constituent également des menaces importantes, notamment au regard des objectifs de la protection que sont la confidentialité et la disponibilité.
6	Introduction de logiciels malveillants via des supports amovibles et du matériel externe	L'utilisation de supports amovibles et de composants informatiques mobiles par le personnel externe comporte toujours un risque élevé d'infection par des logiciels malveillants.
7	Lecture et inscription d'informations dans le réseau des systèmes de contrôle industriels	Dans la mesure où la plupart des composants de contrôle utilisent actuellement des protocoles en texte clair, les communications ne sont pas protégées. Il est ainsi relativement facile de lire et d'introduire des commandes de contrôle.
8	Accès non autorisé aux ressources	La tâche s'avère particulièrement aisée pour les auteurs d'attaques internes ou ceux qui mènent des attaques après une première pénétration d'origine extérieure si les services et les composants du processus réseau ne font pas appel à des méthodes d'authentification et d'autorisation ou si les méthodes mises en place ne sont pas sécurisées.
9	Attaques contre des composants standard	Les auteurs d'attaques peuvent manipuler les composants d'un réseau, par exemple pour effectuer des attaques de l'intercepteur ou pour faciliter le reniflage réseau.
10	Dysfonctionnements techniques ou cas de force majeure **Source** : OSCE 2013, p. 34	Les coupures de courant provoquées par des conditions météorologiques extrêmes ou des défaillances techniques peuvent survenir à tout moment – dans de tels cas, on peut seulement limiter autant que faire se peut les risques et les dommages potentiels.

1.3.2 Menaces internes et menaces externes

Si la protection des infrastructures critiques contre les attaques extérieures bénéficie d'un volume considérable de directives de la part d'organismes nationaux et internationaux de réglementation, les menaces que font peser les acteurs internes se voient accorder une moins grande attention. Par rapport aux acteurs extérieurs, qui ne peuvent avoir accès aux infrastructures critiques que par la violence ou par des stratagèmes, les auteurs internes jouissent d'avantages incontestables. Il s'agit souvent d'employés ou de fournisseurs de ces entreprises, qui peuvent être les principaux conspirateurs ou agir comme complices (par exemple, en qualité d'informateurs) d'acteurs extérieurs. Ils sont souvent en mesure d'observer pendant un certain temps les processus sans être dérangés. Leurs connaissances (ou la facilité avec laquelle ils peuvent acquérir des connaissances) relatives aux installations pertinentes peuvent être facilement exploitées à des fins criminelles.

Dans cette optique, les méthodes d'évaluation des risques qui pèsent sur des sites spécifiques devraient tenir compte de chaque fonction au sein du système et les vulnérabilités liées aux acteurs internes ne devraient pas être considérées comme relevant d'une catégorie distincte. En lieu et place, il convient d'examiner les différents types de menaces en incluant, dans chaque catégorie, un élément « acteur interne ». Par exemple, lorsqu'ils examinent une catégorie de menace telle que celle d'un engin explosif artisanal porté par une personne et utilisé pour attaquer un aéronef, les

responsables de l'évaluation devraient analyser, séparément, le cas d'un engin explosif artisanal porté par un passager et celui d'un engin explosif artisanal introduit par l'équipage ou par des employés.

La section 2.8 donne quelques exemples de mesures destinées à protéger les infrastructures critiques contre ce type de menace. Dans ce domaine, les exploitants de ces infrastructures peuvent jouer un rôle préventif clef en commençant par appliquer des procédures efficaces de contrôle préalable et de sélection du personnel.

1.3.3 Cibles isolées et cibles multiples

Les menaces qui pèsent sur les infrastructures critiques peuvent, soit se traduire par des actes isolés et sporadiques, soit s'inscrire dans le cadre de plans de plus grande envergure visant à attaquer des infrastructures qui font partie d'un même secteur (par exemple, des centrales nucléaires), appartiennent à un même propriétaire ou exploitant ou sont situées dans une même zone géographique. On peut très bien placer les actions terroristes ciblant les infrastructures critiques sur le même plan que l'espionnage industriel, qui conduit souvent à lancer des cyberattaques sous la forme de « campagnes » ou d'attaques en série. Par exemple, en 2011, l'attaque dite « LURID » a notamment visé les systèmes informatiques d'un certain nombre de missions diplomatiques et d'agences spatiales gouvernementales.

L'identification des tendances présentes dans des scénarios similaires exige souvent des outils analytiques puissants et le traitement d'informations provenant de sources multiples et hétérogènes. Pour compliquer davantage les choses, comme le souligne l'OSCE en ce qui concerne le secteur de l'énergie, la plupart des cyberattaques ne sont pas rendues publiques parce que les exploitants concernés sont réticents à faire connaître ces incidents. Néanmoins, la capacité de reconnaître le plus tôt possible la dynamique et les méthodes sous–jacentes contribue de façon déterminante à ce que les autorités responsables puissent échanger des informations en temps réel, ce qui donne davantage de moyens pour réagir plus efficacement aux attaques en cours et pour anticiper les attaques imminentes susceptibles de provoquer des victimes (OSCE, 2013).

Dans certains cas, ce qui peut sembler être une attaque isolée visant des cibles relativement « sans importance » est en réalité susceptible de faire partie de stratégies criminelles plus ambitieuses et en constante évolution.[3]

[3] Selon un rapport conjoint du Département de la sécurité du territoire et du Bureau d'enquête fédéral (FBI), publié en 2017, certains réseaux du gouvernement des États–Unis dans les secteurs de l'énergie, du nucléaire, de l'eau, de l'aviation et dans des branches critiques de la fabrication étaient la cible de menaces persistantes et sophistiquées. Pour le Département de la sécurité du territoire, il s'agissait d'une « campagne d'intrusion en plusieurs étapes menée par des acteurs qui cherchaient à se frayer un accès via des réseaux de faible sécurité et des réseaux de petite taille pour ensuite se déplacer latéralement vers des réseaux représentant des actifs de grande valeur dans le secteur de l'énergie ». D'après le rapport, les auteurs de la menace poursuivaient activement leurs objectifs ultimes dans le cadre d'une campagne à long terme, des entreprises comme des fournisseurs tiers étant initialement ciblées pour devenir ensuite des rampes de lancement. (Voir : EDS, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, 20 octobre 2017, à l'adresse suivante : www.us–cert.gov/ncas/alerts/TA17–293A. Voir également : Conner Forrest, « DHS, FBI warn of cyberattacks targeting energy infrastructure, government entities », 23 octobre 2017, TechRepublic, à l'adresse www.techrepublic.com/article/dhs–fbi–warn–of–cyberattacks–targeting–energy–infrastructure–government–entities).

1.4 Les motivations des attaques terroristes visant les infrastructures critiques

En raison du caractère hétérogène des infrastructures critiques et aussi de la diversité de leurs cadres géographique et institutionnel, il apparaît extrêmement difficile de tirer des conclusions générales sur ce qui motive les terroristes à commettre des attentats contre ces infrastructures plutôt que contre des cibles non critiques. Il reste que l'analyse des motivations terroristes pourrait suggérer des pistes utiles dans le cadre des évaluations globales de la menace qu'exigent les stratégies nationales de protection des infrastructures critiques.

La recherche empirique limitée menée dans ce domaine (Ackerman, 2007) révèle que, pour diverses raisons, les infrastructures critiques présentent un certain attrait. Premièrement, elles peuvent constituer des cibles intéressantes en raison de leur valeur stratégique pour les sociétés, en particulier celles des pays hautement industrialisés de l'hémisphère occidental. Perturber le fonctionnement d'une infrastructure critique, de préférence en provoquant des réactions en chaîne, permet aux terroristes de maximiser les dégâts lors d'une seule opération et d'insuffler la peur à des niveaux qu'ils ne pourraient pas atteindre aussi aisément en attaquant des cibles « ordinaires ». Dans le même ordre d'idées, des agents d'Al–Qaïda auraient passé beaucoup de temps à surveiller les sièges de différentes sociétés financières et organisations internationales basées aux États–Unis. On peut soutenir que cette activité méticuleuse faisait suite à l'édit de 2001 d'Oussama ben Laden ; qui exhortait ses adeptes à « s'attacher à porter des coups à l'économie américaine par tous les moyens possibles ».

D'autres infrastructures critiques peuvent être ciblées pour démontrer l'impuissance des institutions étatiques. Par exemple, des organisations terroristes peuvent décider d'attaquer des centrales électriques ou des oléoducs afin d'interrompre la fourniture de services de base et de mettre en lumière la fragilité des organismes publics et des politiques gouvernementales (Ackerman 2007, p. 170).

Une troisième motivation possible, liée aux deux précédentes, serait la volonté d'atteindre un niveau de publicité supérieur à celui que l'on pourrait viser en se concentrant sur des cibles de faible visibilité.

Paradoxalement, les terroristes peuvent chercher à contrôler des infrastructures critiques non pas pour causer des dommages ou pour intimider, mais pour des motifs tout à fait opposés, à savoir asseoir leur légitimité ou assurer leur acceptabilité sociale. Comme on l'a noté, si la plupart des opérations menées par l'ISIL en rapport avec des infrastructures liées à l'eau visaient à perturber les mouvements des troupes et à combattre les forces armées, « ces actions présentaient souvent aussi l'avantage supplémentaire de promouvoir les recrutements ; en facilitant l'écoulement de l'eau vers des villes acquises à la cause de l'État islamique ou même en améliorant tout simplement la prestation des services de base, le groupe pourrait attirer davantage d'hommes et de femmes dans ses rangs » (Vishwanath 2015).

Dans plusieurs cas, il existe probablement une combinaison de facteurs qui incitent les groupes terroristes à perpétrer des attentats contre des infrastructures critiques. Ces incitations sont contrebalancées par un certain nombre de contraintes. La décision finale quant au choix de

l'infrastructure à cibler dépendra des capacités opérationnelles dont dispose un groupe pour lancer une attaque donnée. Les mesures de protection mises en place dans une infrastructure critique donnée influeront naturellement sur cette décision. Il n'en découle pas que les terroristes attaqueront une infrastructure critique seulement lorsqu'ils seront sûrs de pouvoir perturber son fonctionnement. Une simple tentative, même si elle échoue ou si elle cause des dommages très limités, peut offrir le retentissement médiatique souhaité, particulièrement lorsque la cible est choisie pour sa valeur symbolique.

1.5 Lutter contre les menaces terroristes qui visent les infrastructures critiques en s'appuyant sur une démarche fondée sur les droits de l'homme

Le terrorisme remet sérieusement en question les éléments fondamentaux de l'état de droit, la protection des droits de l'homme et leur application effective. Dans le cadre des obligations qui leur incombent en vertu du droit international des droits de l'homme, les États ont le devoir de protéger les personnes relevant de leur juridiction contre toute atteinte à leurs droits fondamentaux par des tiers, y compris des acteurs terroristes. Cette obligation revêt une importance particulière, compte tenu de l'impact potentiel que les attaques visant les infrastructures critiques peuvent avoir sur les populations, étant donné le rôle que ces infrastructures jouent souvent dans le maintien ou la réalisation de fonctions sociétales vitales. La perturbation ou la destruction d'infrastructures critiques ou les dommages qui leur sont infligés peuvent avoir des répercussions considérables sur un large éventail de droits de l'homme, allant du droit à la vie et à la sécurité de la personne au droit à la santé et à un environnement sain, au droit à l'éducation, à l'eau, à l'assainissement et à d'autres aspects du droit à un niveau de vie décent.

Le devoir des États de protéger les droits de l'homme comporte l'obligation de prendre les mesures nécessaires et adéquates pour prévenir, combattre et punir les activités qui mettent en danger ces droits, telles que les menaces à la sécurité nationale ou les crimes violents, notamment le terrorisme. À cet égard, les États devraient être guidés, notamment, par la Stratégie antiterroriste mondiale des Nations Unies, selon laquelle lutter effectivement contre le terrorisme et veiller au respect des droits de l'homme ne sont pas des objectifs antagoniques mais plutôt des objectifs complémentaires et synergiques. En effet, la promotion et la protection des droits de l'homme constituent un pilier indépendant et une nécessité transversale garants de la mise en œuvre effective des quatre composantes de la Stratégie antiterroriste mondiale. En outre, les dispositions pertinentes des résolutions du Conseil de sécurité exigent que toute mesure prise pour prévenir et combattre le terrorisme soit conforme aux obligations qui incombent aux États en vertu du droit international, en particulier du droit international des droits de l'homme, du droit des réfugiés et du droit international humanitaire.

Dans l'intérêt de la lutte contre les menaces terroristes qui pèsent sur les infrastructures critiques, les autorités étatiques peuvent prendre temporairement des mesures qui se traduisent par la limitation de certains droits, à condition que ces restrictions soient conformes aux conditions énoncées dans le droit international des droits de l'homme. Les mesures prises dans ce cadre doivent véritablement répondre à la menace visée, être adaptées aux exigences de la situation, avoir une base juridique claire et être nécessaires et proportionnées, de manière à apporter une

réponse efficace. Les États doivent donc veiller à ce que des garanties satisfaisantes soient mises en place pour protéger les droits de l'homme de toute ingérence arbitraire et disproportionnée. Pour s'acquitter effectivement de ces obligations, les États sont vivement encouragés à procéder régulièrement à des évaluations des mesures prises pour lutter contre la menace terroriste qui pèse sur les infrastructures critiques et à veiller à ce que ces mesures soient fondées sur des données factuelles et, par conséquent, efficientes.

2. ÉLABORER DES STRATÉGIES NATIONALES VISANT À RÉDUIRE LES RISQUES POSÉS AU REGARD DES INFRASTRUCTURES CRITIQUES

Résolution 2341 (2017) du Conseil de sécurité
Paragraphe 2

La résolution du Conseil de sécurité [...]

Demande aux États d'envisager d'élaborer des stratégies de réduction des risques posés par les attaques terroristes au regard des infrastructures critiques, ou d'améliorer celles qu'ils ont déjà en place, en prévoyant notamment d'évaluer et de faire mieux connaître les risques, de prendre des mesures de préparation, y compris pour intervenir de manière efficace en cas d'attaque, de favoriser une meilleure interopérabilité dans la gestion de la sécurité et des conséquences, et de faciliter des échanges fructueux entre toutes les parties prenantes concernées.

2.1 Pourquoi une stratégie nationale ?

La plupart des pays ont prévu des mesures de sûreté et de sécurité pour leurs infrastructures critiques bien avant que la protection des infrastructures critiques ne devienne un domaine politique à part entière. Les mesures de protection ont été adoptées pour la plupart de façon progressive et fragmentaire sous la forme de règlements couvrant des secteurs ou des menaces spécifiques, ou se concentrant sur certaines parties des processus de gestion des risques. Il arrivait que les politiques des États atteignent un niveau de sophistication considérable et se conforment aux normes internationales les plus élevées. C'est ainsi que dans le secteur de l'énergie nucléaire, après la fin de la guerre froide, l'Ukraine a mis au point un système moderne et efficace de protection physique des installations et matières nucléaires.

On peut donc se demander pourquoi les pays devraient définir des stratégies générales de protection de leurs installations critiques à l'échelle nationale alors qu'ils ont souvent déjà mis en place des règlements, des politiques et des pratiques détaillés couvrant la plupart, sinon la totalité, des secteurs critiques. La raison la plus impérieuse est que, dans les sociétés modernes, la protection des infrastructures essentielles est une tâche de plus en plus transversale. L'interdépendance des secteurs, alliée au risque d'effets en cascade en cas d'accidents (qu'ils soient d'origine naturelle ou humaine), rend la capacité d'« avoir une vue d'ensemble de la situation » nécessaire pour pouvoir coordonner efficacement les mesures de prévention, d'intervention et de relèvement entre les secteurs. En outre, le recours à des approches purement sectorielles ou « verticales » semblerait multiplier inutilement les agences impliquées, causer des chevauchements d'activités et entraîner un gaspillage des ressources. Une stratégie globale vise par conséquent à rationaliser les flux de travail, à réaliser des « économies d'échelle » et à mieux répartir les ressources financières et humaines autour d'un ensemble d'objectifs prédéfinis.

Cela ne veut pas dire que les stratégies nationales de protection des infrastructures critiques devraient automatiquement remplacer les mesures de protection sectorielles existantes, surtout lorsque ces mesures se sont révélées efficaces ou conformes aux cadres réglementaires internationaux contraignants. Ce qu'il faut, cependant, c'est que les pays regroupent les différents

éléments de la mosaïque dans un cadre commun et les intègrent dans un système cohérent de gouvernance. La protection des installations critiques étant liée à plusieurs domaines d'activité (tels que la politique énergétique, la politique des transports, la politique de sécurité, etc.), les principaux objectifs d'une stratégie à l'échelle nationale consistent à :

- Définir les structures organisationnelles ;
- Établir des objectifs et des échéanciers mesurables ;
- Jeter les bases d'une prévention et d'une gestion efficaces des incidents grâce à l'harmonisation des tâches entre les différents domaines politiques.

Dans cette optique, les stratégies de protection des infrastructures critiques peuvent être adaptées aux besoins et aux approches spécifiques de chaque pays. Comme le montre la section 2.5, les pays ont adopté divers modèles institutionnels reflétant non seulement leurs traditions juridiques propres, mais aussi des attitudes culturelles différentes à l'égard du rôle du droit dans la société, de la relation entre le gouvernement, les citoyens et le secteur privé.

Les pays disposent d'une marge de manœuvre considérable pour déterminer les modalités de protection de leurs infrastructures critiques. Toutefois, ils doivent tous avoir en place les éléments conceptuels de base (une stratégie) pour faire le lien et assurer des relations de travail harmonieuses entre tous les acteurs concernés.

2.2 Approches tous risques par rapport aux approches à risques spécifiques

Les infrastructures critiques sont soumises à des types de menaces polymorphes. Ces menaces peuvent être naturelles : le 11 mars 2011, par exemple, un tremblement de terre suivi d'un tsunami a provoqué un accident nucléaire majeur à Fukushima, au Japon.

Les menaces peuvent trouver leur origine dans un comportement humain négligent : en 2006, une panne de courant a touché dix millions de personnes en Europe suite à l'action d'un opérateur de l'approvisionnement en électricité qui avait mis hors tension un câble électrique à travers la rivière Ems pour laisser passer un bateau de croisière.

D'autres menaces peuvent être motivées par des buts liés au terrorisme ou d'autres objectifs criminels. Les cyberattaques contre rançon sont un exemple d'activités lucratives qui peuvent gravement toucher les infrastructures critiques en chiffrant les données des utilisateurs et en exigeant un paiement en échange du déblocage des données. Les menaces qui pèsent sur les infrastructures critiques peuvent également être liées au comportement criminel de manière plus subtile et indirecte. En Europe, la Fédération française du bâtiment a mis en garde à plusieurs reprises contre l'implication de réseaux criminels dans le trafic de matériaux contrefaits et de qualité inférieure utilisés dans la construction de bâtiments. Selon certaines sources, de nombreuses entreprises du secteur du bâtiment achètent des matériaux non conformes et de mauvaise qualité qui affectent la solidité des infrastructures et les exposent à un risque d'effondrement plus élevé.

Vu que les pays sont appelés à protéger leurs infrastructures critiques contre de multiples niveaux de risque, une des questions clefs est la suivante : les gouvernements doivent–ils adopter un plan unique couvrant toutes les menaces possibles, ou plutôt envisager d'adopter des stratégies spécifiques aux dangers/risques ? En principe, l'une ou l'autre approche est conforme au cadre juridique international.

Parmi les pays qui ont adopté des stratégies de protection des infrastructures critiques, la majorité suit une approche tous risques[4]. Cela signifie que les objectifs stratégiques et les structures organisationnelles sont conçus de manière à tenir compte des menaces accidentelles, intentionnelles et naturelles auxquelles sont exposées les infrastructures critiques de manière globale. Une approche tous risques est souvent considérée comme la condition préalable permettant de tirer le meilleur parti des modestes ressources disponibles et d'éviter les doubles emplois inutiles. La logique qui sous–tend cette démarche est que les mêmes processus de gestion des risques et de collaboration ainsi que les mêmes mécanismes d'intervention en cas de crise peuvent être largement utilisés pour répondre à tous les types de menaces de manière indistincte. Les approches tous risques sont appliquées par des pays comme le Canada et le Royaume–Uni.

D'autres pays adoptent une approche mixte. L'Australie, par exemple, a élaboré des directives spécifiques sur la protection des infrastructures critiques contre les attaques terroristes. Ces lignes directrices complètent la stratégie générale du pays en matière de protection d'infrastructures critiques, qui étend sa portée à d'autres dangers. En Espagne, l'architecture institutionnelle de protection des infrastructures critiques est définie dans la loi 8/2011 « établissant les mesures prévues à cet effet ». Contrairement à d'autres pays, la loi espagnole est axée sur la lutte contre la menace terroriste, bien qu'elle s'applique à d'autres risques (non spécifiés).

L'impératif énoncé dans la résolution 2341(2017) du Conseil de sécurité est que la menace terroriste se reflète pleinement et de toute urgence dans l'élaboration des plans stratégiques des gouvernements visant à protéger les infrastructures critiques. Cela étant, chaque pays est libre de déterminer, dans le cadre de sa politique nationale, les meilleures formes et modalités de protection des infrastructures critiques contre les actes terroristes dans un environnement à menaces multiples.

2.3 Stratégies de protection des infrastructures critiques par rapport aux autres politiques nationales

La plupart des pays, y compris ceux qui ne se sont pas dotés de stratégies propres en matière de protection des infrastructures critiques, abordent les questions qui s'y rapportent dans divers instruments politiques adoptés par différents organismes gouvernementaux. Ces documents comprennent généralement des stratégies et des politiques nationales (notamment en matière de cybersécurité) axées sur la lutte contre le terrorisme. Bien que ces diverses politiques aient pu être adoptées à des moments différents et par plusieurs organismes publics, il est essentiel qu'elles

[4] Dans le contexte de l'aviation, l'OACI utilise le terme « dangers » pour désigner les questions liées à la sécurité. Les événements liés à la sécurité sont plus précisément définis comme des «accidents».

deviennent toutes partie intégrante d'une approche et d'un message cohérents lié à la protection des infrastructures critiques. Il faut, particulièrement pour cela, que les pays déterminent :

- L'interaction entre ces autres politiques et une stratégie de protection des infrastructures critiques en tant que telle ;
- La mesure dans laquelle ces autres politiques et la stratégie de protection des infrastructures critiques elle–même devraient être adaptées et rationalisées afin d'éviter les conflits et d'assurer une coordination générale des politiques au niveau national.

Les sections suivantes donnent un aperçu des politiques nationales qui ont une incidence notable sur la protection des infrastructures critiques sans être nécessairement (ou entièrement) conçues à cette fin.

2.3.1 Politiques relatives aux cibles « vulnérables »

La résolution 2396(2017) du Conseil de sécurité souligne que les États Membres doivent élaborer, réviser ou modifier les évaluations des risques et des menaces pour tenir compte des cibles « vulnérables » en vue d'établir des plans d'urgence et des plans d'intervention d'urgence adéquats en cas d'attentats terroristes. La même année, la Commission européenne a mis en place un plan axé sur les espaces publics en tant que principale catégorie d'objectifs non protégés (Commission européenne 2017).

Comme indiqué à la section 1.2, la notion de cibles vulnérables est conceptuellement distincte de celle d'infrastructures critiques. L'une des conséquences majeures est que les politiques des pays en matière d'objectifs non protégés ne répondent pas automatiquement aux conditions et exigences de protection des infrastructures critiques, en particulier lorsqu'il s'agit d'appliquer la résolution 2341 (2017) du Conseil de sécurité.

Cela ne revient toutefois pas à dire que ces deux domaines doivent être traités de manière isolée. Les politiques et pratiques nationales élaborées au sujet de cibles vulnérables peuvent être utiles et constituer une source de pratiques de référence dans le domaine des infrastructures critiques, et vice versa. C'est manifestement la démarche empruntée par EOS, entité représentant les secteurs européens de la sécurité et de la recherche. Vu que certains aspects des politiques relatives aux cibles vulnérables et aux infrastructures critiques se recoupent, EOS les traite au sein du même groupe de travail.

ÉTUDE DE CAS 1
Points d'intérêt fédéral de la Belgique

La loi belge du 1er juillet 2011 sur la protection des infrastructures critiques englobe la notion de Points d'intérêt fédéral. Il s'agit de « lieux non désignés comme infrastructures critiques, mais présentant un intérêt particulier pour l'ordre public, pour la protection spéciale des personnes et des biens, pour la gestion des situations d'urgence ou pour des intérêts militaires, et qui peuvent nécessiter des mesures de protection prises par la Direction générale Centre de crise (DGCC) ».

Cette loi fournit un exemple de cadre normatif unique prenant en compte à la fois les infrastructures critiques et les cibles vulnérables. Bien que les Points d'intérêt fédéral ne remplissent pas les conditions requises pour être considérés comme des infrastructures critiques, ils sont néanmoins jugés dignes d'attention et de protection particulières.

Au lieu d'adopter une approche compartimentée, il faudrait explorer les possibilités de complémentarité. Tout en gardant à l'esprit les différences entre les cadres conceptuels et normatifs applicables aux objectifs non protégés et aux infrastructures critiques, les pays sont encouragés à développer des synergies, compte tenu du fait que, souvent, les mêmes organismes publics ont des responsabilités institutionnelles et opérationnelles dans les deux domaines, simultanément.

2.3.2 Politiques de sécurité nationale

La sécurité nationale est un concept fluide que les pays traduisent en divers sous–éléments et approches en fonction d'un certain nombre de facteurs et de perceptions enracinés dans leur histoire propre, leur situation géographique ou leur contexte géopolitique. Dans la plupart des cas, elle englobe des principes, politiques, procédures et fonctions qui visent à garantir l'indépendance, la souveraineté et l'intégrité d'un pays ainsi que les droits de ses citoyens.

Certains pays inscrivent expressément la protection des infrastructures critiques parmi leurs priorités en matière de sécurité nationale. L'établissement d'un lien étroit entre la protection des infrastructures critiques et les objectifs de sécurité nationale peut aider à assurer un appui politique renforcé en vue de l'élaboration ultérieure de stratégies spécifiques de protection des infrastructures critiques et à favoriser leur mise en œuvre.

ÉTUDE DE CAS 2
La stratégie de sécurité nationale de la Pologne pour 2014

Le document fait explicitement référence à la protection des infrastructures critiques dans sa section sur les "mesures de protection". Bien que la présente section n'évoque pas en détail le thème et n'attribue pas de rôles et de responsabilités précis, elle a l'avantage de définir sans ambiguïté la protection des infrastructures critiques comme une priorité en matière de sécurité nationale. D'autres parties de la stratégie fixent des objectifs pertinents au titre de cette protection, tant au niveau transversal que dans des secteurs spécifiques, notamment pour :

Améliorer et développer le système national de gestion des crises afin d'assurer sa cohésion et son intégrité internes et de permettre une coopération non faussée dans le cadre des systèmes de gestion des crises des organisations internationales dont la Pologne est membre ;

Assurer la sécurité énergétique et alimentaire ;

Sensibiliser davantage l'opinion publique à la sécurité et élargir les compétences des citoyens pour qu'ils puissent réagir comme il se doit face aux situations de crise.

2.3.3 Politiques antiterroristes

Bien que la plupart des stratégies de lutte contre le terrorisme ne fassent pas expressément mention des infrastructures critiques, un certain nombre d'objectifs et d'arrangements institutionnels qui y sont énoncés contribuent à préserver leur intégrité et les fonctions sociales vitales qu'elles remplissent. Par exemple, les stratégies antiterroristes tiennent implicitement compte des questions de protection des infrastructures critiques lors de l'établissement des procédures de gestion générale des crises suite à un attentat terroriste. En outre, elles définissent souvent les cadres généraux de prévention de la commission d'infractions terroristes (par exemple, en s'attaquant aux actes préparatoires, en créant des synergies entre les services de renseignement et les services de répression, etc.).

La Stratégie antiterroriste mondiale d'INTERPOL[5] intègre la dimension liée aux infrastructure critiques CI dans son axe d'action 4.6 « Armes et matériels » en définissant le mandat de l'Organisation en termes de « renforcement de la capacité des pays membres de protéger leurs infrastructures critiques et leurs cibles vulnérables contre les attaques terroristes physiques et informatiques[6]. »

Les stratégies de protection des infrastructures critiques devraient intégrer les concepts et les procédures énoncés dans les cadres stratégiques de lutte contre le terrorisme en les adaptant aux besoins et contextes spécifiques liés à la protection desdites infrastructures.

ÉTUDE DE CAS 3
La stratégie suédoise de lutte contre le terrorisme

La Suède articule sa stratégie de lutte contre le terrorisme autour de trois piliers : prévenir, devancer et protéger. L'objectif de « protéger », en particulier, vise à « assurer une forte protection des personnes, de l'information, des fonctions et des installations – les personnes doivent se sentir en sécurité et libres dans la société ». La stratégie fait spécifiquement référence à l'Agence suédoise pour la protection civile, qui joue officiellement un rôle de coordination en matière de protection des infrastructures critiques en Suède. La stratégie suédoise de lutte contre le terrorisme a été publiée en 2014, l'année même où son plan d'action en faveur de la protection des infrastructures critiques a également été diffusé. L'élaboration de documents de politique générale connexes à court intervalle les uns des autres facilite l'adoption de formulations, de terminologies et d'approches uniformes dans les divers instruments.

2.3.4 Politiques de cybersécurité

La cybersécurité peut être définie comme « l'ensemble des outils, politiques, concepts de sécurité, garanties de sécurité, lignes directrices, approches de gestion des risques, actions, formations, meilleures pratiques, assurances et technologies susceptibles de servir à protéger l'environnement et l'organisation cybernétiques et les actifs des utilisateurs » (GFCE–Meridian 2016, p. 8). Les

[5] RES –03 – –2016

[6] La mise en œuvre concrète de l'axe d'action 4.6 se traduit par une étroite collaboration entre la Direction de la lutte contre le terrorisme d'INTERPOL, basée au Secrétariat général à Lyon (France), et le Centre d'innovation de l'Organisation, situé dans le Complexe mondial pour l'innovation d'INTERPOL à Singapour.

politiques de cybersécurité occupent une place centrale dans la protection des infrastructures critiques car elles fournissent le cadre dans lequel les pays définissent les objectifs et les moyens de protection des infrastructures d'information critiques. Ce concept est examiné plus en détail à la section 2.4.2.

Un certain nombre d'instruments régionaux associent explicitement les concepts de cybersécurité aux infrastructures critiques. C'est ainsi que, la Convention de l'Union africaine sur la cybersécurité (2014) exige que les États parties « s'engagent à élaborer, en collaboration avec les parties prenantes, une politique nationale de cybersécurité qui reconnaisse l'importance des infrastructures d'information critiques (IIC) pour la nation, détermine les risques auxquels la nation est exposée en utilisant l'approche tous risques et indique comment les objectifs de cette politique doivent être atteints[7]. »

Un autre exemple est la stratégie de l'Union européenne en matière de cybersécurité de 2013, dans le cadre de laquelle la Commission européenne s'est engagée à « poursuivre ses activités, menées par le Centre commun de recherche en étroite coordination avec les autorités des États membres et les propriétaires et exploitants d'infrastructures critiques, pour déceler les vulnérabilités des infrastructures critiques européennes liées à la sécurité des réseaux et des informations et encourager le développement des systèmes résistants » (Commission européenne 2013). En vertu de la Directive de l'Union européenne sur la sécurité des réseaux et de l'information[8] (la « Directive SRI »), les États membres de l'UE sont tenus de désigner des exploitants de services essentiels (« OSE ») et d'introduire de nouvelles exigences de sécurité et de déclaration pour ces entités.

Cela dit, toutes les stratégies nationales de cybersécurité n'accordent pas la même place et le même « poids » aux infrastructures critiques et les écarts sont considérables entre les pays. Comme on l'a noté, « certaines stratégies ont été rédigées sous l'angle de la cybercriminalité ou de l'Internet uniquement. Elles ont tendance à négliger les perturbations (nationales) et la gestion des crises liées aux infrastructures d'information critiques ainsi que les incidences intersectorielles. Les stratégies élaborées du point de vue de la cybersécurité à partir d'une évaluation nationale des risques s'inscriront dans une perspective plus large qui fera une place à la protection des infrastructures critiques et à celle des infrastructures d'information critiques » (GFCE–Méridien 2016, p. 8).

Un outil utile proposé par l'UIT est le dépôt des stratégies nationales de cybersécurité. Il s'agit notamment d'une vaste collection de stratégies nationales de cybersécurité, sous forme de documents uniques ou multiples ou d'éléments de stratégies plus larges en matière d'informatique et de communications ou de sécurité nationale[9]. Compte tenu de la diversité des approches entre les différentes sortes de stratégies existantes en matière de protection des infrastructures critiques et de cybersécurité, l'UIT mène actuellement une initiative en coopération avec plusieurs acteurs mondiaux en vue de l'élaboration d'un guide de référence commun sur les stratégies

[7] Art. 24, Cadre national de cybersécurité.
[8] Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union.
[9] https://www.itu.int/en/ITU–D/Cybersecurity/Pages/National–Strategies–repository.aspx.

nationales de cybersécurité. Cet outil vise à donner aux pays une idée claire de l'objectif et du contenu d'une stratégie nationale de cybersécurité, à décrire les modèles et les ressources existants et à guider les pays dans l'élaboration et l'évaluation de leur stratégie[10].

ÉTUDE DE CAS 4
Projet de loi de Singapour sur la cybersécurité

Le projet de loi officialise la politique du pays dans ce domaine et place fermement la protection des infrastructures d'information critiques dans les concepts et les mesures de protection de la cybersécurité. Le projet de loi poursuit quatre objectifs :

- Fournir un cadre normatif formalisant les obligations qui incombent aux détenteurs d'infrastructures d'information critiques d'assurer la cybersécurité de leurs infrastructures d'information critiques respectives ;
- Confier à la Cyber Security Agency of Singapore (l'Agence de la cybersécurité de Singapour) le pouvoir de gérer les menaces et les incidents liés à la cybersécurité et d'y réagir ;
- Établir un cadre en vue de l'échange d'informations sur la cybersécurité avec et par l'Agence, et de la protection de ces informations ;
- Mettre en place un dispositif souple de régime de licences pour les prestataires de services de cybersécurité.

Source : projet de loi sur la cybersécurité consultable à l'adresse ci–après :
www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.pdf

Étude de cas 5
États–Unis – Initiatives du Département de la sécurité du territoire

Aux États–Unis, le Département de la sécurité du territoire dirige les initiatives du Gouvernement fédéral visant à sécuriser les infrastructures critiques du pays. Afin de prévenir et d'atténuer les menaces et d'y faire face, il entend notamment :

- Élaborer un cadre de cybersécurité volontaire technologiquement neutre ;
- Promouvoir et encourager l'adoption de pratiques de cybersécurité ;
- Accroître le volume, la rapidité et la qualité du partage de l'information sur les cybermenaces ;
- Intégrer de solides mesures de protection de la vie privée et des libertés civiles dans toutes les initiatives visant à protéger les infrastructures critiques ;
- Se doter d'une capacité d'appréciation de la situation lui permettant d'examiner à la fois les aspects physiques et cybernétiques du fonctionnement de l'infrastructure en temps quasi–réel ;
- Comprendre les conséquences en cascade des défaillances de l'infrastructure ;
- Évaluer et développer le partenariat public–privé ;
- Mettre à jour le Plan national de protection des infrastructures ;
- Élaborer un plan complet de recherche–développement.

Le Département encourage l'adoption du cadre de cybersécurité du National Institute of Standards and Technology) pour améliorer la cybersécurité des infrastructures critiques. Révisé en avril 2018, le cadre

[10] https://www.itu.int/en/ITU–D/Cybersecurity/Pages/National–Strategies.aspx.

de l'institut national définit des lignes directrices autour de quatre fonctions clés pour améliorer la gestion des risques liés à la cybersécurité :

Identifier – développer une compréhension organisationnelle pour gérer les risques en matière de cybersécurité auxquels sont exposés les systèmes, les personnes, les actifs, les données et les capacités ;
Protéger – élaborer et mettre en œuvre des mesures de protection adéquates pour assurer la prestation des services essentiels ;
Détecter – élaborer et mettre en œuvre des activités appropriées pour déterminer le moment où survient un incident en matière de cybersécurité ;
Réagir – élaborer et mettre en œuvre des activités pertinentes permettant de prendre des mesures concernant un incident de cybersécurité détecté ;
Récupérer – élaborer et mettre en œuvre des activités adaptées au maintien des plans de résilience et au rétablissement des capacités ou des services qui ont été affaiblis en raison d'un incident de cybersécurité.

Sources :

Department of Homeland Security, Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD–21 Critical Infrastructure Security and Resilience, at: www.dhs.gov/sites/default/files/publications/eo–13636–ppd–21–fact–sheet–508.pdf ;

Department of Homeland Security, Critical Infrastructure Cyber Community Voluntary Program, à l'adresse ci–après : www.us–cert.gov/ccubedvp

NIST Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, 16 avril 2018, à l'adresse ci–après : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.3.5 Autres politiques nationales

Lors de l'élaboration d'une stratégie nationale en matière de protection des infrastructures critiques, il importe de dresser un inventaire complet de toutes les politiques nationales qui ont une incidence sur elle. Certaines politiques et certains cadres réglementaires portant sur des infrastructures en général peuvent être en place. Par exemple, en 2017, Singapour a adopté une loi sur la protection des infrastructures. La loi, qui est spécifiquement consacrée à la protection des infrastructures contre les actes terroristes, introduit un certain nombre de concepts tels que celui de « zone protégée », de « lieu protégé » et d'« infrastructure protégée ». Elle ne fait cependant pas expressément référence aux infrastructures « critiques » en termes d'actifs ou de systèmes remplissant des fonctions essentielles pour la communauté. En pareilles circonstances, il faut déterminer le rôle et la place des cadres normatifs existants dans les objectifs généraux de protection des infrastructures critiques.

Certaines politiques peuvent ne pas mentionner les infrastructures critiques simplement parce qu'elles ont été adoptées à une époque où la notion même de protection des infrastructures critiques n'avait pas encore fait son chemin dans les discours politiques courants, ou pour d'autres raisons. Si elles empiètent sur des questions de fond liées aux infrastructures critiques, elles devraient faire l'objet d'un examen attentif afin de garantir leur compatibilité et leur complémentarité avec les stratégies nationales de protection nouvellement conçues à cet effet.

D'autres politiques pertinentes découlent des obligations internationales qui incombent aux pays dans divers domaines. C'est ainsi que pour se conformer aux instruments internationaux pertinents[11], les pays ont mis en place une série de politiques, lois, règlements, stratégies, plans et mesures visant à renforcer la sécurité des matières, installations et informations sur les armes chimiques, biologiques, radiologiques et nucléaires.

Étude de cas 6
Programme fédéral suisse d'approvisionnement économique national

L'approvisionnement économique national trouve son fondement juridique dans l'article 102 de la Constitution, qui stipule que « la Confédération assure l'approvisionnement du pays en biens et services de première nécessité afin de pouvoir faire face à une menace de guerre, à une autre manifestation de force ou à une grave pénurie à laquelle l'économie n'est pas en mesure de remédier par ses propres moyens. Elle prend des mesures préventives ».

Comme le précise la Stratégie nationale suisse pour la protection des infrastructures critiques, « l'approvisionnement économique national couvre environ la moitié des secteurs et sous–secteurs critiques de la stratégie nationale de protection des infrastructures critiques et contribue ainsi de manière décisive à la réalisation des objectifs de cette dernière ». Fait décisif, l'approvisionnement du pays est axé principalement sur les pénuries nationales à long terme, tandis que la stratégie de protection des infrastructures critiques tient également compte des troubles locaux ou à court terme (p. ex. les pannes ou perturbations régionales).

2.4 Quelles sont les infrastructures critiques ?

Il est explicitement reconnu dans la résolution 2341 (2017) que « chaque État détermine quelles sont ses infrastructures critiques ». Aucune méthode de sélection particulière n'y est toutefois recommandée qui permette d'isoler dans la myriade d'infrastructures situées sur le territoire d'un État celles qui sont critiques. On ne trouve pas non plus d'orientations dans d'autres instruments internationaux. Les dispositions de la Convention de l'Union africaine sur la cybersécurité, par exemple, se limitent à ce qui suit : « Chaque État adopte des mesures législatives et/ou réglementaires qu'il jugera nécessaires pour identifier les secteurs considérés comme sensibles pour sa sécurité nationale et le bien–être de l'économie ainsi que les systèmes de technologies de l'information et des communications conçus pour fonctionner dans ces secteurs comme des infrastructures critiques de l'information[12] [...] ».

Les pays jouissent donc d'une latitude considérable quant au choix des critères permettant de déterminer parmi les infrastructures opérant sur leur territoire celles qui sont à considérer comme « critiques ». La tâche n'est pas simple. Faire une différence entre les infrastructures importantes

[11] Il s'agit notamment de la Convention sur l'interdiction de la mise au point, de la fabrication et du stockage des armes bactériologiques (biologiques) ou à toxines ; de la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction ; de la Convention sur la protection physique des matières nucléaires ; de la Convention internationale pour la répression des actes de terrorisme nucléaire ; de la Stratégie antiterroriste mondiale des Nations unies et de la résolution 1540 (2004) du Conseil de sécurité de l'ONU.
[12] Art. 25, Mesures légales.

ou pertinentes et celles à tenir pour « critiques » est essentiel pour pouvoir prioriser les ressources si précieuses pour ce qui est de la protection d'un large éventail d'installations, de systèmes et d'activités. D'un côté, si de trop nombreuses infrastructures entrent dans la catégorie « critique », la tâche peut devenir ingérable (en plus d'être financièrement non viable). De l'autre, l'adoption d'une approche trop restrictive risque de laisser sans protection un certain nombre d'installations et d'activités cruciales, d'où des conséquences potentiellement catastrophiques en cas d'accident. Un auteur a souligné que les États avaient tendance à grossir leur liste d'infrastructures critiques car trop peu de décideurs étaient prêts à accepter le risque politique du retrait d'un élément de la liste, et que la tentation était grande d'élargir continuellement la liste d'éléments considérés comme critiques. Un tel niveau d'ambiguïté engendre un gaspillage car les ressources ne sont pas affectées là où elles peuvent avoir le plus d'impact [...] (Clemente 2013, p. ix).

Malgré l'absence de critères ayant une portée générale, il est possible de disposer d'orientations dans certains secteurs. Par exemple, si les instruments de l'Organisation de l'aviation civile internationale (OACI) ne définissent pas d'« infrastructures critiques » en tant que telles, le Manuel de l'aviation de l'OACI entend par « point vulnérable, toute installation située à l'aéroport ou rattachée à celui–ci, dont la détérioration ou la destruction entraverait gravement le bon fonctionnement de l'aéroport ». Les tours de contrôle de la circulation aérienne, les installations de télécommunication, les aides à la radionavigation, les transformateurs de puissance, les alimentations électriques primaires et secondaires ainsi que les installations de carburant, tant à l'aéroport qu'en dehors, devraient être considérés comme des points vulnérables. Les systèmes d'aide à la communication et à la radionavigation susceptibles d'être piratés devraient bénéficier d'un niveau de sécurité plus élevé[13].

Dans le secteur maritime, le Code ISPS recense les éléments essentiels que les organismes publics, les administrations locales, les secteurs maritime et portuaire doivent protéger contre les menaces à la sûreté les navires ou les installations portuaires utilisés dans le cadre du commerce international. Par conséquent, les « plans de sûreté du navire » sont ceux conçus pour assurer l'application à bord de mesures destinées à protéger les personnes, la cargaison, les engins de transport, les provisions de bord ou le navire lui–même contre les risques liés à la sécurité. Des plans de sûreté doivent également être élaborés pour protéger les installations portuaires ainsi que les navires, les personnes, les cargaisons, les engins de transport et les provisions de bord situés à l'intérieur des installations portuaires contre les risques liés à la sécurité[14].

2.4.1 Déterminer le caractère « critique » de certaines infrastructures

La première étape du recensement des infrastructures critiques consiste en général à adopter une définition globale de ce que l'on entend par l'expression « infrastructures critiques », ce qui présente l'intérêt d'établir le contexte dans lequel d'autres cadres politiques et réglementaires seront élaborés. Le réseau CIPRNet[15] a répertorié plus de 100 définitions de cette expression, et le

[13] Manuel de sécurité aérienne (Doc 8973 – distribution limitée).
[14] http://www.imo.org/fr/ourwork/security/guide_to_maritime_security/pages/solas–xi–2%20isps%20code.aspx.
[15] Voir, en particulier, CIPedia, service communautaire en ligne de type Wikipédia axé sur la protection et la résilience des infrastructures critiques, élaboré par le réseau CIPRNet avec l'appui du septième programme–cadre de recherche et de développement technologique de l'Union européenne (7e PC) et poursuivi par des volontaires (https://publicwiki–01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure).

tableau 2 en présente une sélection. Dans l'ensemble, si les définitions retenues par certains pays mettent l'accent sur la finalité de l'infrastructure visée (son caractère critique étant lié à l'exécution de tâches essentielles à la société), d'autres, en revanche, soulignent les effets de sa perturbation ou de sa destruction (le caractère critique de l'infrastructure résultant alors des conséquences propres à l'interruption du service rendu par ladite infrastructure).

Il est possible de définir les infrastructures critiques, notamment, en tenant compte du rôle qu'elles jouent dans la promotion et la protection des droits de la personne (par exemple, dans le cas où une infrastructure est indispensable au fonctionnement des systèmes de soins de santé ; aux systèmes d'urgence ou, entre autres, d'approvisionnement en eau et d'évacuation des eaux usées) ainsi que de l'impact de leur détérioration, perturbation ou destruction sur ces mêmes droits (par exemple, si cette situation se traduit par l'incapacité de fournir des services de santé adéquats, voire de sauver des vies, par des dommages environnementaux pouvant entraîner des pertes en vies humaines, ou encore par des déplacements forcés ayant une incidence négative sur le droit à la santé). Une telle approche est conforme à l'esprit des définitions existantes. Ainsi, selon l'Union européenne, une « infrastructure critique » se dit d'« un point, système ou partie de celui–ci, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien–être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif du fait de la défaillance de ces fonctions[16] ». Dans le même ordre d'idées, le droit des conflits armés accorde une protection spéciale aux infrastructures indispensables à la survie de la population civile ou dont la destruction causerait des pertes sévères ou compromettrait la santé et la survie de la population (premier Protocole additionnel aux Conventions de Genève de 1949, art. 54 à 56).

Tableau 2 : définitions des infrastructures critiques, par pays

Autriche	Les infrastructures critiques sont les infrastructures ou parties de celles–ci qui revêtent une importance cruciale pour assurer des fonctions sociales importantes. Leur défaillance ou destruction a des effets graves sur la santé, la sécurité et le bien–être économique et social de la population ou le fonctionnement des institutions gouvernementales (Stratégie pour la cybersécurité de l'Autriche, 2013).
Canada	On entend par infrastructures critiques les activités, les systèmes, les installations, les technologies, les réseaux, les biens et les services qui sont essentiels à la santé, à la sécurité, à la sûreté ou au bien–être économique des Canadiens et des Canadiennes, ainsi qu'au fonctionnement efficace du Gouvernement (Gestion des urgences, Canada, 2011).
France	Les points d'importance vitale représentent tout établissement, installation ou ouvrage dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement : si son activité est difficilement substituable ou remplaçable, d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, ou de mettre gravement en cause la santé ou la vie de la population. (Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, Secrétariat général de la défense et de la sécurité nationale.)

[16] Directive 2008/114/CE du Conseil de l'Union européenne, article 2.

Allemagne	Les infrastructures critiques sont des structures et des installations organisationnelles et physiques d'une importance vitale pour la société et l'économie d'un pays au point que leur défaillance ou leur dégradation entraînerait des pénuries durables d'approvisionnement, des perturbations majeures de la sécurité et de la sûreté publiques ou d'autres conséquences de grande ampleur (Stratégie nationale de protection des infrastructures critiques, 2009).
Italie	L'infrastructure critique s'entend de tout système et de toute ressource, activité ou structure – même virtuelle – dont la destruction, l'interruption, voire l'indisponibilité même partielle ou temporaire a pour effet d'affaiblir sensiblement l'efficacité et le fonctionnement normal d'un pays ainsi que la sécurité et les systèmes économiques, financiers et sociaux, y compris les organes de l'administration publique centrale et locales (Agence de protection civile, glossaire).
Kenya	Les infrastructures critiques désignent les biens qui sont essentiels au bon fonctionnement de la société et de l'économie (par exemple le réseau électrique, les télécommunications et l'approvisionnement en eau) (Stratégie nationale de cybersécurité du Kenya).
Norvège	Les infrastructures critiques sont les dispositifs et systèmes indispensables à l'exercice des fonctions essentielles de la société, permettant de répondre aux besoins fondamentaux de cette dernière et de préserver la sécurité de la population (Stratégie de cybersécurité pour la Norvège).
Pakistan	Les infrastructures critiques s'entendent notamment des infrastructures ainsi désignées par toute administration publique au Pakistan et des autres structures, systèmes et réseaux, physiques ou virtuels, d'une importance vitale pour l'État ou ses organes, y compris le pouvoir judiciaire, au point que leur défaillance ou leur destruction peut nuire, entre autres, à la sécurité, l'économie, la santé publique et la sûreté du pays ainsi qu'à d'autres domaines qui leur sont liés (Projet de loi sur la cybercriminalité, 2015).
Qatar	Les infrastructures physiques s'entendent des biens, systèmes ou installations physiques dont la défaillance, la mise en péril ou la destruction aurait des incidences graves sur la santé, la sécurité, la sûreté ou le bien–être économique du Qatar ou sur le bon fonctionnement des services gouvernementaux qatariens (Stratégie du Qatar en matière de cybersécurité, 2014).
Arabie saoudite	On entend par infrastructures critiques des systèmes et des biens, physiques ou virtuels, indispensables à l'Arabie saoudite au point que leur défaillance ou leur destruction nuirait à la sûreté, à la sûreté économique nationale, à la santé publique ou à la sécurité publique nationale, ou à ces domaines combinés (Septième projet d'élaboration d'une stratégie nationale de sécurité de l'information pour le Royaume d'Arabie saoudite).
Trinité–et–Tobago	On entend par infrastructures critiques les systèmes, dispositifs et réseaux informatiques, les programmes et données informatiques revêtant une importance vitale pour le pays au point que leur défaillance, destruction ou perturbation nuirait à la sûreté, à la défense ou aux relations internationales de l'État ; ou à la prestation des services directement liés à la sûreté nationale ou économique, aux services bancaires et financiers, à l'infrastructure de communication, à la santé et à la sécurité publiques nationales, aux transports publics, à l'infrastructure à clefs publiques ou à ces secteurs combinés (Stratégie nationale de cybersécurité, 2012).

Fédération de Russie	Les infrastructures critiques de la Fédération de Russie désignent tout élément dont la perturbation ou l'interruption du fonctionnement se solde par la perte de contrôle ou la destruction desdites infrastructures, des transformations négatives (ou des défaillances) irréversibles de l'économie ou pout tout ressortissant de la Fédération de Russie ou toute unité administrative territoriale, ou par une dégradation importante de la santé et de la sécurité des personnes qui vivent dans ces zones, et ce, à long terme (Sécurité nationale de la Russie – sécurité informatique, 3 février 2012, n. 803).
Espagne	Les infrastructures critiques sont des infrastructures stratégiques (installations, réseaux, systèmes et équipements physiques et informatiques sur lesquels repose la prestation des services essentiels, dont l'exploitation est indispensable) qu'il n'est pas possible de remplacer par d'autres solutions de sorte que leur perturbation ou destruction aurait de graves répercussions sur les services essentiels (loi 8/2011).
Suisse	On entend par infrastructures critiques les infrastructures dont la perturbation, la défaillance ou la destruction aurait des conséquences graves pour la société, le secteur privé et l'État (Stratégie nationale de protection de la Suisse contre les cyber–risques, 2012).
Ukraine	On entend par infrastructures critiques les entreprises, institutions et organisations, quelle que soit leur forme de propriété, dont les activités sont directement liées aux procédés technologiques ou à la fourniture de services de grande importance pour l'économie et l'industrie, le fonctionnement de la société et la sécurité de la population, et dont la défaillance ou le dysfonctionnement peut avoir un impact négatif sur la sûreté nationale et la défense de l'Ukraine, l'environnement ou causer un choc matériel et/ou constituer une menace pour la vie et la santé (loi intitulée « Sur les principes fondamentaux de la garantie d'une cybersécurité en Ukraine, 2163–19).
États–Unis	Les infrastructures critiques s'entendent des systèmes et biens, physiques ou virtuels, d'une importance vitale pour les États–Unis au point que leur défaillance ou destruction nuirait à la sûreté, à la sécurité économique nationale, à la santé ou la sécurité publique nationale, ou à une combinaison de ces domaines (*Patriot Act*, 2001).

La deuxième étape du recensement des infrastructures critiques est la plus difficile, étant donné qu'elle consiste à établir un ordre de priorité. Elle vise notamment à déterminer les secteurs et sous–secteurs (ou services) considérés comme critiques. Dans un premier temps, on pourrait étudier la situation d'autres pays qui présentent des similitudes sociétales et géographiques ainsi qu'un niveau comparable de développement technique et économique.

Il existe un certain nombre de secteurs que tous les pays peuvent considérer comme critiques. Le secteur de l'énergie en est un exemple type. Les pays sont tributaires de la fourniture d'électricité pour l'accomplissement de presque toutes les fonctions sociales et économiques, depuis les télécommunications jusqu'au système de pompage de l'eau en passant par la prestation des soins médicaux vitaux. En même temps, il est important de noter qu'un secteur ou sous–secteur particulier peut être primordial pour un pays, mais pas pour un autre. La taille et les spécificités de l'économie d'un pays peuvent fort bien permettre de déterminer ce qui est critique et ce qui l'est moins. Ainsi, certains pays peuvent dépendre massivement de l'industrie du tourisme au niveau des recettes, gage, en définitive, du maintien de leur cohésion sociale et de leur stabilité

interne. Pour ces pays, le fait de protéger l'industrie du tourisme en raison de sa nature « critique » peut contribuer à garantir la fourniture de services essentiels à la société.

De plus, il ne faudrait pas automatiquement déduire du fait qu'un certain secteur est considéré comme critique que tous les services connexes le soient. Par exemple, dans le secteur de l'énergie, il est très probable qu'un service de chauffage urbain ne fera pas partie des infrastructures critiques à l'échelon national, contrairement à la fourniture d'électricité. Compte tenu de ces variations, les pays parviennent, dans une très grande mesure, à des conclusions analogues. On trouvera dans le tableau 3 la liste des 11 secteurs définis par l'Union européenne et des 37 sous–secteurs correspondants.

Tableau 3 : Liste indicative des secteurs et sous–secteurs définis par l'UE

I Énergie	1 Production pétrolière et gazière, raffinage, traitement, stockage et distribution par oléoducs et gazoducs 2 Production d'électricité 3 Transport d'électricité, de gaz et de pétrole 4 Distribution d'électricité, de gaz et de pétrole
II Technologies de l'information et des communications (TIC)	5 Protection des systèmes d'information et des réseaux 6 Systèmes d'instrumentation, d'automatisation et de contrôle (SCADA, etc.) 7 Internet 8 Fourniture de services de télécommunications fixes 9 Fourniture de services de télécommunications mobiles 10 Radiocommunication et radionavigation 11 Communications par satellite 12 Radiodiffusion
III Eau	13 Fourniture d'eau potable 14 Contrôle de la qualité de l'eau 15 Systèmes de digues et contrôle quantitatif des eaux
IV Alimentation	16 Fourniture de vivres et sécurité alimentaire
V Santé	17 Soins médicaux et hospitaliers 18 Médicaments, sérums, vaccins et produits pharmaceutiques 19 Laboratoires de biologie et agents biologiques
VI Finance	20 Services de paiement/structures de paiement (privés) 21 Services financiers publics
VII Ordre public et juridique et sécurité publique	22 Maintien de l'ordre public et juridique, de la sécurité et de la sûreté 23 Administration de la justice et détention
VIII Administration civile	24 Fonctions gouvernementales 25 Forces armées 26 Services de l'administration civile 27 Services d'urgence 28 Services postaux et de messagerie
IX Transports	29 Transports par route 30 Transport ferroviaire 31 Transport aérien 32 Navigation intérieure 33 Transport hauturier et transport maritime à courte distance

X Industrie chimique et nucléaire	34 Production et stockage/traitement de substances chimiques et nucléaires 35 Transport de substances dangereuses (chimiques) par pipelines
XI Espace **Source :** Commission européenne 2005	36 Espace 37 Recherche

ÉTUDE DE CAS 7
L'approche néerlandaise : des secteurs critiques aux activités critiques

En 2014, les Pays–Bas ont réformé en profondeur leur politique en matière d'infrastructures critiques et la notion de « secteurs critiques » s'est substituée à celle d'« activités critiques ». Ces dernières sont désormais celles qui, en cas de défaillance ou de perturbation, pourraient entraîner de graves troubles sociaux. Étant donné que toutes les activités de tel ou tel secteur ne sont pas critiques, l'accent est mis actuellement sur les activités critiques et non sur les secteurs critiques. Le recensement des activités critiques permet d'utiliser les outils et les ressources limitées à disposition d'une manière plus efficace et mieux ciblée. Il est procédé à l'évaluation du degré de caractère critique à partir de critères d'impact prédéfinis, tels que les dommages économiques et les conséquences physiques. Les évolutions de la société, par exemple en termes de nouvelles menaces et d'évaluations des problèmes rencontrés, peuvent se traduire par la redéfinition des activités critiques. L'évaluation distingue deux catégories critiques, A et B. La défaillance des activités critiques classées A a des effets potentiels bien supérieurs à celle des activités critiques classées B. Cette différenciation des infrastructures critiques en deux catégories peut servir à mesurer l'importance des problèmes rencontrés ou du renforcement des capacités à prévoir en vue d'une meilleure résilience.

Catégorie A
- Transport et distribution d'électricité à l'échelle nationale
- Production de gaz naturel
- Approvisionnements en pétrole
- Stockage, production ou traitement de matières nucléaires
- Approvisionnement en eau potable
- Gestion des ressources en eau

Catégorie B
- Distribution régionale d'électricité et de gaz
- Gestion des vols et des avions
- Gestion de la navigation maritime et intérieure
- Stockage, production ou transformation à grande échelle de ressources pétrochimiques
- Secteur financier (services bancaires, virements électroniques entre banques et entre banques et particuliers)
- Communication avec et entre les services d'urgence
- Mobilisation de la police
- Services gouvernementaux qui dépendent de systèmes d'information et de données numériques fiables et disponibles

Il incombe à chaque ministère d'évaluer les activités critiques qui relèvent de sa responsabilité. Le Ministère de la justice et de la sécurité, chargé de la coordination, examinera régulièrement la méthodologie suivie pour vérifier qu'elle est à jour et déterminera si certaines indications font supposer l'émergence de nouvelles activités critiques.

Source : Pays–Bas 2018

La troisième étape consiste à relier des secteurs et sous–secteurs déjà recensés à une liste d'infrastructures, de systèmes et d'activités. Leur nombre peut varier de quelques milliers seulement à plusieurs milliers, selon la taille des pays, leur niveau de développement économique, etc. Les pays ont élaboré de nombreux ensembles d'indicateurs de recensement des infrastructures considérées comme « critiques ». Ces indicateurs visent généralement à « apprécier » les effets d'une panne ou d'une défaillance fonctionnelle des infrastructures et réunissent une sélection ou une combinaison des éléments suivants :

- Portée géographique des effets ;
- Durée des effets ;
- Gravité des effets potentiels sur les plans suivants :
- Conséquences économiques (impact sur le PIB, pertes économiques directes et indirectes, effectifs employés et recettes fiscales) ;
- Nombre de victimes et de personnes évacuées ;
- Perte d'autorité de l'État/perturbation de l'administration publique ;
- Dommages causés à l'environnement.

ÉTUDE DE CAS 8
Importance systémique et importance symbolique des infrastructures critiques en Allemagne

La stratégie menée par l'Allemagne dans le domaine de la protection des infrastructures d'information critiques distingue ces dernières selon l'importance systémique et l'importance symbolique de leur dimension critique. Une infrastructure critique présentera une importance systémique toutes les fois où – compte tenu de la place qu'elle occupe sur les plans structurel, fonctionnel et technique dans l'ensemble du système des secteurs d'infrastructures – elle jouera un rôle particulièrement important par rapport à d'autres infrastructures. Tel est le cas, par exemple, des infrastructures électriques, informatiques et de télécommunication qui, en raison de la taille et de la densité de leurs réseaux respectifs, revêtent une importance particulière et dont une panne à grande échelle et prolongée peut entraîner de graves perturbations dans la vie et les activités de la population et nuire considérablement à la sûreté et à la sécurité publiques. Une infrastructure critique présentera une importance symbolique si – compte tenu de son poids culturel ou de son rôle majeur dans la création d'un sentiment d'identité – sa perte est à l'origine de troubles émotionnels pour la société d'un pays et si elle déséquilibre psychologiquement cette dernière de manière durable.

Source : Allemagne 2009

Diverses méthodes peuvent être utilisées. Un consortium dirigé par TNO, une organisation néerlandaise de la recherche scientifique appliquée, s'est employé à les regrouper schématiquement en trois grands types : i) une approche axée sur les services (notamment en Suisse) où l'État recense les biens critiques sur la base de certains critères sectoriels en fixant des

seuils pour ce qui est du service fourni ou de la production quantifiable générée par les biens, par exemple le nombre de mégawatts fournis ; ii) une approche axée sur l'opérateur (notamment en France), selon laquelle il revient à chaque opérateur d'infrastructures de déterminer les installations ou services qui présentent une dimension critique ; iii) une approche axée sur les biens ou hybride (notamment au Royaume–Uni), qui utilise des éléments de l'approche axée sur les services et de celle axée sur l'opérateur (RECIPE 2011, p. 23).

ÉTUDE DE CAS 9
Méthodes de recensement des infrastructures critiques : l'Union européenne, la France et le Royaume–Uni

Union européenne
La directive 2008/114/CE du Conseil de l'Union européenne du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection prévoit une procédure en quatre étapes. Bien que, sur le plan technique, la directive ne concerne que le recensement des infrastructures critiques européennes (ICE) dans les secteurs des transports et de l'énergie, il y est implicitement suggéré que cette procédure s'applique aussi au recensement des infrastructures critiques nationales pour ce qui est des secteurs autres que l'énergie et les transports. Est énoncée à l'annexe III ladite procédure comme suit :

Étape 1
Chaque État membre applique les critères sectoriels afin d'opérer une première sélection parmi les infrastructures critiques existant au sein d'un secteur.
Étape 2
Chaque État membre applique la définition des infrastructures critiques visée à l'article 2, point a), à l'ICE potentielle recensée lors de l'étape 1. La gravité de l'impact sera déterminée par application des méthodes nationales de recensement des infrastructures critiques ou sur la base des critères intersectoriels [voir étape 4 ci–dessous], à l'échelon national approprié. En ce qui concerne les infrastructures qui offrent un service essentiel, il sera tenu compte de l'existence de solutions de remplacement ainsi que de la durée de l'arrêt/de la reprise d'activité.
Étape 3
Chaque État membre applique l'élément transfrontalier de la définition d'ICE visée à l'article 2, point b), à l'ICE potentielle qui a franchi les deux premières étapes de la procédure. Si l'ICE potentielle répond à la définition, elle est soumise à l'étape suivante de la procédure. En ce qui concerne les infrastructures qui offrent un service essentiel, il sera tenu compte de l'existence de solutions de remplacement ainsi que de la durée de l'arrêt/de la reprise d'activité.
Étape 4
Chaque État membre applique les critères intersectoriels aux ICE potentielles restantes. Les critères intersectoriels tiennent compte des éléments suivants : la gravité de l'impact et, pour les infrastructures qui offrent un service essentiel, l'existence de solutions de remplacement, ainsi que la durée de l'arrêt/de la reprise d'activité. Les ICE potentielles qui ne répondent pas aux critères intersectoriels ne seront pas considérées comme étant des ICE. L'identification des ICE potentielles qui franchissent toutes les étapes de cette procédure n'est communiquée qu'aux États membres susceptibles d'être affectés considérablement par lesdites infrastructures.

France

En France, ce n'est pas l'État qui recense directement les points importants des infrastructures critiques mais un « opérateur d'importance vitale » (OIV) désigné qui est chargé de dresser la liste des points d'importance vitale. Le code de la défense prévoit qu'un opérateur d'importance vitale est désigné comme tel par le ministre coordonnateur de son secteur d'activités d'importance vitale, en concertation avec le ou les ministres intéressés. La notification à l'opérateur de l'intention de le désigner OIV est l'occasion d'une concertation entre l'autorité administrative et l'opérateur. Le statut d'OIV repose sur deux conditions :

– que son activité s'exerce en tout ou en partie dans un secteur d'activités d'importance vitale ;

– qu'il gère ou utilise au moins un établissement, un ouvrage ou une installation dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait de quelque manière que ce soit d'avoir des conséquences majeures sur les capacités de survie de la nation ou sur la santé ou la vie de la population.

De manière générale, un OIV peut être :

– une société

– une association, une fondation ou une organisation internationale ;

– un service de l'État, une collectivité territoriale, un groupement de collectivités, un établissement public, une autorité administrative indépendante.

S'agissant d'une entreprise, ce peut être une société mère ou une filiale. Le choix de l'entité ad hoc se fait après concertation avec l'opérateur concerné.

Plusieurs filiales d'un même groupe peuvent, le cas échéant, être désignées. Lorsque la désignation d'un opérateur est envisagée simultanément par plusieurs ministres coordonnateurs, une concertation est menée afin d'arrêter le choix du ministère privilégié. Autant que possible, le correspondant privilégié est le ministre coordonnateur responsable du secteur d'importance vitale dans lequel l'opérateur exerce son activité principale.

Dans le cadre de son activité normale, un OIV peut avoir sous–traité ou externalisé une ou plusieurs fonctions concourant à la réalisation de l'activité d'importance vitale. Dans ce cas, il appartient à l'OIV de prendre les dispositions nécessaires vis–à–vis de son sous–traitant ou de son fournisseur pour que celui–ci concoure à la réalisation des objectifs de sécurité et de sûreté dans le domaine de la protection des infrastructures critiques.

À la suite de sa désignation, l'OIV élabore son plan de sécurité d'opérateur (PSO). L'analyse de risque qu'il conduit pour élaborer son PSO lui permet de proposer, en annexe à ce plan, la liste de ses installations, établissements ou ouvrages qu'il estime pertinent de faire désigner comme points d'importance vitale (PIV).

Source : France, 2014.

Royaume–Uni

Le Royaume–Uni a recensé 9 secteurs critiques et 20 sous–services critiques, lesquels sont à leur tour composés de biens à déterminer. Le ministère responsable d'un secteur effectue une première sélection de biens et d'exploitants (les exploitants étant choisis en fonction de leur part de marché relative). Le Centre pour la protection des infrastructures nationales (CPNI) effectue sa propre évaluation en parallèle. Les contributions des exploitants, du ministère responsable et du CPNI permettent, à elles toutes, de définir un bien (ou une activité) en fonction des conséquences engendrées par une défaillance éventuelle du service. Six degrés critiques (de CAT0 à CAT5) ont été établis et sont fixés selon trois critères intersectoriels, à savoir : l'impact sur la vie, l'impact économique et l'impact sur les services essentiels.

Officiellement, ces critères sont uniquement descriptifs et subjectifs. Mais, pour ce qui est des informations classifiées, chacun des 18 critères possibles est assorti de valeurs quantitatives et objectives (métriques). Cette segmentation s'effectue selon des critères propres à chacun des neuf secteurs critiques, de sorte que très peu de biens ou d'activités relèvent du degré critique le plus élevé. Seuls les éléments classés à CAT3 et plus sont considérés comme véritablement « critiques ». Le classement des biens est établi en combinant le degré critique retenu et la probabilité d'une attaque à l'encontre du bien en question, ce qui revient à associer, d'une part, vulnérabilité (par exemple, en fonction de la facilité d'accès de tel ou tel bien) et, d'autre part, menace (par exemple, en fonction du type d'attaques et de leur probabilité ou, en termes de dangers, des risques de défaillance). S'agissant des menaces à la sécurité, les niveaux de l'échelle de probabilité peuvent varier considérablement et très souvent au cours d'une année.

Source : RECIPE 2011, p. 23.

2.4.2 Infrastructures d'information critiques

Dans les économies modernes, les chaînes de production industrielle et la fourniture de biens et de services par le secteur public et le secteur privé sont, pour la plupart, gérées par des systèmes informatisés, appelés systèmes de supervision. Au cours des dernières décennies, ces systèmes ont été progressivement reliés à Internet et aux réseaux d'entreprises privées, d'où une rationalisation de la production et de la prestation des services. De plus, le fait de mettre en réseau à plus grande échelle les systèmes de supervision industrielle permet d'accroître la synergie et l'efficacité et, en raison de la déréglementation des services publics, il est de plus en plus important à des fins commerciales d'obtenir des informations en temps réel (Shea 2003, p. 3).

En même temps, le fait que les systèmes de supervision soient de plus en plus reliés aux systèmes informatiques des entreprises par Internet les expose d'autant plus aux cyberattaques. D'autre part, les systèmes les plus anciens, c'est–à–dire ceux qui ont été installés avant l'ère de l'Internet et qui n'ont pas été conçus à des fins de connectivité, posent des problèmes de sécurité particuliers.

Point essentiel, les systèmes de supervision sont utilisés dans pratiquement tous les secteurs d'infrastructures critiques, car ils régissent souvent le fonctionnement en continu des centrales électriques, barrages, ponts, tours de télécommunication, etc. Ce sont donc des éléments clefs des infrastructures d'information critiques. Il existe plusieurs définitions de ce concept selon les pays. L'OCDE définit comme infrastructures d'information critiques les systèmes d'information qui ont un caractère critique parce que leur perturbation ou leur destruction pourrait avoir des conséquences graves pour la santé, la sûreté, la sécurité, le bien–être économique des citoyens, le bon fonctionnement de l'État ou de l'économie (OCDE 2008).

Il est fondamental que, dans le cadre des stratégies de protection des infrastructures critiques, les infrastructures d'information critiques soient traitées sur un pied d'égalité avec les infrastructures physiques et bénéficient comme elles d'une protection, et ce, d'autant plus que l'on pourrait presque tenir les différences entre « infrastructures » et « infrastructures d'information » comme non pertinentes, étant donné que ces deux catégories ne forment qu'une seule classe dans le cercle grandissant des éléments critiques. Plus la dépendance à l'égard des infrastructures informatisées et connectées augmente, plus les « nœuds » critiques sont nombreux (c'est–à–dire les points d'un système dont la défaillance dégraderait considérablement l'ensemble du réseau) (Clemente 2013).

Il est déterminant de tenir compte de cette dépendance lors du recensement des infrastructures d'information critiques. Par conséquent, il pourrait être nécessaire de prendre en considération les infrastructures qui ne sont pas en soi critiques (comme, par exemple, une petite centrale électrique) dans la mesure où elles sont reliées en interne à une infrastructure critique (par exemple, un barrage).

2.4.3 Interconnexions et interdépendances

La fourniture de biens et services essentiels à la société est de plus en plus le fait d'interactions entre de multiples fournisseurs. Ces derniers sont issus de tous les secteurs et sous–secteurs d'infrastructures critiques, ce qui crée des liens complexes. Si l'interconnectivité des installations, systèmes et activités s'explique par le souci d'une gestion plus efficace des ressources, cette évolution accroît les dépendances. Celles–ci peuvent se définir au sens large comme « le lien qui unit deux produits ou services et dans le cadre duquel l'un des deux produits ou services est nécessaire à la production de l'autre »[17]. À titre d'exemples, l'approvisionnement en denrées alimentaires dépend des transports, les secteurs bancaire et financier reposent sur les télécommunications pour l'authentification des transactions, et les télécommunications, elles, sont tributaires de la distribution de l'électricité. La plupart des services essentiels dépendent de la fourniture simultanée d'autres services par plusieurs secteurs. Ainsi, les soins de santé ne peuvent pas être dispensés sans la fourniture simultanée d'électricité, d'eau et de services d'urgence.

Les dépendances peuvent avoir des effets d'intensité variable et être de types différents. En particulier, à la suite d'une attaque terroriste, les infrastructures critiques peuvent souffrir de :

- Dépendances physiques : le fonctionnement d'une infrastructure dépend de la production matérielle d'une autre infrastructure ;
- Dépendances informatiques : le fonctionnement d'une infrastructure dépend des informations transmises par une infrastructure d'information.

[17] CIPRNet Project, https://www.ciprnet.eu/home.html.

Étude de cas 10
Interdépendances et zones d'importance vitale en France

La France a mis en œuvre une stratégie de protection des infrastructures critiques dans laquelle elle a soulevé la question de la dépendance en introduisant le concept de zone d'importance vitale (ZIV). Une zone d'importance vitale est une aire dans laquelle sont implantés plusieurs points d'importance vitale (PIV) relevant d'OIV différents, pour lesquels une prise en compte commune de la sécurité présente une plus–value. Il y a ainsi interdépendance en termes de sécurité entre les PIV dès lors que :

- l'exécution d'une menace sur l'un d'eux aurait des conséquences sur l'intégrité ou l'activité des autres ; ou que
- les mesures de sécurité mises en œuvre pour l'un des points ou sur une partie commune ont une incidence sur la sécurité d'un ou de plusieurs autres PIV.

Il existe trois types de zone géographique :

- Cas 1 : une zone constituée de PIV voisins. Les PIV sont contigus ou situés à une distance relativement réduite les uns des autres ;
- Cas 2 : une zone constituée de PIV enclavés. Un PIV « 2 » se situe à l'intérieur d'un PIV « 1 » ;
- Cas 3 : une zone combinant les caractéristiques des deux premières.

Dans tous les cas, la création d'une zone d'importance vitale doit répondre à un besoin opérationnel et contribuer à améliorer la protection des PIV par la mise en commun et la rationalisation des moyens engagés. L'aire concernée doit s'entendre comme une zone présentant des caractéristiques homogènes, telles qu'il est possible d'en trouver dans certains aéroports, zones industrielles ou ports maritimes ou fluviaux.

Source : France, 2014.

Point essentiel, les dépendances augmentent les niveaux de vulnérabilité. Cette menace est d'autant plus grande que les organismes publics et le secteur privé dépendent largement des technologies de l'information et de la communication, ce qui aggrave l'effet des dépendances intersectorielles et transnationales. On a observé, à cet égard, que le cas de figure le plus préoccupant pour les experts est celui d'une cyber–attaque lancée sur des infrastructures critiques parallèlement à une attaque physique. Cette forme de cyberterrorisme pourrait amplifier les effets de l'attaque physique. Un attentat à la bombe classique contre un bâtiment, combiné à une attaque temporaire par déni de services privant les usagers de la distribution d'électricité ou du téléphone, pourrait en être un bon exemple. La perturbation des services d'intervention d'urgence qui en résulte, jusqu'à ce que les systèmes électriques ou de communication de secours puissent être mis en place et utilisés, pourrait accroître le nombre de victimes et semer la panique (Shea 2003, p. 9).

Lorsque les vulnérabilités se traduisent par des pannes à la suite d'une attaque terroriste, les dépendances peuvent produire des effets en cascade. Par exemple, le déversement de substances toxiques dans la chaîne d'approvisionnement en eau entraîne des défaillances du système de santé.

Il est crucial que les stratégies de protection des infrastructures critiques s'appuient sur les liens de cause à effet qui existent entre les interconnexions, les dépendances et les vulnérabilités des infrastructures critiques afin de remplir les objectifs suivants :

- Parvenir à un niveau adéquat de compréhension (de la part de toutes les parties prenantes concernées, qu'elles proviennent du secteur privé ou public) des points de vulnérabilité systémique, résultat qui devrait se traduire par une gestion plus précise des risques et des crises. L'intégration du concept de dépendance dans la gestion des risques et des crises est rendue plus complexe par le fait que les dépendances peuvent varier en fonction du mode de fonctionnement d'une infrastructure critique donnée. Par exemple, bien qu'un hôpital n'utilise pas en général de combustible diesel, il peut lui arriver, à la suite d'une panne du réseau électrique, de devenir subitement dépendant d'un approvisionnement en diesel pour faire fonctionner son groupe électrogène de secours. Il conviendrait que, dans les stratégies de protection des infrastructures critiques, les dépendances soient envisagées comme des interconnexions dynamiques et en évolution rapide et non comme des liens statiques ;
- Sensibiliser aux dépendances mutuelles par l'établissement de réseaux intersectoriels (sur la base, par exemple, de la discussion de scénarios de risques), afin de stimuler davantage la coopération entre les différents acteurs.

Étude de cas 11
Pays–Bas : ateliers intersectoriels et partage des connaissances sur les dépendances

Dans le cadre de leur stratégie de protection des infrastructures critiques, les Pays–Bas ont organisé une série d'ateliers intersectoriels qui ont permis aux secteurs concernés de mieux comprendre les effets des interdépendances. Les parties prenantes ont recensé les réseaux techniques et organisationnels dans lesquels les secteurs critiques opèrent. Grâce à ces ateliers, un ensemble d'acteurs publics et privés a pu anticiper différents scénarios de menace et en discuter. Il n'a été établi aucun modèle précis pour examiner les analyses de dépendance, l'idée sous–jacente étant que l'échange de connaissances par le réseautage et le partage d'expertise permettrait aux secteurs de prendre davantage conscience des dépendances et de la manière de faire face aux vulnérabilités. De plus, les parties prenantes concernées apprendraient à mieux à se connaître et seraient plus au fait de leurs capacités respectives, ce qui maximiserait les possibilités d'une coopération efficace en cas d'accident. Les différents scénarios abordés ont notamment permis d'examiner les questions suivantes :

- les effets des perturbations directes ou indirectes des infrastructures critiques, la chaîne d'approvisionnement, les questions d'accès, de rareté et d'intégrité, la période de perturbation, les caractéristiques du secteur et les facteurs humains ;
- les dépendances, les redondances et la reprise ;
- les mesures visant à réduire les vulnérabilités.

Source : RECIPE 2011, p. 32.

Les interconnexions et les dépendances dépassent souvent les frontières, et par conséquent les stratégies de protection des infrastructures critiques doivent également tenir compte de leur dimension internationale. Cet aspect est examiné plus avant au chapitre 6.

2.5 Concevoir l'architecture de protection des infrastructures critiques

Aucun modèle institutionnel, unique et prédéterminé n'impose aux pays une manière de protéger leurs infrastructures critiques. Les gouvernements doivent donc choisir le système le mieux adapté aux menaces auxquelles ils font face, à la taille et à la structure de leur économie, et plus généralement, à la culture de leurs politiques publiques et aux pratiques établies de leurs institutions. En particulier, les architectures de gouvernance élaborés en matière de protection des infrastructures critiques devraient tenir compte de la structure constitutionnelle de base du pays, par exemple, selon qu'il s'agit d'un État unitaire et centralisé ou fédéral et décentralisé. Cette prise en compte est particulièrement importante dans l'attribution des rôles et des responsabilités aux différents échelons de l'administration.

2.5.1 Principaux modèles de gouvernance

Les architectures de protection des infrastructures critiques oscillent entre deux modèles de base. À une extrémité du spectre, il y a une gouvernance des infrastructures critiques fondée sur certains principes : l'autoréglementation, la motivation et le respect volontaire des règles. Cette approche dite « volontaire » met l'accent sur les politiques axées sur des orientations non contraignantes. Toutes les parties prenantes (du secteur public ou privé) y sont encouragées à contribuer à la définition et à la mise en œuvre des politiques de protection des infrastructures critiques par des recommandations, la persuasion et le partage du sentiment d'un objectif poursuivi en commun. Le recours à la force contraignante de la législation et des régimes réglementaires est peu fréquent et uniquement en guise de complément, sauf dans certains secteurs (comme le nucléaire) où il peut jouer un rôle prédominant.

À l'autre extrémité, il y a l'approche dite « obligatoire » fondée sur l'idée que la meilleure façon de parvenir à une coopération dans le domaine de la protection des infrastructures critiques est d'établir des cadres juridiques contraignants, assortis de sanctions pour les exploitants d'infrastructures critiques qui ne respectent pas les normes requises dans les délais fixés.

Dans la pratique, les pays n'appliquent aucune de ces approches dans leur forme « pure » mais adoptent des éléments de chacune d'elles. Les systèmes mis en place ne peuvent donc être définis que comme étant principalement « volontaires » ou « obligatoires ». Par exemple, les États-Unis, le Royaume-Uni, le Canada et la Suisse entrent dans la première catégorie et la France, l'Espagne, la Belgique et l'Estonie dans la seconde.

Les pays peuvent avoir du mal à déterminer le système qui correspond le mieux à leurs besoins. En particulier, lorsqu'ils établissent des politiques de protection des infrastructures sensibles pour la première fois, il peut leur arriver d'adopter des structures et des processus qui peuvent, en définitive, se révéler inadéquats. C'est pourquoi ils mettent souvent en place des mécanismes garantissant une réévaluation périodique de leurs stratégies. Les États-Unis offrent l'exemple d'un pays qui est d'abord parti de la notion pure de participation volontaire des exploitants d'infrastructures critiques au processus. Bien que le système américain repose toujours sur ce principe, les États-Unis ont constaté au fil du temps la nécessité de renforcer leur cadre juridique

de protection des infrastructures critiques. Cela montre bien que les pays doivent tirer les leçons de leur expérience.

Les cadres institutionnels de protection des infrastructures critiques doivent, au minimum, couvrir les aspects suivants :

- Désigner l'organisme public chargé de coordonner la définition et la mise en œuvre de la stratégie nationale de protection des infrastructures critiques ;
- Attribuer les responsabilités de certains secteurs, généralement à différents ministères, sur la base d'une expertise et d'une compétence *ratione materiae* reconnues (par exemple, la sécurité alimentaire aux ministères de l'agriculture, la santé aux ministères de la santé, etc.) ;
- Déterminer la portée et les modalités de l'interaction entre les organismes gouvernementaux concernés et les exploitants d'infrastructures critiques. La section 4.5.2 examine de plus près les dynamiques en jeu du point de vue des partenariats public-privé.

Tableau 4 : Architecture de protection des infrastructures critiques de certains pays

Australie	Dans le système fédéral australien, les responsabilités des différents gouvernements en matière d'infrastructures critiques varient en fonction du type d'infrastructure ou de la nature de la menace. Le travail intergouvernemental est mené sur une base coopérative. Les gouvernements des États et Territoires sont responsables de la gestion des menaces qui pèsent sur la vie et les biens matériels relevant de leur compétence. Ils sont en charge de la préparation et de la réponse aux urgences et veillent au maintien de l'ordre public. Il leur arrive souvent également d'assurer certains services tels que dans les domaines de la santé et de l'approvisionnement en eau. Tous les gouvernements des États et Territoires australiens disposent de leurs propres programmes d'infrastructures critiques correspondant au contexte et aux modalités d'exploitation de ces dernières dans chaque entité. La stratégie de résilience des infrastructures critiques du Gouvernement australien vise à compléter ces programmes et à appuyer leurs objectifs dans la mesure du possible. Les gouvernements des États et Territoires participent également de manière déterminante au Trusted Information Sharing Network (TISN), le principal mécanisme de mobilisation du pays pour le partage de l'information entre entreprises et gouvernements et, d'autre part, les initiatives visant à renforcer la résilience. Le Gouvernement australien est responsable de la défense et de la sécurité nationales, ainsi que de l'aide à fournir aux États et Territoires pour répondre, à leur demande, aux situations d'urgence de grande ampleur. Il exerce également une surveillance réglementaire directe sur un certain nombre de secteurs d'infrastructures critiques, tels que l'aviation, les communications, l'exploitation pétrolière et gazière au large des côtes et les banques. Dans un certain nombre de cas, les agences de régulation concernées participent au TISN (à titre non réglementaire) dans le but de contribuer à la résilience de tel ou tel secteur.

États-Unis d'Amérique	La Secrétaire du Département de la sécurité du territoire fournit des orientations stratégiques et coordonne l'ensemble de l'effort fédéral. Les organismes fédéraux sectoriels dirigent les processus de collaboration en matière de sécurité dans chacun des 16 secteurs d'infrastructures critiques. Chaque organisme est chargé d'élaborer et de mettre en œuvre un plan adapté aux spécificités de chaque secteur. L'administration des États et les autorités locales, autochtones et territoriales veillent à la sécurité et à la résilience des infrastructures critiques sous leur contrôle, comme de celles détenues et exploitées par des parties tierces dans les limites de leurs compétences. Les mécanismes de collaboration entre, d'une part, les propriétaires et exploitants privés et, d'autre part, les organismes publics s'articulent autour de plusieurs structures de coordination sectorielles ou intersectorielles.
Royaume-Uni	Le Civil Contingencies Secretariat, qui fait partie du Secrétariat de la sécurité nationale, appuie le Premier Ministre et son Cabinet, et coordonne l'ensemble des efforts déployés par le Gouvernement en matière de planification et d'interventions civiles d'urgence. Les responsabilités propres au Civil Contingencies Secretariat en matière de politiques sont les suivantes : - L'estimation nationale des risques et l'inventaire national des risques (qui recense et évalue les risques pour la sûreté et la sécurité nationales relevant du terrorisme, des accidents industriels majeurs et des risques naturels, sur une période de cinq ans) ; - L'évaluation nationale des risques de sécurité (qui recense les risques mondiaux encourus par les intérêts du Royaume-Uni en matière de sécurité, sur une période de 5 à 20 ans). En collaboration avec les propriétaires d'infrastructures critiques et les autorités de réglementation, les ministères responsables des 13 secteurs critiques sont tenus de produire annuellement des plans de sécurité et de résilience sectoriels. Fondés sur les risques recensés dans l'estimation nationale y afférente, ces plans détaillent, d'une part, la manière dont chaque ministère perçoit les risques associés à son secteur et, d'autre part, les principales mesures envisagées pour y faire face au cours de l'année à venir. Plusieurs organismes fournissent à l'administration centrale, aux autorités de réglementation ainsi qu'aux propriétaires et exploitants d'infrastructures des conseils sur les risques encourus par les infrastructures et leur atténuation, comme en particulier le Centre chargé de la protection des infrastructures nationales et le Centre national de cybersécurité. Aucune sanction ni aucune autre conséquence n'est expressément prévue en cas de non-coopération d'un opérateur d'infrastructures critiques avec le Gouvernement.
Canada	L'architecture canadienne de protection des infrastructures critiques repose sur une approche particulièrement volontaire. Les responsabilités sont partagées par les gouvernements fédéral, provinciaux et territoriaux, les administrations

	municipales et les propriétaires et exploitants d'infrastructures critiques. Toutes ces parties prenantes sont représentées dans des réseaux sectoriels nationaux (pour chacun des dix secteurs d'infrastructures critiques recensés), dont les objectifs sont les suivants : - la promotion de l'échange, en temps opportun, de l'information ; - la détermination des questions d'intérêt national, régional ou sectoriel ; - l'exploitation des connaissances spécialisées des experts des secteurs des infrastructures critiques pour offrir des orientations quant aux difficultés actuelles et futures en matière d'infrastructures critiques ; et - l'élaboration d'outils et de pratiques exemplaires pour renforcer la résilience des infrastructures critiques couvrant tous les aspects de la prévention, de l'atténuation, de la préparation, de l'intervention et du rétablissement. La participation à ces réseaux est volontaire. Leurs membres dirigent également des plans de travail sectoriels. Pour maintenir une démarche exhaustive et concertée en vue d'améliorer la résilience des infrastructures critiques, un Forum national intersectoriel encourage la mise en commun de l'information entre les réseaux sectoriels et traite des interdépendances entre les différentes sphères de compétence ou les différents secteurs.
France	La coordination de la protection des infrastructures critiques est assurée par le secrétariat général de la défense et de la sécurité nationale (SGDSN) au nom du Premier Ministre. Le SGDSN approuve les directives nationales de sécurité (DNS) rédigées par les ministères coordonnateurs de chaque secteur critique. Ces ministères sont également les points de contact privilégiés des exploitants. Les préfets de zone et de département (c'est-à-dire les représentants de l'État dans un département ou une région) agissent sous la direction générale du Ministère de l'intérieur en tant qu'acteurs territoriaux en charge de la coordination du dispositif de protection des infrastructures critiques. Une fois désignés, les exploitants doivent répondre à plusieurs types d'obligations : la désignation d'un délégué pour la défense et la sécurité (interlocuteur privilégié de l'autorité administrative), la rédaction d'un plan de sécurité d'opérateur (PSO), l'élaboration d'un plan de sécurité d'opérateur (PSO) qui décrit l'organisation et la politique de sécurité de l'opérateur et la rédaction de plans particuliers de protection (PPP) pour chacun des points d'importance vitale identifiés. Le contrôle de la conformité des niveaux de sécurité des points d'importance vitale avec les exigences minimales attendues sur le site est confié à la commission interministérielle de défense et de sécurité et à la commission zonale de défense et de sécurité appuyées par les préfets départementaux. Les rapports de contrôle visent à mettre en évidence les vulnérabilités des points d'importance vitale face aux menaces identifiées et les mesures à prendre pour renforcer la résilience. Dans des cas extrêmes de non-respect, le contrôle peut conduire à la saisine de

	l'autorité judiciaire aux fins de poursuites à l'encontre de l'auteur du délit et d'application de sanctions pénales en cas de violation des réglementations.
Espagne	Le Secrétaire d'État à la sécurité, par l'intermédiaire du Centre national pour la protection des infrastructures critiques, est le plus haut échelon du Ministère de l'intérieur qui soit en charge du système de protection des infrastructures critiques. Pour chaque secteur stratégique, au moins une entité de l'Administration générale de l'État a la responsabilité de promouvoir, dans le cadre de ses compétences, les politiques de sécurité du Gouvernement et d'assurer leur application. En termes de mobilisation des exploitants d'infrastructures critiques, l'Espagne est un exemple typique d'« approche obligatoire ». Le système repose sur des dispositions réglementaires détaillées prévoyant l'adoption de divers niveaux de plans stratégiques et de sécurité dont l'élaboration et l'approbation incombent à différents acteurs dans des délais précis. En particulier : a) Le plan national de protection des infrastructures critiques établit des critères et des directives afin de mobiliser les capacités opérationnelles des administrations publiques en coordination avec les exploitants ; b) Les plans stratégiques sectoriels permettent de déterminer la portée des services essentiels dans chacun des secteurs recensés, les vulnérabilités du système, les conséquences potentielles de l'inactivité et les mesures stratégiques nécessaires pour assurer la résilience du système ; c) Les plans de sécurité de l'opérateur définissent les politiques générales des exploitants touchant à la sécurité des installations ou des systèmes qu'ils possèdent ou gèrent et doivent être soumis dans un délai de six mois à compter de l'avis de nomination de l'opérateur par le Ministère de l'intérieur ; d) Les plans de protection spécifiques déterminent les mesures concrètes déjà adoptées et celles à adopter par les exploitants pour garantir la sécurité (physique et logique) de leur infrastructures critiques, plans qui doivent être soumis dans les quatre mois suivant l'approbation du plan de sécurité de l'opérateur par le Ministère de l'intérieur ; e) Les plans d'appui opérationnel énoncent les mesures concrètes que les administrations publiques doivent mettre en œuvre pour appuyer les exploitants d'infrastructures critiques.
Pays-Bas	La responsabilité première de la continuité et de la résilience des processus relatifs aux infrastructures critiques est assumée par leurs exploitants mêmes. Ces derniers ont ainsi la charge de comprendre les menaces, les vulnérabilités et les risques, et de mobiliser et de maintenir les capacités permettant d'améliorer et de préserver la résilience desdits processus. Le ministère concerné établit les cadres généraux des secteurs sous sa responsabilité (en matière de politiques ou de lois et de réglementations). Les ministères doivent protéger et contrôler les capacités relatives aux infrastructures critiques en association avec les exploitants des processus de ces infrastructures. Les mécanismes de sûreté et de

	sécurité des régions offrent un appui aux exploitants de ces processus en cas de perturbation ou de défaillance (imminente) si les capacités ne sont pas appropriées et que la sécurité et l'ordre publics sont menacés. Cet appui intervient en coordination avec les exploitants des processus en question et les ministères. La multiplicité et la diversité des parties prenantes rendent nécessaires des efforts de coordination et de gestion. Le coordinateur national pour la sécurité et la lutte contre le terrorisme du Ministère de la justice et de la sécurité est responsable des tâches de coordination et de gestion.
Allemagne	L'architecture de protection des infrastructures critiques du pays repose sur la définition de six programmes de travail correspondant aux différentes phases du cycle de gestion des risques. Le secteur public (sous la coordination du Ministère fédéral de l'intérieur) dirige la mise en œuvre des quatre premiers programmes avec la collaboration du secteur privé et des exploitants. Pour la mise en œuvre des programmes 5 et 6, les rôles sont inversés, ce sont donc les entreprises et les exploitants qui dirigent le processus. Ces programmes de travail sont les suivants : 1. Définition des objectifs généraux de protection ; 2. Analyse des menaces, des vulnérabilités et des capacités de gestion ; 3. Évaluation des risques ; 4. Définition plus précise des objectifs de protection en tenant compte des mesures de protection déjà en place ; analyse des réglementations existantes et, le cas échéant, proposition de mesures complémentaires pouvant contribuer à atteindre l'objectif visé ; si besoin est, établissement de dispositions législatives ; 5. Mise en œuvre de mesures de réalisation de l'objectif visé, principalement au moyen : i) de solutions spécifiques à une association et de réglementations internes ; ii) d'accords d'engagement volontaire conclus par les entreprises et l'industrie ; iii) de l'élaboration de concepts de protection par les entreprises ; 6. Processus continu et intensif de communication des risques (dialogue sur les résultats des analyses, les évaluations, les objectifs de protection et les mesures possibles). Le système prévoit un certain nombre de plateformes institutionnalisées faisant intervenir les pouvoirs publics, les entreprises et les associations. Ces plateformes de partenariat en matière de sécurité peuvent être organisées sous les formes suivantes : - tables rondes sur la protection des infrastructures critiques (au niveau fédéral) ; - tables rondes sur la protection des infrastructures critiques [au niveau des Länder (États)] ; - tables rondes sur la protection des infrastructures critiques (au niveau des administrations locales) ; - tables rondes conjointes entre les autorités fédérales et des Länder ou entre les autorités des Länder et des collectivités locales.

2.5.2 Partenariats public-privé pour la protection des infrastructures critiques

Dans la plupart des pays, la grande majorité des biens considérés comme des infrastructures critiques appartiennent à des particuliers. De plus, les exploitants privés sont à la pointe des investissements et des efforts visant à développer de nouvelles technologies de production et de protection. Combinés au fait que la responsabilité principale de la protection des biens et systèmes considérés comme des infrastructures critiques incombe à leurs propriétaires ou exploitants, ces différents éléments soulignent l'importance d'établir des partenariats public-privé efficaces afin d'atteindre un niveau adéquat de résilience.

Lorsqu'ils traitent des partenariats public-privé, les rédacteurs des stratégies de protection des infrastructures critiques devraient s'efforcer de créer les conditions garantissant leur efficacité : i) en appréciant les facteurs favorables et défavorables ; ii) en définissant leur champ d'application ; iii) en définissant leurs formes ; iv) en anticipant les problèmes et les défis.

i) Apprécier les facteurs favorables et défavorables aux partenariats public-privé

Forum ouvert destiné à l'échange d'idées sur la protection des infrastructures critiques et à la collaboration entre les hauts responsables politiques, le processus Meridian a recensé comme essentiels à l'efficacité des partenariats public-privé les facteurs suivants (GFCE-Meridian 2016, p. 55) :

La confiance : étant donné que les partenariats public-privé touchent souvent à des questions délicates (du point de vue commercial ou bien en termes de réputation, de sécurité ou de transfert de responsabilités), il est essentiel de créer un climat de confiance dans lequel toutes les organisations sont conscientes du besoin de discrétion des unes et des autres et agissent de manière cohérente en conséquence. Des directives d'affiliation claires sur les règles de fonctionnement peuvent favoriser l'instauration d'un climat de confiance.

L'intérêt : la participation à un partenariat public-privé doit être bénéfique, sinon la motivation retombe rapidement ;

Le respect : toutes les organisations doivent reconnaître et respecter ce qu'apportent les autres organisations à cette collaboration. Ce respect peut s'obtenir en « vantant » ce que vous-mêmes apportez au partenariat (du point de vue de votre partenaire) tout en cherchant activement ce que vos partenaires vous apportent ;

Le code de conduite : il est nécessaire d'avoir des règles claires, spécifiques et prévisibles qui n'offrent aucune marge d'appréciation et empêchent tout conflit d'intérêts ;

La conscience des possibilités et des limites de chacun : cette prise de conscience prévient tous conflits résultant d'une mauvaise appréciation des raisons d'une réponse négative et permet de tirer le meilleur parti des efforts entrepris dans le cadre du partenariat. Cela suppose que les deux organisations connaissent leurs activités respectives. Un bon moyen d'y parvenir est d'avoir travaillé ensemble pendant une longue période, de préférence des années ;

Des attentes réalistes : toutes les organisations doivent tenir compte, entre autres, de l'accessibilité des ressources et du budget de développement pour être en mesure d'avoir des attentes réalistes en matière de partenariat.

ii) Définir le champ d'application des partenariats public-privé

Les partenariats public-privé ne devraient pas se concentrer sur une étape particulière du cycle de la protection des infrastructures critiques, mais englober toutes les étapes, depuis les phases de conception et de mise en œuvre des mesures jusqu'aux phases de gestion des risques et des crises. Les avantages de la mutualisation des ressources, du soutien mutuel et de la prise de décision conjointe entre le secteur public et les exploitants privés d'infrastructures critiques s'étendent à des domaines tels que, notamment, l'évaluation des conditions de sécurité, l'examen des mesures de sécurité, le recensement des biens considérés comme des infrastructures et des processus connexes, l'élaboration de plans d'intervention et la formation du personnel d'intervention en cas de problème de sécurité.
Dimension cruciale (bien que non exclusive) des partenariats public-privé, le partage de l'information soulève des défis particuliers, par exemple dans le domaine de la protection des données. Les questions liées au partage de l'information sont examinées au chapitre 4.

iii) Définir la forme des partenariats public-privé

La forme la plus appropriée d'un partenariat donné dépend de multiples considérations telles que les objectifs recherchés, le nombre de parties prenantes et le fait que les questions à traiter par le partenariat soient d'ordre stratégique ou opérationnel. Les partenariats public-privé peuvent prendre diverses formes, depuis des types de coopération très informels jusqu'à des cadres plus formels. Le degré de formalité atteint est souvent lié au niveau de contrôle que les organismes gouvernementaux souhaitent exercer. Sous un autre angle, on a fait valoir que les partenariats public-privé axés sur des projets tendent à être plus efficaces que ceux axés sur des processus, car les premiers comprennent généralement des missions, des calendriers et des budgets plus clairement définis (Kolesnikova 2017, p. 13-15).

ÉTUDE DE CAS 12
Partenariats public-privé pour la résilience des infrastructures critiques en Finlande

Créée en 1993, l'Agence nationale d'approvisionnement d'urgence (NESA) est chargée de planifier, développer et maintenir la sécurité de l'approvisionnement en Finlande. Bien que son rôle historique de maintien des stocks de réserve aux fins de la protection des moyens de subsistance de la population ainsi que du fonctionnement de l'économie demeure l'une de ses tâches stratégiques, la NESA travaille de plus en plus activement au recentrage de la continuité et de la résilience des opérations dans divers secteurs de l'économie grâce à des partenariats public-privé. Elle a établi un réseau de groupes thématiques où les principales parties prenantes des secteurs d'infrastructures critiques établissent des partenariats afin d'évaluer leur vulnérabilité et leur performance et de planifier leur résilience. Elle propose également des outils spécialisés, tels que des systèmes d'information et des installations de stockage et de transport permettant de soutenir la continuité des opérations dans ces domaines. Elle finance en outre certaines activités liées à la continuité des opérations et à la protection des infrastructures critiques. L'agence établit des rapports annuels qui évaluent la performance des entreprises dans les secteurs d'infrastructures critiques et qui sont assortis d'un classement et de recommandations particulières. Parmi ses résultats, la NESA s'enorgueillit d'un nombre accru de partenariats public-privé conclus avec des entreprises dans les secteurs d'infrastructures critiques (plus de 1 000 à ce jour) qui ont tous donné lieu à un plan de continuité des opérations spécifique à leurs activités et à leur secteur.

Source : OCDE, Toolkit for Risk Governance, consultable à l'adresse : www.oecd.org/governance/toolkit-on-risk-governance/home/

iv) Anticiper les défis des partenariats public-privé

Les partenariats public-privé qui ne sont pas adéquatement conçus risquent de devenir des « boîtes vides », n'apportant que peu, voire aucune valeur ajoutée à la protection des infrastructures critiques. Pour que des accords de coopération entre secteur public et secteur privé voient le jour et continuent d'être bien conçus et productifs, il est nécessaire que les pays tiennent compte des raisons les plus fréquentes de leur échec. Ce dernier peut être lié, entre autres, à des attentes différentes entre secteur privé et secteur public, à des modèles de financement non viables ou à un manque de clarté dans la répartition des tâches. On peut soutenir que les préférences et les perceptions coûts-avantages des parties prenantes détermineront finalement le succès ou l'échec du partenariat. Un sentiment d'urgence contribue à créer un lien entre les secteurs public et privé, ce qui renforce la volonté de collaborer et de parvenir à une vision commune et, en définitive, permet au partenariat de mûrir et de s'inscrire dans la durée. La longévité des partenariats dépend de l'interaction de ces facteurs, et il s'agit là d'un processus dynamique marqué par des périodes de performance tantôt faible et tantôt forte. (Kolesnikova 2017, p. 13-15).

D'autres défis à relever peuvent être liés au manque de motivation des entreprises quant au fait d'investir financièrement dans la protection de leurs propres infrastructures critiques. La section 2.10.1 traite de la nécessité d'établir des stratégies de protection des infrastructures critiques propres à déterminer les types de mesures incitatives appropriées à cet égard.

L'OSCE a élaboré des orientations en huit étapes sur la manière dont les pays devraient maximiser les avantages à tirer des partenariats public-privé en valorisant les intérêts communs de toutes les parties prenantes concernées. Certes, ces orientations s'inscrivent dans le cadre des bonnes pratiques destinées

aux infrastructures énergétiques critiques, mais elles semblent bien applicables, en général, à tous les secteurs (OSCE 2013, p. 69) :

- Étape 1 : analyser et identifier la motivation de chaque partenaire à être inclus dans les partenariats de protection des infrastructures critiques afin de clarifier les attentes et contributions mutuelles ;
- Étape 2 : définir les ambitions et les objectifs des partenariats de protection des infrastructures critiques en fonction des objectifs nationaux ; clarifier l'objectif de ces partenariats et les tâches à accomplir (voir aussi l'étape 5) ;
- Étape 3 : examiner le cadre réglementaire existant pertinent pour chaque secteur des infrastructures critiques ; recenser les normes, règles et principes obligatoires et volontaires ; évaluer l'adéquation du cadre réglementaire existant au regard des risques prévisibles et des niveaux de préparation existants ; discuter de la façon de combler les éventuelles lacunes ;
- Étape 4 : établir des mécanismes, des mesures de protection et une sécurité juridique pour l'échange d'informations relatives à la protection des infrastructures critiques entre toutes les parties prenantes concernées, ainsi que des mécanismes pour les efforts volontaires, y compris l'élaboration et l'échange de pratiques exemplaires, la consultation et le dialogue, et ce afin d'assurer un partenariat continu et efficace ;
- Étape 5 : mettre en place une structure institutionnelle qui favorise la coopération et l'échange d'informations entre les organisations ; clarifier les rôles et les contributions de chaque partenaire (organismes gouvernementaux, propriétaires et exploitants d'infrastructures critiques, fournisseurs de produits ou associations) ; désigner un point de contact unique pour chaque partenaire et établir des directives de coopération ;
- Étape 6 : faire d'abord preuve de modestie en se concentrant sur un ou deux secteurs d'infrastructures critiques ; puis, donner régulièrement de l'ampleur aux partenariats en misant sur la volonté de toutes les parties prenantes de coopérer et d'examiner les niveaux de menace ;
- Étape 7 : poser des jalons permettant de se pencher sur ce qui a été accompli et déterminer les prochaines étapes envisageables ;
- Étape 8 : prévoir une procédure régulière d'examen afin de revoir et mettre à jour les partenariats existants, de manière à assurer la continuité des progrès continus à la hauteur de l'ensemble des risques encourus et des mesures de sécurité et de sûreté propres à garantir un niveau optimal de protection.

ÉTUDE DE CAS 13
UP KRITIS : la plateforme allemande de partenariat public-privé en matière de protection des infrastructures critiques

Institutionnalisée en 2007 et adaptée en 2013, UP KRITIS est la plateforme public-privé mise en place par l'Allemagne en vue d'établir une coopération sectorielle et intersectorielle dans le domaine de la protection des infrastructures critiques. Son action repose sur la confiance mutuelle. Les participants à cette plateforme mettent en commun savoir-faire et expériences et partagent les enseignements qu'ils ont tirés en matière de protection des infrastructures critiques. UP KRITIS est le cadre dans lequel les concepts prennent forme, les contacts s'établissent, les exercices se tiennent et une approche commune de la gestion des crises informatiques s'élabore et voit le jour. Parallèlement, UP KRITIS traite de questions qui débordent du domaine de l'informatique, étant entendu qu'un examen séparé de la sûreté physique et de la sécurité informatique n'est pas suffisant pour atteindre l'objectif commun de protection des infrastructures critiques.

UP KRITIS propose deux formes de coopération : une coopération opérationnelle et technique (entre tous les participants) et une collaboration stratégique et conceptuelle (au sein des entités en place). Point essentiel, les activités sont menées progressivement et peuvent être plus ou moins intenses selon le degré de participation des entreprises, l'objectif étant de veiller à ce que le système reste gérable tout en approchant autant d'entreprises que possible dans tous les secteurs d'infrastructures critiques. Une entité est d'abord intégrée dans UP KRITIS en tant que « participante ». Tous les exploitants d'infrastructures critiques basés en Allemagne, les associations professionnelles et sectorielles nationales des différents secteurs d'infrastructures critiques ainsi que les autorités gouvernementales compétentes peuvent demander à devenir participants d'UP KRITIS. Les entités participantes désignent leurs représentants auxquels est accordé l'accès aux produits d'UP KRITIS, y compris des informations confidentielles. Si une entité souhaite collaborer plus activement, elle peut devenir « partenaire » et demander l'intégration de ses représentants dans des groupes de travail sectoriels et thématiques. Chaque groupe de travail constitue son réseau d'information, dans le cadre duquel il est possible d'échanger des renseignements de manière confidentielle.

Le Plénum et le Conseil constituent d'autres éléments clefs de la structure organisationnelle. Le Plénum est le comité de coopération du système. Il intervient dans l'ensemble des secteurs en mettant en place les principales activités stratégiques d'UP KRITIS, en décidant de la création ou de la dissolution de groupes de travail, en planifiant de futures actions conjointes, etc. Il est composé de représentants des exploitants d'infrastructures critiques, de leurs associations professionnelles et sectorielles ainsi que de représentants du secteur public. Le Conseil, lui, renforce le partenariat et la coopération au sein d'UP KRITIS et contribue activement à la réalisation des objectifs et projets stratégiques. Il veille également à la bonne exécution des tâches de la plateforme à l'aide de ressources adéquates et avec l'appui nécessaire de la direction des secteurs public et privé. Il est composé de décideurs de haut niveau issus des exploitants d'infrastructures critiques et du secteur public.

Source : UP KRITIS 2014

2.5.3 Le rôle de la société civile et du public

Le grand public a un rôle important à jouer à la fois dans la prévention des attaques contre les infrastructures critiques et dans la réduction des dommages à l'issue d'une attaque (gestion des crises). Certains pays prévoient explicitement et activement le rôle dévolu aux personnes dans le cadre des stratégies de protection des infrastructures critiques. En France par exemple, le Plan Vigipirate[18] explique à la population comment se comporter en cas d'attaques dans certaines situations qui intéressent la protection des infrastructures critiques, comme dans le métro, dans un train et à bord d'un avion ou d'un navire, ou bien en cas d'attaques au moyen de substances toxiques. La Suède, quant à elle, met en pratique une stratégie à l'échelle de l'ensemble de la société, la constatation ayant été faite que les personnes et les familles sont souvent celles qui sont le plus directement touchées par une crise ou qui se trouvent sur les lieux avant l'arrivée des premiers intervenants et autres représentants de la société, preuve qu'il conviendrait de considérer les personnes comme des atouts (Lindberg & Sundelius 2013, p. 1304).

Les méthodes et les voies à suivre pour obtenir la collaboration du public diffèrent considérablement de celles qui sont nécessaires pour mobiliser les exploitants d'infrastructures

[18] http://www.gouvernement.fr/vigipirate.

critiques. Pour commencer, la participation de la population et des personnes à l'ensemble des efforts menés en faveur de la résilience des infrastructures critiques implique l'adoption de programmes d'éducation et de campagnes de sensibilisation à grande échelle. Les stratégies de communication devraient donc s'adapter aux différents groupes cibles. Elles peuvent s'appuyer, au niveau local et en fonction du contexte, sur des mesures telles que la mise en service de numéros d'urgence spéciaux ou encore la répétition de messages transmis par haut-parleurs et rappelant aux usagers des transports publics leurs obligations de signalement. À la suite des vagues d'attentats terroristes perpétrés dans les réseaux de transport de grandes capitales ces vingt dernières années, les administrations publiques de plusieurs pays ont par exemple pris des mesures pour inviter la population à être vigilante et à signaler aux autorités les situations suspectes.

L'utilisation généralisée d'appareils technologiques par le public incite également à conclure que les médias sociaux peuvent jouer un rôle essentiel pour accroître la prise de conscience du problème par le public, informer ce dernier des mesures prises par le gouvernement et diffuser des consignes de sécurité en temps opportun. Tout cela semble particulièrement important étant donné l'évolution rapide de la situation.

ÉTUDE DE CAS 14
Le Système d'alerte et d'information aux populations ou SAIP (France)

Élaborée par la Direction générale de la Sécurité civile et de la gestion des crises (DGSCGC) du Ministère de l'intérieur, en collaboration avec le Service d'information du Gouvernement (SIG), l'application mobile SAIP permet d'alerter les citoyens d'être alertés sur leur téléphone en cas d'attaque supposée ou d'événement à caractère exceptionnel résultant probablement d'une attaque.
Les consignes de sécurité transmises aux usagers de l'application les invitent à prendre certaines mesures particulières : trouver refuge dans un bâtiment, évacuer une zone dangereuse, éviter d'appeler (sauf en cas d'urgence médicale), ne pas aller chercher ses enfants à l'école, etc. Son déclenchement et le contenu du message sont réservés à une autorité chargée de la protection générale de la population, de l'ordre public et de la défense civile. Sur le terrain, cette compétence est détenue par le maire et le préfet de département. Cette application complète le Système d'alerte et d'information aux populations (SAIP) et fait partie d'une approche globale de sensibilisation de la population aux risques encourus.

Source : www.gouvernement.fr/risques/l-application-d-alerte-mobile-saip.

2.6 Élaboration des stratégies de protection des infrastructures critiques axées sur les concepts de gestion des risques et de gestion des crises

Pour garantir l'efficacité de toute stratégie nationale, les processus de gestion des risques et de gestion des crises devraient être mis au centre des efforts de protection des infrastructures critiques. Quel que soit le modèle institutionnel retenu, les parties prenantes à la protection des infrastructures critiques (qu'il s'agisse de propriétaires ou d'exploitants publics ou privés d'infrastructures critiques ou bien encore des pouvoirs publics) doivent maîtriser ces concepts et les appliquer de manière cohérente à leurs secteurs et domaines de compétence respectifs.

2.6.1 Gestion des risques

Le Bureau des Nations Unies pour la prévention des catastrophes définit la gestion des risques comme « l'adoption systématique d'une démarche et de pratiques consistant à gérer l'incertitude afin de minimiser les dommages et pertes possibles. La gestion des risques comprend l'estimation des risques et l'analyse des risques ainsi que l'application de stratégies et de mesures spécifiques afin de contrôler, de réduire et de transférer les risques » (Bureau des Nations Unies pour la prévention des catastrophes, 2009).

Dans le cadre des processus de gestion des risques tels qu'ils s'appliquent à la protection des infrastructures critiques, il est important de bien comprendre les concepts clefs qui sont souvent (et à tort) utilisés de façon interchangeable, notamment les suivants :

- *Menace* : tout ce qui exploite la vulnérabilité d'une infrastructure critique ;
- *Vulnérabilité* : toute faiblesse d'une infrastructure critique qui peut être exploitée par une menace ;
- *Risque* : risque de pertes, de dommages, de destruction ou de perturbation de la capacité d'une infrastructure critique de fournir ses services, résultant de l'exploitation d'une vulnérabilité par une menace.

Il n'existe pas de norme unique ou universelle dans le domaine de la gestion des risques. L'utilisation de cahiers des charges différents par les diverses parties prenantes chargées de cette tâche peut aboutir à des résultats incompatibles. À l'échelon des pays, l'emploi de méthodes différentes peut compliquer, voire rendre impossible, la comparaison des résultats dans un même secteur et entre secteurs, ce qui risque d'influer sur la fiabilité de l'exercice dans son ensemble. Il importe donc que les pays soutiennent la mise en place du processus de gestion des risques compte tenu, au minimum, des éléments suivants :

- Mise en contexte – établir la portée et les paramètres de l'évaluation des risques ;
- Évaluation des risques (recenser, analyser, estimer) – transformer les données relatives aux risques en informations permettant la prise de décisions ;
- Réduction des risques – traduire les informations relatives aux risques en décisions et en mesures d'atténuation ;
- Tout au long du processus :
- Communication et consultation – déterminer les méthodes de communication utilisées par toutes les parties prenantes tout au long du processus ;
- Suivi et examen – procéder régulièrement à des vérifications ou à des contrôles en vue d'une meilleure gestion des risques, de la détection des changements intervenus dans le contexte des risques existants et du recensement de nouveaux risques.

Afin de garantir le choix de mesures de sécurité préventives adaptées, le système de gestion des risques devrait présenter de manière détaillée les mécanismes utilisés pour obtenir des informations fiables sur les menaces et procéder à des évaluations de risques, en tenant compte des situations et des environnements à l'échelon international, national et régional. Les mesures de sécurité et les procédures y relatives devraient être flexibles et proportionnelles à l'évaluation

des risques qui peut fluctuer en fonction de diverses variables. Ce système devrait être mis en œuvre dans les délais et avec efficacité de manière à garantir que l'évaluation des risques en résultant est toujours à jour, exacte et complète.

Au niveau international, en publiant la norme ISO 31000, l'Organisation internationale de normalisation a établi un paradigme universellement reconnu dans ce domaine, qu'elle définit comme un « ensemble d'éléments établissant les fondements et dispositions organisationnelles présidant à la conception, la mise en œuvre, la surveillance, la revue et l'amélioration continue du management du risque dans tout l'organisme[19]. » Point essentiel, la norme ISO 31000 n'est pas particulière à une industrie ou à un secteur donné.

ÉTUDE DE CAS 15
Méthode d'évaluation des risques dans le domaine de la sûreté de l'aviation (OACI)

Conçue par l'OACI, la méthode d'évaluation des risques dans le domaine de la sûreté de l'aviation vise à faire comprendre en quoi consiste un risque résiduel courant et à en établir un classement relatif dans la perspective de l'élaboration de politiques. Bien que la mise au point de cette méthode réponde au souci de faire face aux menaces pesant sur l'aviation civile, la plupart de ses éléments peuvent être considérés, d'une manière générale, comme applicables. Ce processus d'évaluation des risques comprend les éléments suivants :

- recensement et analyse de scénarios de menace vraisemblable et probabilité d'occurrence de ceux-ci, ainsi que de leurs conséquences ;
- évaluation des mesures d'atténuation des risques en place et des vulnérabilités persistantes ;
- évaluation des risques résiduels en tenant compte de la probabilité d'occurrence d'un scénario de menace particulier, de ses conséquences et des vulnérabilités qui lui sont associées ;
- recommandations quant à de futures actions en fonction des risques et à d'éventuelles mesures d'atténuation.

Les principaux éléments issus de la réalisation de l'évaluation des risques sont les suivants :

Scénario de menace : détermination et description d'un acte crédible d'intervention illicite comprenant les éléments suivants : une cible (aérogare, infrastructure connexe ou aéronef, ou toute autre infrastructure critique), le mode opératoire (y compris moyens de transport et dissimulation), les méthodes d'attaque utilisées (par exemple, un engin explosif improvisé) et l'adversaire (en fonction de son rôle au regard du système aéronautique – passager, personne qui ne voyage pas ou personne qui travaille sur place). Ces informations doivent être suffisamment détaillées pour permettre une évaluation et une analyse précises ; une description du type « attaque contre un aéronef » ne constitue pas en soi un scénario assez complet, alors que tel est le cas sous cette forme : « un passager attaque une aérogare au moyen d'un engin explosif improvisé (EEI) dissimulé dans un bagage de soute » ;

Probabilité d'occurrence d'une attaque (menace) : probabilité d'une tentative d'attaque (scénario de menace), évaluée d'après les intentions et capacités des terroristes mais NE prenant PAS en compte les

[19] ISO 31000:2009(fr), consultable à l'adresse suivante : www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:fr.
Adoptant la même approche de gestion des risques que la norme ISO 31000, la série ISO 27000 constitue la norme de référence dans le domaine des systèmes de sécurité de l'information. La norme ISO 27000 offre donc un cadre d'orientation utile pour la protection des infrastructures d'information critiques.

mesures de sécurité en place. La probabilité sert d'indice de menace et prend en considération les intentions et capacités des terroristes de mettre à exécution un scénario de menace ;

Conséquences : nature et ampleur des conséquences de l'attaque sur le plan humain, économique et politique et sur le plan de la réputation, dans le scénario le moins favorable qui puisse raisonnablement être envisagé ;

Mesures d'atténuation en place : normes et pratiques recommandées pertinentes (ne figurant peut-être pas toutes dans l'annexe 17 de la Convention relative à l'aviation civile internationale et devant, en général, être effectivement appliquées, leur non-application entraînant une augmentation du risque) ou autres programmes et réglementations nationaux ou locaux applicables visant à nuire au succès d'une attaque probable ou à en atténuer les conséquences si celle-ci devait se produire. On part du principe qu'aucune menace ne peut être entièrement éliminée ;

Vulnérabilité *:* vulnérabilités persistantes une fois que les mesures d'atténuation en place ont été prises en compte ;

Risque : persistance du risque global de réussite d'une attaque, dans l'hypothèse de la mise en œuvre des mesures d'atténuation, compte tenu de la probabilité d'occurrence de la menace et des conséquences encourues ;

Autres mesures d'atténuation possibles : mesures arrêtées que l'OACI ou les États membres pourraient mettre en application pour atténuer encore les risques résiduels, si nécessaire.

Il importe que l'évaluation des risques recense avec soin et de façon suffisamment détaillée les scénarios plausibles, chaque forme de menace étant clairement définie et examinée sous tous les angles. Les menaces pourraient viser certains aéroports, aérogares ou autres infrastructures, telles que des parcs de stockage du carburant, des bâtiments abritant les activités relatives au contrôle de la circulation aérienne ou du matériel de navigation, ainsi que des aéronefs, notamment différentes formes d'aviation, comme l'aviation générale, les aéronefs de passagers et les avions tout cargo. Les moyens et méthodes par lesquels une menace pourrait être mise à exécution devraient également être évalués. Cette évaluation porterait sur la façon de fabriquer une arme ou un engin explosif, les moyens de les transporter (qu'ils le soient, par exemple, par une personne ou dans un véhicule) et la personne responsable de leur transport (par exemple, un membre du personnel, un passager ou un citoyen quelconque), la manière de les dissimuler, de les utiliser ou de les activer afin de commettre un acte d'intervention illicite. Toutefois, une telle évaluation ne couvre pas la liste complète des scénarios possibles et les États ou autres entités procédant à des évaluations des risques sont encouragés à élaborer leurs propres versions en tenant compte des réalités locales, selon qu'il convient.

Certains pays, notamment les États-Unis et le Canada, ont élaboré des programmes publics de manière à inciter plus particulièrement les exploitants d'infrastructures critiques à adopter un cadre d'évaluation commun. Ces programmes sont aussi conçus pour fournir une assistance technique dans le cadre de la réalisation des évaluations selon une « démarche douce », qui repose sur des mesures incitatives et des plans axés sur une approche volontaire.

ÉTUDE DE CAS 16
Programme d'évaluation de la résilience régionale du Canada (PERR)

Le PERR est un programme complet d'évaluation des risques à l'intention des propriétaires et exploitants d'infrastructures critiques au Canada. Ce programme comporte des évaluations de sites destinées à aider les organisations à mesurer et à accroître leur résilience à tous les risques au Canada, comme les cybermenaces, les événements anthropiques accidentels ou intentionnels et les catastrophes naturelles. Les évaluations de sites sont volontaires, non réglementaires, gratuites et confidentielles.

- Pour renforcer la résilience des infrastructures critiques, le PERR utilise trois principaux outils :
- Outil d'évaluation de la résilience des infrastructures critiques : outil d'évaluation sur le terrain, qui évalue les mesures de résilience et de protection d'une installation ;
- Outil multimédia pour les infrastructures critiques : logiciel multiplateforme qui génère un rendu visuel interactif de l'installation d'une infrastructure critique et présente des photos panoramiques à 360 degrés ;
- Examen de la cyberrésilience du Canada : outil d'évaluation sur le terrain qui mesure le degré de cyberrésilience d'une organisation.

Ce programme propose également des ateliers, des réunions, des produits géospatiaux et des entretiens avec des experts en la matière. Les résultats des évaluations visent à aider les propriétaires et exploitants à cerner les dépendances et les vulnérabilités dans leur organisation. Les évaluations de sites permettent aussi de définir un volet de mesures rentables et optionnelles pour aider les propriétaires et exploitants à atténuer les risques et à accroître leur capacité d'intervention en cas de perturbations et de rétablissement par la suite. En particulier, le PERR contribue à l'obtention des résultats suivants :

- Une meilleure gestion des risques – le programme fait mieux comprendre à l'organisation ses vulnérabilités, au moyen d'outils d'évaluation fiables.
- Un renforcement des relations avec le Gouvernement – le programme favorise les relations avec différentes administrations, y compris les premiers intervenants.
- Une sensibilisation accrue de la cybersécurité – le programme aide à mieux comprendre le degré de préparation d'une organisation à des cyberattaques et autres cybermenaces.

D'autres éléments clefs sont à prendre en considération pour les propriétaires et exploitants d'infrastructures critiques :

- Investissement minimal de temps et de ressources – les services du PERR sont offerts rapidement et gratuitement.
- Sécurité – Sécurité publique Canada protégera le caractère confidentiel des documents et de l'information fournis par les propriétaires et exploitants d'infrastructures critiques.

Source : Sécurité publique Canada, consultable à l'adresse suivante : www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-fr.aspx.

2.6.2 Gestion des crises

La gestion des crises détermine les processus à activer lorsque des menaces se matérialisent. Les étapes de la gestion des crises sont, entre autres, les suivantes :

- Identifier une crise ;
- Planifier des réponses appropriées à la crise ;
- Faire face à la crise et la régler.

Sur le plan terminologique, il arrive qu'en matière de gestion de crises, les expressions « plans d'intervention » et « plans d'intervention d'urgence » soient indistinctement employées par les responsables de certains pays. Or, au sens strict, les plans d'intervention d'urgence sont, par nature, adoptés en réaction à une situation, alors que les plans d'intervention consistent à anticiper la survenue d'un problème. Si les plans d'intervention d'urgence sont conçus pour limiter les conséquences ou l'incidence d'un événement, les plans d'intervention le sont pour prévenir tous problèmes et préparer l'ensemble des parties concernées à faire face à une urgence ainsi qu'à permettre le retour à un service normal le plus rapidement possible.

C'est à une seule entité, désignée par l'État, qu'il conviendrait de confier la responsabilité principale et l'autorité de décider des moyens d'action à mettre en œuvre en cas de crise. Celle-ci devrait coordonner l'ensemble des actions avec toutes les entités concernées et touchées. Dans le cadre du plan de gestion des crises, il conviendrait d'élaborer un plan d'intervention d'urgence efficace, notamment pour garantir l'interopérabilité des systèmes de communication et l'adéquation des temps de réaction, ainsi que des plans d'évacuation pour limiter les effets de la crise. L'action de l'équipe d'intervention d'urgence devrait être planifiée, testée et évaluée à l'avance, de manière à atténuer les effets d'une attaque.

2.7 Cartographier les menaces, les conséquences et les vulnérabilités

En axant leurs stratégies de protection des infrastructures critiques sur une approche de gestion des risques, les pays devraient tenir compte d'un certain nombre de principes directeurs. Ces principes sont développés ci-dessous.

2.7.1 Un exercice à plusieurs niveaux

La détermination de la nature et des niveaux des menaces pesant sur les infrastructures critiques ainsi que des vulnérabilités connexes ne peut être que le résultat harmonisé et commun d'évaluations effectuées à différents échelons. Tel le zoom d'un objectif qui permet de prendre une image d'ensemble et ensuite de grossir le champ pour en saisir les moindres détails, une stratégie pour la protection des infrastructures critiques devrait être en mesure d'intégrer des évaluations de menaces, conséquences et vulnérabilité réalisées à différents échelons. Schématiquement, ces échelons sont les suivants : i) le niveau national ; ii) le niveau sectoriel ; iii) le niveau des infrastructures ou des entreprises.

i) Évaluations au niveau national

L'évaluation des risques au niveau national a pour objectif d'obtenir une vue d'ensemble de la menace à laquelle les infrastructures critiques d'un pays font face collectivement, de leurs vulnérabilités et des conséquences encourues en cas d'attaque réussie. Les évaluations nationales contribuent de manière significative à mettre en lumière la manière dont les différents secteurs

interagissent entre eux. Les informations communiquées par les services de renseignement sur lesquelles se fondent les stratégies nationales de sécurité et de lutte contre le terrorisme peuvent fournir des orientations et des indications utiles à l'élaboration de ce type de documents.

ÉTUDE DE CAS 17
Évaluation nationale des risques de la Suède

Conformément au droit interne, toutes les entités gouvernementales sont tenues d'établir une analyse des risques et de la vulnérabilité et de la soumettre à l'Agence suédoise pour la protection civile (MSB). Sur la base de ces rapports, la MSB produit des évaluations nationales des risques depuis 2011. Celles-ci (dont la plus récente a été publiée en 2016) visent à jeter les bases stratégiques, qui serviront à orienter et à élaborer les politiques en matière de protection civile.

Dans l'estimation de 2016, la MSB recense cinq domaines dans lesquels elle estime qu'il importe tout particulièrement d'intervenir afin de renforcer la préparation en prévision des catastrophes (domaines qui concernent donc directement la protection des infrastructures critiques) :

- Les parties prenantes responsables en Suède doivent accorder un plus haut degré de priorité à l'action menée dans les domaines de la préparation aux catastrophes et de la protection civile ;

- Il convient de mettre l'accent sur les connaissances et la sensibilisation des parties concernées quant aux rôles et aux responsabilités en matière de préparation aux catastrophes, en particulier quand il s'agit des responsabilités liées à des zones géographiques ;
- Les analyses des risques et de la vulnérabilité effectuées à l'échelon local, régional et national doivent être affinées, de manière à servir de base de planification à la préparation aux catastrophes et à la protection civile ;
- La planification et l'élaboration des politiques de préparation aux catastrophes pourraient s'appuyer sur les scénarios fournis par la MSB ;
- En ce qui concerne les infrastructures critiques, il convient d'établir des demandes de mesures de protection plus explicites.

La MSB souligne qu'il est nécessaire de renforcer encore les capacités dans les domaines suivants :

- La capacité de réagir aux interruptions de l'approvisionnement en électricité ;
- La capacité de prévenir les interruptions de l'approvisionnement en eau potable et d'y remédier ;
- Les domaines de l'information et de la cybersécurité ;
- La capacité de prévenir les interruptions de l'approvisionnement en médicaments et d'y remédier ;
- La capacité de prévenir la survenue d'événements radiologiques et nucléaires et d'y remédier.

Source : Suède (2016).

ii) Évaluations au niveau sectoriel

Il est important d'élaborer des profils de risque pour certains secteurs d'infrastructures critiques. Ce qui est essentiel, c'est que ces profils comprennent une évaluation des mesures d'atténuation, des conséquences et des vulnérabilités existantes. Selon le secteur considéré, les estimations des risques

peuvent être entreprises pour des sous-secteurs particuliers et, par la suite, intégrées aux profils de risques du secteur plus généraux. Par exemple, la Stratégie relative à la résilience de l'infrastructure critique de l'Australie divise le secteur des transports en sous-secteurs : aviation, transport collectif terrestre de passagers (y compris ponts et tunnels), fret terrestre et maritime (navigation et ports). Dans le cadre de la même stratégie, le secteur de l'énergie se compose des systèmes électriques, de l'exploitation pétrolière et gazière au large des côtes, de l'exploitation pétrolière et gazière terrestre et de l'approvisionnement en charbon.

iii) Évaluations au niveau des infrastructures

Les exploitants d'infrastructures critiques sont souvent ceux qui maîtrisent le mieux le fonctionnement de leurs infrastructures en termes de systèmes et de processus. Par conséquent, ils connaissent particulièrement bien leurs vulnérabilités intrinsèques. En outre, il est fréquent que ces entreprises procèdent à des exercices de gestion des risques, indépendamment du rôle institutionnel qu'elles sont appelées à jouer dans la protection des infrastructures critiques. Les sociétés de capitaux se livrent à des exercices de gestion des risques pour minimiser les dommages préjudiciables à la réalisation des objectifs de l'entreprise, afin de garantir la continuité des opérations ou de limiter les conséquences d'une menace. Bien que ce type de gestion des risques ne soit pas axé sur la protection des infrastructures critiques, il vise à recenser les risques posés à la continuité de la production et à mettre en place des mesures d'atténuation. En conséquence, il peut servir directement les intérêts des infrastructures des entreprises et en accroître la résilience. Les pays devraient donc examiner avec soin le rôle que les exercices de gestion des risques menés par les entreprises devraient jouer dans le cadre des stratégies de protection des infrastructures critiques, y compris quant à la manière d'intégrer les évaluations réalisées au niveau des entreprises dans les processus de prise de décisions relatifs à la protection des infrastructures critiques.

2.7.2 Un processus multipartite

Pour assurer la réussite d'un exercice d'évaluation des risques, il faut qu'il soit le résultat d'un processus de consultations s'appuyant sur les perspectives et les conclusions d'une diversité d'organismes gouvernementaux, de services d'urgence et d'entités du secteur privé. Même si, d'ordinaire, les organismes gouvernementaux pilotent l'élaboration des évaluations des menaces aux niveaux national et sectoriel, et les exploitants d'infrastructures critiques celle des plans relatifs aux infrastructures critiques, il est souhaitable que toutes les parties prenantes contribuent et participent à ces processus. Si la participation d'un large éventail de parties prenantes peut ralentir le processus dans son ensemble, l'expérience des pays montre cependant que le souci de n'exclure personne et la transparence liée au processus décisionnel sont des valeurs contribuant à l'établissement d'un consensus. Il s'agit là d'une condition préalable essentielle, étant donné que la mise en œuvre des stratégies de protection des infrastructures critiques relève de la responsabilité de multiples acteurs.

La participation de tous au processus permet également d'examiner les risques sous plusieurs angles. L'interaction entre des infrastructures et des secteurs différents est ainsi mieux comprise par tous. Toutefois, il est difficile de concilier, d'une part, la participation de tous au processus et, d'autre part, la cohérence d'ensemble de ce dernier. En effet, d'une manière générale, différentes parties prenantes perçoivent les risques de différentes manières. Comme il a été noté, « les partenaires d'infrastructures critiques gèrent les risques en fonction de divers engagements pris envers la collectivité, tantôt

privilégiant la satisfaction de la clientèle, tantôt les structures de gouvernance d'entreprise. La tolérance au risque variera d'une organisation à l'autre, ainsi que d'un secteur à l'autre, en fonction des plans de développement, des ressources, de la structure opérationnelle et du cadre réglementaire. De plus, elle ne sera pas la même pour le secteur privé et les organismes gouvernementaux du fait de contraintes sous-jacentes. Il est fort probable que des entités différentes ne partageront pas les mêmes priorités en matière d'investissement dans la sécurité ni, sans doute, le même point de vue quant au meilleur des seuils de tolérance au risque possibles » (NIPP 2013, p. 15).

Il importe non seulement de reconnaître que les parties prenantes n'ont pas toutes le même avis ou la même approche, mais aussi de comprendre comment leurs différences peuvent influer sur tout le processus d'établissement des priorités communes. De ce point de vue, la réalisation de « l'objectif de sécurité et de résilience des infrastructures critiques dépendra de la mise en œuvre des pratiques de gestion des risques du secteur industriel et du gouvernement, outre les ressources et les mesures incitatives disponibles, visant à guider et à appuyer les efforts consentis » (NIPP 2013, p. 15).

2.7.3 Cartographier les menaces terroristes contre les infrastructures critiques

Par rapport aux évaluations des menaces liées à d'autres dangers, la détermination et l'évaluation des menaces terroristes pesant sur les infrastructures critiques soulèvent des problèmes particuliers. Certains découlent du plus grand degré d'incertitude qui entoure ce type d'exercice d'évaluation. Comme il a été noté, « le fait que les terroristes adaptent leur comportement aux changements dans le paysage sécuritaire constitue un problème fondamental dans ce contexte » (CTED 2017). De ce point de vue, la menace terroriste devrait être considérée comme une menace évolutive, qui s'adapte, par exemple, à la variation des ressources à disposition d'un groupe terroriste et à celle des dispositifs de sécurité d'une cible potentielle.

En ce qui concerne les sources à partir desquelles tirer des éléments pour évaluer les menaces liées au terrorisme, les stratégies de protection des infrastructures critiques devraient prendre en compte le rôle traditionnellement dominant de la communauté du renseignement. Les services de renseignement sont chargés de protéger la sécurité nationale. Dans l'exécution de leurs missions, ils ont souvent accès à des informations confidentielles en tant que moyen de protéger leurs sources et leurs méthodes, afin, entre autres, de ne pas alerter les cibles des activités de surveillance en cours. Par conséquent, il faut que les stratégies de protection des infrastructures critiques disposent de mécanismes capables de traiter des renseignements dont la distribution est restreinte. Comme l'indique la section 4.2, l'un des principaux défis à relever consiste à faire en sorte que le plus de renseignements possible circulent entre toutes les parties prenantes sans porter atteinte à leur caractère confidentiel. Il peut s'agir d'informations commerciales sensibles détenues par des entreprises ou d'informations classifiées en possession d'organismes publics.

ÉTUDE DE CAS 18
Protection des infrastructures critiques contre les attaques terroristes en Australie : une approche axée sur le renseignement

L'Australie s'appuie sur un solide système de prévention et de préparation, axé sur le renseignement, qui renforce son dispositif de lutte antiterroriste. Cette approche englobe des mesures ciblées de prévention et de préparation qui reposent sur les principes de gestion des risques et le maintien des capacités permettant de faire face à divers types de menaces ou d'attaques terroristes ainsi qu'à leurs conséquences. Ce sont l'Australian Security Intelligence Organisation (ASIO) et les services de détection et de répression qui sont chargés du renseignement antiterroriste et des enquêtes criminelles. La communication rapide et appropriée d'informations sur des menaces terroristes pesant sur telles ou telles infrastructures critiques permet à leurs propriétaires et exploitants de faire face à ce contexte de menaces en prenant des décisions mieux éclairées en matière de gestion des risques ainsi que des mesures efficaces d'atténuation des risques.

En particulier, les évaluations de l'ASIO indiquent le niveau et la nature probable des menaces ambiantes, qu'il s'agisse de terrorisme, de violence à caractère politique, d'espionnage, d'ingérence étrangère, de manifestations violentes et de sabotage. Il est possible de conduire des évaluations des menaces à propos d'événements, d'installations, de personnes ou de secteurs particuliers et ces évaluations sont distinctes du niveau d'alerte officiel face à une menace terroriste sur le territoire national. L'ASIO communique ses évaluations des menaces aux organismes gouvernementaux australiens concernés, aux gouvernements des États et Territoires, aux services de la Police fédérale australienne et aux autorités de police des États et Territoires. Les propriétaires et exploitants d'infrastructures critiques reçoivent également une copie des évaluations des menaces terroristes sur le territoire national et doivent les mettre à profit dans le cadre de leurs processus de préparation et de planification. L'ASIO fournit des conseils en cas de menaces pesant sur le secteur privé et les organismes gouvernementaux par l'intermédiaire du Business Liaison Unit. En cas d'urgence particulière, l'ASIO contactera les services de police des États et Territoires et les autres structures concernées, y compris les propriétaires et exploitants d'infrastructures critiques, et ce dès que possible et préalablement à l'envoi d'un avis écrit. Si les évaluations de l'ASIO tiennent compte des intentions et des capacités des terroristes, elles n'évaluent pas la vulnérabilité des infrastructures critiques ou l'adéquation des mesures de sécurité qu'elles ont mises en place. Par la suite, les évaluations des menaces devraient être utilisées dans l'analyse des risques en matière de sécurité afin de décider de la nécessité et du type de mesures d'atténuation pour chacune des installations d'infrastructures critiques.

Source : Australie-Nouvelle-Zélande (2015).

Les stratégies de protection des infrastructures critiques devraient également tenir compte du fait qu'il faut disposer des capacités de traiter de multiples ensembles d'indicateurs ainsi que de replacer l'information disponible dans son contexte pour effectuer des évaluations des menaces terroristes pesant sur des infrastructures critiques. Les changements intervenus sur le plan, entre autres, des réalités géopolitiques, des situations économiques et de la dynamique du pouvoir entre organisations criminelles devraient être tous pris en considération et inciter à répéter l'exercice à intervalles réguliers.

Les preuves d'attaques ou de menaces antérieures contre des infrastructures critiques sont un indicateur utile, en particulier lorsque ces attaques et menaces se reproduisent au fil du temps ou visent constamment certains secteurs ou infrastructures critiques dans des régions particulières. Les évaluations pourraient aussi tirer profit des données disponibles provenant d'autres pays, notamment en cas d'analogies. À titre d'exemple, si un groupe terroriste a déjà attaqué des installations nucléaires dans un pays X et que le

pays Y est allié à ce pays X, il serait possible d'en déduire un niveau de menace supérieur pour les installations nucléaires du pays Y.

ÉTUDE DE CAS 19
Analyse allemande des menaces contre la cybersécurité

Dans le cadre de ses analyses de cybersécurité, l'Office fédéral allemand de la sécurité informatique a dressé une liste des menaces les plus graves pesant sur les systèmes de contrôle industriel. Ces menaces sont classées en fonction de facteurs tels que les groupes de terroristes, la répartition et la facilité d'exploitation des vulnérabilités ainsi que les conséquences techniques et économiques possibles d'une attaque. Ces informations sont tirées de l'analyse des bases de données relatives à des événements réels.

Source : OSCE 2013, p. 35.

Les radars devraient aussi pouvoir détecter les signes de « faible intensité » d'éventuels plans terroristes en cours. L'enregistrement d'actes constituant des violations du respect des infrastructures critiques, telles que la simple violation de la propriété privée, pourrait témoigner de l'intérêt porté par des terroristes à la construction d'une infrastructure critique ou des efforts déployés pour surveiller de près certains lieux. Cependant, il est souvent impossible de tirer une conclusion sur la base d'actes isolés et sporadiques. Là encore, les services de renseignement ont un rôle clef à jouer dans la mise au jour de ce qui se trame en réalité derrière certains événements apparemment anodins lorsqu'ils sont considérés isolément.

Si les stratégies de protection des infrastructures critiques ne sont pas censées contenir des listes complètes d'indicateurs et de sources, elles devraient néanmoins être conçues de manière à donner aux autorités compétentes les moyens (ou à leur donner mandat, selon les modèles de gouvernance choisis pour la protection des infrastructures critiques) d'adapter les processus d'évaluation des risques au caractère particulièrement fluide et volatile de la menace terroriste.

2.8 Réduire au minimum la vulnérabilité des infrastructures critiques aux attaques terroristes

Dans les sections précédentes, il a été souligné que, pour réduire au minimum la vulnérabilité des infrastructures aux attaques terroristes, il était indispensable de mettre en place un processus complet de gestion des risques et de mener des évaluations des risques à différents niveaux. La gestion des risques devrait à terme se traduire par des plans et mesures préventifs concrets. La présente section porte sur la place des mesures de prévention dans le cadre des stratégies de protection des infrastructures critiques du point de vue de la protection physique, personnelle et informatique.

Lorsque les pays examinent ces mesures, ils sont toujours encouragés à étudier l'ampleur de leurs effets potentiels sur l'exercice des droits de l'homme (notamment les incidences des restrictions d'accès à certains sites pour des raisons sécuritaires sur la liberté de circulation, les ingérences dans la vie privée dues aux technologies de vidéosurveillance, etc.). Dans tous les cas, il faut trouver un équilibre entre l'objectif de protection des infrastructures critiques contre les attaques terroristes et la nécessité de respecter les droits fondamentaux consacrés par les traités

internationaux tels que le Pacte international relatif aux droits civils et politiques, et ne retenir que les mesures jugées nécessaires pour la protection des infrastructures critiques. Ces mesures doivent également être proportionnelles aux objectifs visés.

2.8.1 Prévention

La prévention des attaques terroristes contre les infrastructures critiques fait partie de la tâche qui revient aux États et consiste à anticiper et à déjouer les plans, les complots et toute autre préparation d'actes terroristes de manière générale. La protection des infrastructures critiques dépend, en définitive, des activités coordonnées des services de renseignement ou encore des forces de l'ordre en général. L'approche préventive des lois pénales ainsi que l'attitude des organismes d'enquête (qui doivent agir au lieu de réagir face aux actes terroristes) jouent un rôle fondamental dans les efforts de prévention. Les stratégies de protection des infrastructures critiques devraient s'appuyer sur les cadres existants en privilégiant les politiques et mesures qui permettent directement de renforcer la prévention des attaques terroristes visant spécialement les infrastructures critiques. Ces stratégies peuvent notamment permettre :

- de déterminer les principaux rôles et les responsabilités dans le domaine de la prévention, y compris au niveau des exploitants d'infrastructures critiques (soit les rôles et les responsabilités des cadres supérieurs et des agents responsables de la sécurité) et, plus généralement, d'établir que la mise en œuvre de mesures préventives incombe à l'ensemble de l'entreprise et nécessite un appui à tous les niveaux ;
- de définir les conditions et méthodes de travail en vue de l'élaboration de manuels et de lignes directrices à l'usage des exploitants d'infrastructures critiques dans le domaine de la prévention ;
- de recenser directement les méthodes et approches qui devraient être largement appliquées ou envisagées par les parties prenantes. Par exemple, certains pays promeuvent de plus en plus la prise en compte de la sécurité dès la conception afin d'atteindre les objectifs de prévention. Autre exemple, les propriétaires ou exploitants d'infrastructures critiques sont tenus de prendre des mesures de sécurité efficaces pour maximiser la probabilité d'identifier rapidement les activités de préparation d'actes terroristes, telles que les activités de reconnaissance de sites. Ainsi, dans le cadre de sa stratégie de protection des infrastructures critiques, le Gouvernement australien impose de signaler à la police toute activité suspecte de ce genre et a spécialement mis en place une permanence téléphonique nationale de sécurité ;
- d'encourager ou de prescrire (selon le modèle de gouvernance choisi) l'adoption de mesures préventives concrètes, sectorielles ou intersectorielles, par les exploitants d'infrastructures critiques.

ÉTUDE DE CAS 20
Prise en compte de la sécurité dès la conception

De plus en plus de pays prennent en compte la sécurité dès la conception des infrastructures, dans le cadre de leurs stratégies visant à améliorer la résilience des infrastructures critiques aux attaques terroristes et autres risques. Cette méthode vise à assurer une prévention durable à long terme. Selon le Centre britannique chargé de la protection des infrastructures nationales, la prise en compte de la

sécurité physique dès la conception du bâtiment ou des installations permet souvent d'améliorer la sécurité à moindre coût. Il faudrait ajouter des normes de sécurité élevées dans les directives initiales des nouvelles constructions. Il importe également de prendre en compte les normes de sécurité physique lors de la construction de nouveaux bâtiments ou de la modification d'installations existantes, dans la mesure où ces bâtiments sont exposés à différents risques et problèmes. Il faut envisager :

- de recenser et d'évaluer les risques existants et nouveaux pesant sur la sécurité ;
- de recenser les normes de sécurité pour les travaux de construction et de modification de la sécurité des installations (selon que les travaux ont lieu à proximité ou à l'intérieur des installations) ;
- de déterminer le passage des mesures de sécurité du stade de la « phase de construction » à celui des opérations normales.

La prise en compte de la sécurité dès la conception est une approche qui peut s'appliquer non seulement aux biens matériels, mais aussi aux infrastructures d'information critiques. Dans le cadre de sa stratégie de cybersécurité pour 2016, Singapour s'est fixé l'objectif de prévenir les vulnérabilités cybernétiques en travaillant en amont et en favorisant les pratiques axées sur la sécurité dès la conception. La cybersécurité ne sera plus prise en considération a posteriori mais tout au long du cycle de vie des systèmes technologiques. Le Gouvernement s'est ainsi engagé à prendre les mesures suivantes :

- Institutionnaliser progressivement l'approche de la sécurité dès la phase de la conception dans le cadre du dispositif de gouvernance de protection des infrastructures d'information critiques ;
- Promouvoir la pratique des tests d'intrusion informatique pour déceler les problèmes au plus tôt et y remédier dès la phase de conception ;
- Créer un vaste réseau de praticiens dans le domaine des essais de produits et de systèmes conformes aux normes internationales établies, tels que la certification Critères communs ;
- Continuer de perfectionner les méthodes et d'élaborer de nouveaux outils de validation de sécurité afin d'améliorer l'efficacité de la prise en compte de la sécurité dès la conception.

2.8.2 Processus, sécurité physique (y compris technologique), sécurité du personnel et mesures de cyberprotection

Les stratégies de protection des infrastructures critiques et les mesures de mise en œuvre connexes devraient être fondées sur l'idée que, pour être efficaces, les mesures de protection doivent prendre en compte la dimension physique du problème ainsi que les aspects liés au personnel et à la cybersécurité. Le tableau [numéro] présente une sélection d'outils pratiques élaborés par un certain nombre d'États afin d'orienter les exploitants d'infrastructures critiques. Bien que ces outils aient une portée nationale, la plupart des orientations y figurant sont applicables au-delà des frontières et peuvent être une source d'inspiration pour les autorités et les exploitants d'infrastructures critiques d'autres pays.

i) Processus

Les stratégies de protection des infrastructures critiques devraient tenir compte des obligations réglementaires pour les mesures de sécurité préventives relatives aux infrastructures critiques et devraient avant tout fixer des objectifs de réalisation plutôt que d'établir des mesures ou des procédures particulières. Il conviendrait de mettre en place une organisation complète et une

structure juridique, assorties de responsabilités et de méthodes de mise en œuvre clairement définies. Les stratégies devraient faire siens les principes sous-jacents des règlements, des pratiques et des procédures s'appliquant aux conditions d'exploitation « normales » ainsi que les mesures supplémentaires nécessaires en cas d'augmentation du niveau de menace.

ii) Mesures de sécurité physique (y compris technologique)

La sécurité physique est réellement assurée grâce à l'application du concept dit de « défense en profondeur », selon lequel la protection nécessite la mise en œuvre de différentes mesures à plusieurs niveaux. Le principe sous-jacent à cette approche est que la sécurité des infrastructures n'est guère compromise en cas d'échec d'une mesure.

Afin de détecter tout accès non autorisé et de permettre d'appréhender les intrus avant qu'ils n'atteignent les installations essentielles, toute approche à plusieurs niveaux pourra comporter les éléments suivants :

- la délimitation du périmètre de la zone des infrastructures critiques et sa protection par des barrières physiques ;
- la mise en place de patrouilles et d'une surveillance suffisante ;
- le contrôle des accès grâce à des dispositifs de sécurité supplémentaires permettant de meilleurs résultats et une plus grande efficacité (tels que des barbelés sur les murs, un système de détection des intrusions dans le périmètre, un système d'éclairage ou un dispositif de vidéosurveillance) ;
- le recours à des technologies telles que les méthodes et techniques de contrôle (chiens détecteurs d'explosifs, fouilles manuelles, détecteurs de métaux portatifs, détecteurs de traces d'explosifs et unités mobiles de contrôle, etc.).

Les mesures de sécurité physique devraient s'accompagner du recrutement de personnel dûment formé, d'une planification des interventions d'urgence rigoureuse et complète et de consignes et de plans de sécurité concis et bien rédigés.

ÉTUDE DE CAS 21
Centre pour la protection des infrastructures nationales du Royaume-Uni

Le Centre dresse la liste des éléments suivants à titre d'exemples de mesures de sécurité physique :

- Mesures visant à faciliter la détection des armes faisant peser une menace, comme par exemple les explosifs, les couteaux, les armes à feu ou les matières chimiques, biologiques et radiologiques ;
- Mesures visant à faciliter la détection, le suivi et le contrôle des intrus et d'autres menaces, telles que les véhicules aériens téléguidés ;
- Systèmes de contrôle des accès et de verrouillage ;
- Barrières physiques et actives qui empêchent ou retardent la progression d'adversaires ;
- Mesures visant à protéger les personnes ou les biens contre les effets d'une explosion ou d'une attaque balistique ;
- Mesures visant à protéger contre la propagation de matières chimiques, biologiques ou radiologiques ou à limiter cette propagation ;

- Mesures visant à protéger le matériel ou les biens sensibles (par exemple, le matériel ou les biens classifiés).

Source : Centre pour la protection des infrastructures nationales du Royaume-Uni, à l'adresse suivante : www.cpni.gov.uk

iii) Sécurité du personnel

Il s'agit des politiques et procédures nécessaires pour réduire les risques associés aux menaces internes venant, par exemple, des employés d'une entreprise qui profiteraient de leur accès légitime aux locaux, aux systèmes ou aux dispositifs d'une infrastructure à des fins illicites ou malveillantes. Pour assurer efficacement la sécurité du personnel, il faut prendre un certain nombre de mesures allant de la vérification des antécédents aux procédures de sélection, en passant par des formations en matière de sécurité incitant à la vigilance et encourageant une culture sécuritaire en général, la formation du personnel, les systèmes de sécurité du périmètre et de contrôle des accès au périmètre, la surveillance et le contrôle de la qualité.

Tableau 5 : Outils pratiques destinés aux exploitants d'infrastructures critiques

Titre/Thème et pays	Description
Protection d'infrastructures critiques – Concept de base de protection, Recommandations destinées aux entreprises Allemagne, Ministère fédéral de l'intérieur	Cet outil a été élaboré par le Ministère fédéral de l'intérieur, l'Office fédéral pour la protection des populations et la gestion des catastrophes et l'Office fédéral de police criminelle, avec la contribution des milieux d'affaires dès les premières étapes. Il fournit aux entreprises allemandes des recommandations relatives à la sécurité interne et présente un catalogue de questions et une liste de contrôle. https://www.preventionweb.net/files/9266_2967ProtectionofCriticalInfrastruct.pdf
Sécurité du personnel et des personnes Sécurité physique Royaume-Uni, Centre pour la protection des infrastructures nationales (CPNI)	Dans le cadre de ses orientations, de ses trousses d'information et de ses guides, le CPNI aborde les thèmes et les sous-thèmes suivants : **Sécurité du personnel et des personnes** (réduire les risques internes ; optimiser la sécurité des personnes ; reconnaissance des éléments perturbateurs hostiles) **Sécurité physique** (recherche, contrôle et atténuation de menaces spécifiques ; défenses physiques ; contrôle des accès et verrouillage ; détection et surveillance des intrus ; délai d'activation de l'accès ; structures des bâtiments ; fenêtres et façades ; portes ; services et espaces ; salles de contrôle ; informations et biens sensibles) https://www.cpni.gov.uk/advice
Cyberstratégie	Les orientations disponibles sont organisées par thèmes en fonction des catégories et sous-catégories suivantes :

Infrastructures informatiques **Dispositif de l'utilisateur final** **Technologies opérationnelles** Royaume-Uni, Centre national de cybersécurité www.ncsc.gov.uk/guidance	**Cyberstratégie** (Travail flexible – Gestion des incidents – Sécurité des opérations – Sécurité du personnel – Sécurité physique – Gestion des risques – Compétences et formation – Sécurité sociotechnique) **Infrastructures informatiques** (Cryptographie – Données en transit – Conception et configuration – Destruction et élimination – Protection contre les logiciels malveillants – Surveillance – Sécurité du réseau – Stockage sécurisé – Technologies de l'utilisateur final – AVEC) **Dispositif de l'utilisateur final** (Identité et mots de passe – Communications sécurisées – Services numériques – Services aux citoyens – Sécurité informatique en nuage – Offres SaaS – Contrôle des transactions) **Technologies opérationnelles** (Cybermenaces – Cyberattaques – Vulnérabilités)
Trousse d'informations sur la protection et la résilience des infrastructures critiques États-Unis, Département de la sécurité du territoire	Cette trousse d'informations se veut un point de départ pour les petites et moyennes entreprises leur permettant de prendre en compte la protection et la résilience des infrastructures dans la préparation, la gestion des risques, la poursuite des activités, la gestion des urgences, la sécurité et autres disciplines connexes. Pour plus d'informations : IP_Education@hq.dhs.gov.

iv) Cybersécurité

Les mesures de cybersécurité représentent le troisième groupe de mesures pour l'élaboration desquelles les stratégies de protection des infrastructures critiques doivent établir un cadre adapté. Il s'agit d'un ensemble de mesures destinées à protéger les infrastructures critiques contre les cyberattaques. Outre que ces mesures sont technologiques par nature, elles contribuent à préserver l'intégrité, la résilience et le fonctionnement normal des infrastructures critiques. Il peut s'agir, par exemple, de procédures, de politiques ou de mesures organisationnelles de sécurité, d'activités de sensibilisation et de formation à la sécurité, de directives et de processus de développement particuliers ou d'évaluations régulières de la sécurité.

ÉTUDE DE CAS 22
Guide suédois sur le renforcement de la sécurité des systèmes d'information et de contrôle industriels

L'Agence suédoise pour la protection civile a formulé 17 recommandations sur la base d'orientations, de pratiques et de méthodes de travail internationalement reconnues. Certaines recommandations sont de nature technique et d'autres sont axées sur les méthodes.

1 Garantir l'engagement et la responsabilité de la direction en matière de sécurité des systèmes d'information et de contrôle industriels.
2 Apporter des précisions sur les rôles et les responsabilités en matière de sécurité dans les systèmes d'information et de contrôle industriels.

3 Maintenir les procédures d'examen et de gestion des risques des systèmes d'information et de contrôle industriels.
4 Assurer la gestion systématique du changement pour les systèmes d'information et de contrôle industriels.
5 Garantir le caractère systématique de la planification des interventions d'urgence et de la gestion des incidents pour les systèmes d'information et de contrôle industriels.
6 Fixer d'emblée des normes de sécurité pour toutes les étapes de la planification et de l'approvisionnement des systèmes d'information et de contrôle industriels.
7 Créer une réelle culture sécuritaire et sensibiliser davantage à l'importance d'assurer la sécurité des systèmes d'information et de contrôle industriels.
8 Travailler avec une architecture de sécurité dans le cadre des systèmes d'information et de contrôle industriels.
9 Surveiller en permanence les connexions et les systèmes afin de détecter les tentatives d'intrusion dans les systèmes d'information et de contrôle industriels.
10 Analyser régulièrement les risques liés aux systèmes d'information et de contrôle industriels.
11 Procéder régulièrement à des audits techniques de sécurité des systèmes d'information et de contrôle industriels.
12 Évaluer de manière continue la sécurité physique des systèmes d'information et de contrôle industriels.
13 Vérifier régulièrement que toutes les connexions aux systèmes d'information et de contrôle industriels sont sûres et adaptées.
14 Renforcer et mettre à niveau les systèmes d'information et de contrôle industriels en collaboration avec les fournisseurs des systèmes.
15 Dispenser des formations au sujet des incidents informatiques relatifs aux systèmes d'information et de contrôle industriels et mettre en pratique les enseignements de ces formations.
16 Assurer le suivi des incidents relatifs aux systèmes d'information et de contrôle industriels et suivre les problèmes de sécurité externes.
17 Prendre part à des associations d'usagers, à des organismes de normalisation et à d'autres réseaux dans le domaine de la sécurité des systèmes d'information et de contrôle industriels.

Le texte intégral du Guide (https://www.msb.se/RibData/Filer/pdf/27473.pdf) fournit des précisions sur chaque recommandation, présente le texte des sous-recommandations et donne des exemples de risques et de problèmes susceptibles de survenir.

Source : Suède (2014)

2.9 Intervenir en cas d'attaque terroriste contre les infrastructures critiques et se relever par la suite

La section 2.6 a introduit la notion de « gestion des crises » au sujet des infrastructures critiques. Dans le cadre de la lutte contre le terrorisme, le terme « intervention » désigne les mesures prises pendant et immédiatement après la perpétration d'un acte terroriste ou face à une menace terroriste. Les mesures d'intervention visent généralement à prévenir ou à réduire au minimum les conséquences de l'attaque, telles que les pertes en vies humaines, les blessures, les dommages matériels et les dégâts ou perturbations causés aux infrastructures, à mener des enquêtes criminelles et à apporter une aide et un soutien immédiats aux populations touchées.

Quant au « relèvement », il s'agit généralement de mesures nécessaires à plus long terme pour appuyer les efforts de reconstruction, notamment des infrastructures physiques, et le

rétablissement du statu quo en termes de bien-être physique, social et économique des populations. Les répercussions psychologiques des actes terroristes, qui ne s'arrêtent pas au lieu précis de l'incident, donnent à penser que le relèvement doit parfois supposer une collaboration intégrée et soutenue entre les organismes publics, le secteur privé et les organisations de la société civile.

Il faut réfléchir à la façon dont on peut prendre en compte les structures de gestion des crises existantes dans les stratégies de protection des infrastructures critiques et aux changements qui devraient être apportés aux systèmes généraux en place, le cas échéant, pour mieux faire face aux crises touchant les infrastructures critiques en particulier. Il importe d'établir des cadres juridiques et opérationnels clairs et compatibles avec les droits de l'homme, en gardant à l'esprit que la gestion des crises est importante non seulement en cas d'attentat terroriste particulièrement grave mais aussi en cas d'incident mineur, pour éviter ou limiter les effets d'une aggravation de la crise.

La définition d'un cadre approprié de gestion des crises implique de se poser deux questions fondamentales. La première est de savoir si, dans le contexte de la gestion des urgences, il convient d'adopter une approche générale ou spécifique à chaque type de risque. La Nouvelle-Zélande a, par exemple, choisi d'adopter la seconde approche (voir l'étude de cas ci-dessous). Les deux approches présentent des avantages et des inconvénients. Lorsque les structures de gestion des crises sont destinées à des types de risques particuliers, il est possible d'établir des processus adaptés. Toutefois, le choix de cette approche peut s'avérer problématique lorsque la nature de l'incident n'est pas claire, dans la mesure où il peut être difficile de savoir quel cadre d'intervention s'applique.

La deuxième question à se poser est de savoir si la portée des structures et des procédures de gestion des crises des infrastructures critiques doit être sectorielle ou intersectorielle. Si l'on choisit une approche sectorielle, la législation est souvent adoptée par le ministère responsable du secteur en question ou par l'autorité chargée de sa réglementation, tandis que dans le cas d'une approche intersectorielle, on adopte plutôt des lois générales.

Les cadres normatifs propres au secteur des infrastructures critiques se retrouvent souvent dans le secteur des télécommunications. Aux Pays-Bas, par exemple, le National Continuity Forum Telecommunications (NCO-T) a pour objectif de veiller à ce que les exploitants soient en mesure d'assurer le fonctionnement des services de télécommunications essentiels dans des circonstances exceptionnelles. Les participants à ce dispositif sont les exploitants désignés et la direction générale de l'énergie, des télécommunications et des marchés du Ministère des affaires économiques. En France, le plan PIRANET est déclenché par le Premier ministre en cas de crise majeure d'origine informatique.

D'autres secteurs des infrastructures critiques peuvent établir des dispositions équivalentes sur la base de cadres juridiques adoptés par les autorités responsables de ces secteurs. Après les attentats du 11 septembre 2001, par exemple, la Bourse de New York, qui est constamment la cible potentielle d'attaques terroristes, a pu poursuivre ses opérations dans la mesure où elle avait déjà prévu un parquet de remplacement à l'extérieur de New York, tout comme l'on fait depuis d'autres

organismes de financement afin de pouvoir répliquer leurs opérations commerciales hors de leur zone municipale en cas de catastrophe à caractère terroriste (Sinai, 2016).

La loi estonienne sur les crises, dont le chapitre IV traite de l'organisation de la continuité des services essentiels, est un exemple de cadre normatif intersectoriel. Elle définit les rôles et les responsabilités des ministères, des organismes locaux et nationaux de gestion des crises et des exploitants d'infrastructures critiques pour qu'ils puissent assurer la continuité des 41 services essentiels.

ÉTUDE DE CAS 23
Structure de gouvernance de la gestion des crises en Nouvelle-Zélande

En Nouvelle-Zélande, le manuel national sur le système de sécurité (National Security System Handbook) établit une structure de gouvernance globale pour la gestion des crises potentielles, émergentes ou réelles (notamment les crises relatives aux infrastructures critiques). Les critères de déclenchement du système de sécurité nationale se divisent en deux grandes catégories, portant soit sur les caractéristiques des risques, soit sur la manière dont ils doivent être gérés.

Caractéristiques de risques
• Échelle, nature, intensité ou conséquences potentielles inhabituelles ;
• Risques pour la souveraineté ou l'ordre public national ;
• Problèmes multiples ou interdépendants qui, pris ensemble, constituent un risque national ou systémique ;
• Degré d'incertitude ou de complexité tel que seule l'administration centrale est en mesure d'y faire face ;
• Questions interdépendantes susceptibles d'entraîner des effets en cascade ou l'intensification d'un conflit.

Besoins en matière de gestion
• Les interventions demandent un niveau inhabituel de ressources ;
• On ne sait pas toujours bien qui est responsable de la gestion des risques, ou tout le monde ne s'accorde pas sur les solutions à apporter ;
• La première réaction ne convient pas ou ne suffit pas à l'échelle nationale ;
• Il y a des répercussions interinstitutionnelles ;
• Les autorités publiques peuvent aider à créer des conditions qui amélioreront la sécurité nationale dans son ensemble.

Dès qu'un risque se pose pour la sécurité nationale (ou qu'une composante majeure de ce type de risques se présente), un organisme responsable est désigné. Ces organismes sont chargés (soit explicitement par voie législative, soit en raison de leurs compétences particulières) de gérer une situation d'urgence trouvant son origine dans un des risques particuliers recensés dans une liste les répertoriant.

Groupes de surveillance
Ils sont chargés d'obtenir des informations pour avoir une idée claire de la situation dans des conditions souvent chaotiques et de veiller à ce que des systèmes soient en place pour gérer efficacement les questions difficiles. Ils sont généralement composés de hauts fonctionnaires capables d'engager des ressources et d'arrêter des décisions au nom de leur organisation. Leur composition exacte dépend de la nature de la situation et ils regroupent des organismes ayant un rôle à jouer quant aux mesures à prendre pour résoudre le problème en question. Il peut parfois s'agir d'organismes qui ne se considèrent pas

habituellement comme des organismes de « sécurité nationale » et qui ne sont pas bien au fait du fonctionnement des structures du système de sécurité nationale.

Comité de hauts fonctionnaires chargé de la coordination de la sécurité intérieure et extérieure
Ce comité donne des orientations stratégiques, soutient l'organisme responsable et communique avec les organismes politiques, notamment pour conseiller le Comité national de sécurité du Cabinet.

Groupes de travail ou de spécialistes
Ces groupes sont établis lorsqu'il est souhaitable qu'une profession ou une discipline, par exemple le réseau juridique national, un groupe consultatif économique, la communauté scientifique et la communauté du renseignement, détermine et présente un point de vue général, ou des conseils particuliers, à un groupe de surveillance ou au Comité de hauts fonctionnaires.

Centre national de gestion des crises
Cet organisme sécurisé et centralisé est chargé de mener diverses tâches de coordination, telles que la direction et la planification des interventions et l'appui aux interventions, la collecte, la gestion et le partage des informations et la coordination entre la réponse opérationnelle et la réponse stratégique nationale.
Méthode de l'équipe rouge
La méthode de l'équipe rouge consiste à soumettre un plan, des idées ou des hypothèses à une analyse rigoureuse et à les remettre en question afin d'améliorer la validité et la qualité du plan définitif. Des équipes rouges interinstitutions peuvent être mises sur pied à toutes les étapes d'une crise (et d'un projet) et peuvent travailler en parallèle d'une intervention. Pendant une crise nationale, cette méthode permet d'envisager sous un angle nouveau l'approche de gestions des risques adoptée.

Source : Département du Premier Ministre et du Cabinet, Nouvelle-Zélande, à l'adresse suivante : www.dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security

Une fois que les structures et processus principaux de gestion des crises ont été déterminés, les stratégies de protection des infrastructures critiques doivent permettre de veiller à ce qu'ils fonctionnent sans heurts en cas de besoin. Le chapitre 5 (Assurer la coordination entre les organismes nationaux) examine les conditions préalables à une prise de décisions fluide et rapide et traite des exercices conjoints public-privé comme outils essentiels de la gestion des crises.

Il faut également garder à l'esprit qu'en cas d'attaque chimique, biologique, radiologique ou nucléaire, il convient de prendre des mesures spéciales pour protéger la population et les premiers intervenants de toute contamination et limiter la propagation potentielle de matières dangereuses. Une intervention spécialisée suppose de planifier des interventions d'urgence adaptées et d'avoir recours à du matériel spécialisé aux fins de la détection, de la protection individuelle et de la décontamination.

2.10 Garantir la pertinence et la viabilité des stratégies

Il importe de faciliter la mise en œuvre concrète des stratégies de protection des infrastructures critiques en : i) veillant à leur viabilité financière ; ii) mettant en place des mécanismes d'examen et de suivi dans le cadre des processus de gestion des risques pour les listes existantes d'infrastructures et les stratégies elles-mêmes.

2.10.1 Viabilité financière

Bien qu'il incombe au premier chef aux exploitants d'infrastructures critiques de garantir la résilience de leurs équipements et processus essentiels, l'amélioration des mesures de protection physique et informatique implique souvent d'engager des ressources considérables. Il peut donc être très coûteux de garantir la résilience des infrastructures critiques. Pour cette raison, il importe de garantir la viabilité financière des investissements visant à améliorer la protection des infrastructures critiques. En pratique, les pays doivent trouver un équilibre en termes de partage des coûts entre les propriétaires et exploitants d'infrastructures critiques, les organismes publics et les compagnies d'assurance.

La création de mesures incitatives est un outil important pour encourager la participation des entreprises. Il peut s'agir de réglementations, de subventions, d'exonérations fiscales ou encore de prêts. Ces mesures semblent d'autant plus importantes en période de crise économique, pendant lesquelles les exploitants vont plus facilement privilégier les objectifs de croissance à court terme plutôt que les objectifs de protection à long terme.

ÉTUDE DE CAS 24
Mesures incitatives et mécanismes de financement aux fins de la résilience des infrastructures critiques en Suède, au Japon et aux États-Unis

Suède :
La stratégie suédoise de protection des infrastructures critiques tient compte des besoins supplémentaires en ressources humaines et financières que suppose sa mise en œuvre. Conformément à l'ordonnance de 2006 sur la préparation aux situations d'urgence et les alertes renforcées, les autorités peuvent demander des fonds au titre de la préparation aux situations d'urgence. D'autres organismes peuvent bénéficier indirectement de ce mécanisme de financement en coopérant à des projets avec les autorités désignées dans l'ordonnance.

Source : Plan d'action pour protéger les fonctions vitales de la société et les infrastructures critiques, 2014, disponible à l'adresse suivante : www.msb.se/RibData/Filer/pdf/27412.pdf

Japon :
Le Japon redouble d'efforts pour convaincre les entreprises que les mesures privées visant à renforcer la cybersécurité ne doivent pas être vues comme un fardeau, mais comme un investissement visant à promouvoir les produits et services des entreprises ainsi qu'à améliorer leur compétitivité. Dans ce contexte, il est en train de mettre en place un dispositif consistant à récompenser les entreprises au moyen d'avantages financiers qui donnera la priorité aux questions cybernétiques et, en outre, subventionne des programmes visant à encourager le perfectionnement professionnel des employés ayant des compétences en cybersécurité industrielle.

Source : Arie H.2017

États-Unis :
Dans le cadre du programme de sécurité et de résilience du Plan national de protection des infrastructures, en partenariat avec le National Institute of Hometown Security (NIHS), le Département de la sécurité du territoire finance des idées novatrices qui peuvent permettre à toutes les personnes

concernées par les infrastructures critiques d'obtenir des outils et des technologies. L'objectif est que les projets financés dans le cadre de ce programme obtiennent des résultats concrets à court terme afin qu'ils puissent être élaborés et mis en œuvre rapidement, mais aussi qu'ils soient viables à long terme sur les plans financier, pratique et logistique afin d'améliorer la sécurité et la résilience des infrastructures critiques dans plusieurs secteurs pour les années à venir. Les projets sont évalués par un groupe indépendant du NIHS selon une série de critères qui tiennent également compte de leur viabilité et de leurs effets attendus.

Source : Département de la sécurité intérieure, à l'adresse suivante : www.dhs.gov/nipp-challenge

La viabilité financière des stratégies de protection des infrastructures critiques repose également sur la conception de mécanismes d'assurance efficaces, en particulier en cas de mesures de relèvement nécessaires à la reconstruction de biens gravement endommagés et à la restauration des services interrompus. Les discussions autour de la question des régimes d'assurance des infrastructures critiques n'ont commencé qu'après les attentats du 11 septembre. Auparavant, le risque terroriste était généralement pris en compte dans les polices d'assurance type sans qu'il soit nécessaire de payer des primes plus élevées. Après les attentats du 11 septembre et d'autres attentats terroristes extrêmement destructeurs comme ceux qui ont eu lieu à Madrid le 11 mars 2004, les mentalités ont radicalement changé en raison des indemnisations record qu'ont dû verser les assureurs. Comme l'a observé Michel-Kerjan, en analysant le terrorisme dans le cadre de la question de la protection des infrastructures critiques, on constate que le terrorisme est désormais une source notoire de risques graves, lesquels testent les limites des assurances (Michel-Kerjan, 2018, p. 12). Étant donné qu'il ne suffit pas de dépendre uniquement des dispositifs des marchés, les gouvernements doivent définir la nature et l'ampleur de leur participation financière aux mesures de relèvement des infrastructures critiques. Aujourd'hui, la création et la mise en place d'une protection financière adaptée à de tels événements sont de plus en plus souvent au centre des discussions nationales et dépassent le simple domaine des assurances (Michel-Kerjan, 2018, p. 12).

ÉTUDE DE CAS 25
Régimes d'assurance pour la résilience des infrastructures critiques face aux actes terroristes en France, en Espagne, aux États-Unis et au Royaume-Uni

France :
Le programme GAREAT (Gestion de l'assurance et de la réassurance des risques attentats et actes de terrorisme) est une structure à but non lucratif composée de compagnies d'assurance et active depuis 2002. Cette structure est chargée de la gestion de la réassurance des risques d'« attentats » et d'actes de terrorisme entraînant des dommages sur le territoire français (indépendamment du pays où a eu lieu l'acte de terrorisme). Elle est composée de deux sections : la section des « Grands risques », qui comprend les risques dont les capitaux assurés s'élèvent à 20 millions d'euros et plus, et la section des « Risques petits et moyens », qui gère les risques dont les capitaux assurés sont inférieurs à 20 millions d'euros. Elle repose sur le principe de « mutualité » entre ses adhérents, qui sont solidaires les uns des autres au sein d'une même section. L'État accorde au programme GAREAT une couverture illimitée par l'intermédiaire de la Caisse centrale de réassurance.

Source : GAREAT, www.gareat.com

Espagne :
Le Consortio de compensación de seguros indemnise les dommages causés aux personnes et aux biens par des « risques exceptionnels ». Pour avoir droit à une indemnisation, il faut avoir souscrit une police d'assurance dans certaines de ses succursales. La couverture spéciale qui est proposée par cette entité est automatique lorsque les dommages sont causés par un acte de terrorisme. Il s'agit d'un organisme public rattaché au Ministère de l'économie, de l'industrie et de la compétitivité.

Source : Ministère de l'économie, de l'industrie et de la compétitivité, à l'adresse suivante : www.consorseguros.es/web/inicio

États-Unis :
Le système américain repose sur un accord de partage des risques entre le Gouvernement fédéral, l'assuré et l'assureur. En vertu de la loi de 2002 sur l'assurance contre les risques terroristes, les assureurs sont tenus de proposer à leurs clients une assurance contre le terrorisme, dont ils sont toutefois libres de fixer le prix. Les clients, quant à eux, ne sont pas tenus de souscrire à cette assurance. En vertu de la loi de 2002, l'attaque doit être confirmée comme étant un « acte de terrorisme » par le Secrétaire du Trésor. Par définition, l'attaque doit servir des intérêts étrangers pour être considérée comme telle.

Royaume-Uni :
Le système britannique repose sur un partenariat public-privé intitulé Pool Re. La plupart des compagnies d'assurance proposant des assurances commerciales et des assurances de dommages indirects au Royaume-Uni sont adhérentes à Pool Re et ont accepté de proposer à leurs clients une assurance contre le terrorisme. Toute personne ayant souscrit ce type d'assurance et subissant des dommages causés par un acte de terrorisme doit contacter sa compagnie d'assurance, qui prendra les dispositions nécessaires pour que sa demande soit examinée suivant la procédure habituelle. Pool Re a conclu des accords avec l'ensemble de ses compagnies adhérentes selon lesquels il leur sera remboursé le coût des sinistres versé au titre de l'assurance contre le terrorisme qu'elles offrent. Le Gouvernement s'est engagé à soutenir Pool Re si jamais il ne disposait pas de fonds suffisants pour payer une indemnisation légitime.

Source : Pool Re, www.poolre.co.uk/

2.10.2 Mécanismes d'examen et de suivi

Les économies sont dynamiques et les infrastructures qui assuraient auparavant des services essentiels à la société et à l'économie peuvent être fermées pour une raison quelconque ou remplir des fonctions qui ne sont plus considérées comme essentielles. Par exemple, les mines de charbon peuvent céder la place à d'autres sources de production d'énergie. D'autre part, tout simplement, certains biens peuvent ne plus remplir les fonctions auxquelles ils étaient destinés parce qu'ils sont devenus obsolètes ou n'ont pas été retenus pour d'autres raisons économiques.

De plus, la nature et l'intensité des menaces qui pèsent sur les infrastructures critiques peuvent évoluer. Les résultats de certaines évaluations des risques, même précises, effectuées à un moment donné, peuvent ne plus correspondre à la réalité sur le terrain. Certains groupes terroristes peuvent simplement représenter une menace moindre pour certaines zones géographiques tout en continuant à exercer des pressions ailleurs. Par exemple, à la fin de 2017, l'EIIL avait perdu le

contrôle d'environ 95 % du territoire qu'il contrôlait en 2014. Les infrastructures critiques situées sur ces territoires ne font probablement plus face au même type et à la même intensité de menace de la part de l'EIIL, bien que de nouveaux groupes ou acteurs puissent représenter un danger. Dans d'autres cas, la menace pourrait ne pas avoir évolué autant que la vulnérabilité de certaines infrastructures en raison, par exemple, de leur vieillissement ou de leur manque d'entretien.

Dans cette optique, les stratégies de protection des infrastructures critiques doivent prévoir des mécanismes visant, à intervalles réguliers, les objectifs suivants :

- Mettre à jour les « listes » d'infrastructures critiques nationales, souvent très longues ;
- Réévaluer les risques ;
- Revoir le ou les documents stratégiques de protection des infrastructures critiques afin d'améliorer la gestion des risques, de déceler les changements des risques existants et de recenser de nouveaux risques.

En prenant les trois mesures mentionnées ci-dessus, les organismes publics devraient tout naturellement inciter les exploitants d'infrastructures critiques à suivre la même logique de partenariat public-privé qui a été mise en avant dans les sections précédentes.

ÉTUDE DE CAS 26
Mise à jour du « catalogue » des infrastructures critiques de l'Espagne

Le décret royal 704/2011 portant réglementation de la protection des infrastructures critiques dispose qu'en cas de modification importante des infrastructures apparaissant dans le catalogue national, si ces modifications sont pertinentes aux fins de cette réglementation, les exploitants concernés doivent communiquer, par les moyens mis à leur disposition par le Ministère de l'intérieur, toutes nouvelles informations au Centre national pour la protection des infrastructures et la cybersécurité, qui les validera avant leur intégration au catalogue. En tout état de cause, la mise à jour des informations disponibles devrait avoir lieu tous les ans (article 5, paragraphe 5).

3. ÉTABLIR LA RESPONSABILITÉ PÉNALE

Résolution 2341 (2017) du Conseil de sécurité
Paragraphe 3

Le Conseil de sécurité […]

Rappelle que, dans sa résolution 1373 (2001), il a décidé que tous les États devaient ériger les actes de terrorisme en infractions graves dans la législation et la réglementation nationales et demande à tous les États Membres de veiller à affirmer la responsabilité pénale de ceux qui perpétuent des attaques terroristes visant à détruire les infrastructures critiques ou à les rendre inutilisables, ou qui se livrent à des activités de planification, de formation, de financement ou de soutien logistique en lien avec ces attaques.

3.1 Objectifs de l'incrimination des attaques contre les infrastructures critiques

L'obligation d'incriminer les actes perpétrés contre les infrastructures critiques contribue à la réalisation de trois objectifs intimement liés :

- Offrir des niveaux de dissuasion adéquats par l'application de pénalités graves aux auteurs d'actes de terrorisme contre les infrastructures critiques ;
- Perturber les projets criminels et terroristes dirigés contre des infrastructures critiques par le recours au droit pénal à titre préventif. La dimension préventive de la résolution 2341 (2017) ressort clairement de l'obligation faite aux pays d'incriminer, notamment, les « activités de planification, de formation, de financement ou de soutien logistique » en lien avec des attaques terroristes ;
- Établir les bases juridiques et les conditions préalables en vue d'une coopération internationale fructueuse dans le domaine de la justice pénale relative aux questions liées aux infrastructures critiques.

La section 3.2 examine dans quelle mesure le cadre juridique universel contre le terrorisme fait face aux actes criminels perpétrés à l'encontre d'infrastructures critiques. Les sections 3.3., 3.4 et 3.5 donnent un aperçu de la manière dont les législations pénales des pays traitent des questions de responsabilité relatives aux infrastructures critiques et de la manière dont l'établissement d'infractions pénales est lié à la coopération internationale dans le domaine pénal. De plus, dans ces sections, les principales options offertes par le droit pénal font l'objet d'un examen sous l'angle de la rédaction législative, compte tenu des dispositions et prescriptions internationales, y compris du point de vue des droits de la personne.

3.2 L'incrimination des actes contre les infrastructures critiques dans les résolutions du Conseil de sécurité et les conventions internationales

La résolution 2341(2017) a la particularité d'être le premier instrument du Conseil de sécurité à demander expressément aux États d'incriminer les actes perpétrés contre les infrastructures critiques. Cela dit, cette résolution se fonde sur un certain nombre de résolutions préalablement

adoptées qui énoncent des prescriptions générales visant à établir la responsabilité pénale des auteurs d'actes terroristes. L'instrument qui a fait date en la matière (et auquel la résolution 2341 (2017) renvoie explicitement) est la résolution 1373 (2001). Adopté peu après les évènements du 11 septembre, cet instrument prévoit, notamment, un ensemble complet de prescriptions d'ordre pénal telles que les obligations :

- D'incriminer le fait de fournir ou de réunir des fonds en lien avec la commission d'actes terroristes ;
- De refuser l'asile à quiconque planifie, soutient ou commet des actes terroristes, et de traduire en justice les personnes en cause ;
- D'ériger les actes terroristes en infractions pénales graves en droit interne.

Outre les résolutions du Conseil de sécurité, une série de traités relatifs à la prévention et à la suppression du terrorisme international énonce les prescriptions relatives à l'incrimination en matière d'infrastructures critiques. Faute d'un accord sur le champ d'application d'une convention générale couvrant toutes les formes et manifestations du terrorisme international, ces instruments ont été adoptés sur une période de plus de 50 ans et suivant une approche sectorielle. L'approche progressive et pragmatique retenue par la communauté internationale a débouché sur l'adoption de conventions et de protocoles portant sur des domaines particuliers tels que, par exemple, la sécurité maritime et aérienne, le nucléaire et le financement du terrorisme.

À l'instar des résolutions du Conseil de sécurité, ces conventions et protocoles ne mentionnent pas l'expression « infrastructures critiques ». Cela peut s'expliquer en partie par le fait que la plupart de ces instruments ont été adoptés à une époque où la notion même d'« infrastructures critiques » n'avait pas encore trouvé sa place dans le débat sur les politiques mondiales de lutte contre le terrorisme. Toutefois, comme le montre le tableau [numéro], la plupart d'entre eux prévoient des dispositions érigeant en infractions les actes malveillants qui visent la destruction ou la perturbation du fonctionnement des infrastructures critiques. Les infractions de cette nature sont souvent décrites en détail, étant donné qu'elles ont fait l'objet de travaux de rédaction minutieux dans le cadre de longues négociations techniques et diplomatiques.

Dans la mesure où les pays sont parties à de tels instruments, ils sont tenus d'en incorporer les dispositions dans leur droit interne, notamment en érigeant en infractions pénales les actes mentionnés dans ces textes. Les pays qui ne sont pas parties à certains des protocoles et conventions contre le terrorisme sont engagés à les ratifier ou à y adhérer comme il le leur est demandé, entre autres, dans la résolution 1373 (2001).

Tableau 6 : Infractions relatives aux infrastructures critiques dans les instruments universels de lutte contre le terrorisme

Infrastructures critiques	Conventions et protocoles	Principales infractions * ** (Pour l'éventail complet des prescriptions et le libellé exact employé par les conventions, voir les textes officiels des traités)*

Domaine aérien	**La Convention de 1963 relative aux infractions et à certains autres actes survenant à bord des aéronefs (et son Protocole de 2014 y portant amendement)**	Les États contractants suivants sont compétents pour connaître des infractions commises à bord d'un aéronef : - L'État d'immatriculation de l'aéronef ; - l'État d'atterrissage, lorsque l'aéronef à bord duquel l'infraction est commise atterrit sur son territoire et que l'auteur présumé de l'infraction est encore à bord ; - l'État de l'exploitant, lorsque l'infraction est commise à bord d'un aéronef loué sans équipage à un preneur dont le principal établissement ou, à défaut, la résidence permanente se trouve dans ledit État.
	La Convention de 1970 pour la répression de la capture illicite d'aéronefs (et son Protocole additionnel de 2010)	Commet une infraction pénale toute personne qui s'empare d'un aéronef en service ou en exerce le contrôle par violence ou menace de violence, ou par contrainte, ou par toute autre forme d'intimidation, ou par tout moyen technologique
	La Convention de 1971 pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile **et** **Le Protocole de 1988 pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale, complété par**	Commet une infraction pénale toute personne qui : - accomplit un acte de violence à l'encontre d'une personne à bord d'un aéronef en vol, si cet acte est de nature à compromettre la sécurité de cet aéronef ; - détruit un aéronef en service ou cause à un tel aéronef des dommages qui le rendent inapte au vol ou qui sont de nature à compromettre sa sécurité en vol ; - place ou fait placer sur un aéronef en service, par quelque moyen que ce soit, un dispositif ou des substances propres à détruire ledit aéronef ou à lui causer des dommages qui le rendent inapte au vol ou qui sont de nature à compromettre sa sécurité en vol ;
	La Convention de 2010 sur la répression d'actes illicites dirigés contre l'aviation civile internationale	- détruit ou endommage des installations ou services de navigation aérienne ou en perturbe le fonctionnement, si l'un de ces actes est de nature à compromettre la sécurité d'aéronefs en vol ; - communique une information qu'elle sait être fausse et, de ce fait, compromet la sécurité d'un aéronef en vol ; - utilise contre un aéronef ou à bord d'un aéronef en service une arme biologique, chimique ou

		nucléaire ou des matières explosives ou radioactives, ou des substances semblables, d'une manière qui provoque ou est susceptible de provoquer la mort, ou de causer des dommages corporels graves ou des dégâts graves à des biens ou à l'environnement ; - détruit ou endommage gravement les installations d'un aéroport servant à l'aviation civile internationale ou des aéronefs qui ne sont pas en service et qui se trouvent dans l'aéroport, ou perturbe les services de l'aéroport, si cet acte compromet ou est de nature à compromettre la sécurité dans cet aéroport.
Domaine maritime	**Convention de 1988 pour la répression d'actes illicites contre la sécurité de la navigation maritime**	Commet une infraction pénale toute personne qui : - s'empare d'un navire ou en exerce le contrôle par violence ou menace de violence, ou toute autre forme d'intimidation ; - accomplit un acte de violence à l'encontre d'une personne se trouvant à bord d'un navire, si cet acte est de nature à compromettre la sécurité de la navigation du navire ; - détruit ou cause à un navire ou à sa cargaison des dommages qui sont de nature à compromettre la sécurité de la navigation du navire ; - place ou fait placer sur un navire, par quelque moyen que ce soit, un dispositif ou une substance propre à détruire le navire ou à causer au navire ou à sa cargaison des dommages qui compromettent ou sont de nature à compromettre la sécurité de la navigation du navire ; - détruit ou endommage gravement des installations ou services de navigation maritime ou en perturbe gravement le fonctionnement, si l'un de ces actes est de nature à compromettre la sécurité de la navigation d'un navire ; - communique une information qu'elle sait être fausse et, de ce fait, compromet la sécurité de la navigation d'un navire.

	Protocole de 2005 relatif à la Convention pour la répression d'actes illicites contre la sécurité de la navigation maritime	Commet une infraction pénale toute personne qui : - lorsque cet acte, par sa nature ou son contexte, vise à intimider une population ou à contraindre un gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque : utilise contre ou à bord d'un navire, ou déverse à partir d'un navire des explosifs, des matières radioactives ou des armes nucléaires, biologiques ou chimiques, d'une manière qui provoque ou risque de provoquer des dommages corporels ou matériels graves.
	Protocole de 1988 à la Convention pour la répression d'actes illicites contre la sécurité des plates-formes fixes situées sur le plateau continental	Commet une infraction pénale toute personne qui : s'empare d'une plateforme ou en exerce le contrôle par violence ou menace de violence, ou toute autre forme d'intimidation ; accomplit un acte de violence à l'encontre d'une personne se trouvant à bord d'une plateforme fixe, si cet acte est de nature à compromettre la sécurité de la plateforme ; détruit une plateforme fixe ou lui cause des dommages qui sont de nature à compromettre sa sécurité ; place ou fait placer sur une plateforme fixe un dispositif ou une substance propre à détruire la plateforme fixe ou de nature à compromettre sa sécurité.
	Protocole de 2005 relatif au Protocole pour la répression d'actes illicites contre la sécurité des plates-formes fixes situées sur le plateau continental	Commet une infraction pénale toute personne qui : lorsque cet acte, par sa nature ou son contexte, vise à intimider une population ou à contraindre un gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque : utilise contre ou à bord d'une plateforme fixe, ou déverse à partir d'une plateforme fixe, des explosifs, des matières radioactives ou des armes BCN, d'une manière qui provoque ou risque de provoquer la mort ou des dommages corporels ou matériels graves.

Domaine nucléaire	**Convention internationale de 2005 pour la répression des actes de terrorisme nucléaire** **et** **Amendement de 2005 à la Convention sur la protection physique des matières nucléaires**	Commet une infraction toute personne qui : utilise ou endommage une installation nucléaire, en perturbe le fonctionnement, ou commet tout autre acte dirigé contre une installation nucléaire de façon à libérer ou risquer de libérer des matières radioactives, dans l'intention d'entraîner la mort d'une personne ou de lui causer des dommages corporels graves ; ou dans l'intention de causer des dégâts substantiels à des biens ou à l'environnement ; ou - qui sait que l'acte commis peut provoquer la mort ou des blessures graves pour autrui ou des dommages substantiels aux biens ou à l'environnement par suite de l'exposition à des rayonnements ou du relâchement de substances radioactives, à moins que cet acte ne soit entrepris en conformité avec le droit national de l'État partie sur le territoire duquel l'installation nucléaire est située ; ou - qui menace de commettre une de ces infractions dans le but de contraindre une personne physique ou morale, une organisation internationale ou un État à faire ou à s'abstenir de faire un acte.
Domaine gouvernemental	**Convention de 1973 sur la prévention et la répression des infractions contre les personnes jouissant d'une protection internationale**	Est considéré comme une infraction : le fait de commettre, en recourant à la violence, contre les locaux officiels, le logement privé ou les moyens de transport d'une personne jouissant d'une protection internationale une attaque de nature à mettre sa personne ou sa liberté en danger.
Domaine intersectoriel	**Convention internationale de 1997 pour la répression des attentats terroristes à l'explosif**	Commet une infraction toute personne qui : - livre, pose, ou fait exploser ou détonner un engin explosif ou autre engin meurtrier dans ou contre un lieu public, une installation gouvernementale ou une autre installation publique, un système de transport public ou une infrastructure dans l'intention de causer des destructions massives de ce lieu, cette installation, ce système ou cette infrastructure, lorsque ces destructions entraînent ou risquent d'entraîner des pertes économiques considérables.

	Convention internationale de 1999 pour la répression du financement du terrorisme	Commet une infraction toute personne qui : - fournit ou réunit des fonds dans l'intention de les voir utilisés ou en sachant qu'ils seront utilisés en vue de commettre un acte de terrorisme (selon la définition de la présente Convention) ou tout autre acte constituant une infraction au regard de l'un des instruments universels contre le terrorisme.

Mis à part le cadre juridique universel contre le terrorisme, plusieurs instruments régionaux fixent des prescriptions relatives à l'incrimination en matière d'infrastructures critiques, notamment dans le domaine des infrastructures d'information critiques. Le texte qui marque un tournant en l'occurrence est la convention de 2001 du Conseil de l'Europe sur la cybercriminalité, laquelle, pour la première fois, a introduit au niveau international le descriptif d'actes criminels relatifs à la violation de la sécurité des réseaux (outre l'instauration de pouvoirs et de procédures tels qu'en matière de perquisition et d'interception de données informatiques). Plus récemment, l'Union européenne a adopté une directive visant, entre autres, à harmoniser la législation pénale des États membres dans le domaine des attaques dirigées contre les systèmes informatiques. La Convention de l'Union africaine de 2014 sur la cybersécurité et la protection des données en est un autre exemple (voir l'étude de cas ci-dessous).

ÉTUDE DE CAS 27
Les cadres juridiques de l'Union européenne et de l'Union africaine en matière d'incrimination des attaques contre les systèmes d'information

Directive de l'Union européenne de 2013 relative aux attaques contre les systèmes d'information

Un des objectifs clefs de cet instrument est l'établissement de règles minimales pour la définition des infractions pénales et sanctions correspondantes. La directive prévoit des sanctions pénales, au moins dans les cas où les faits ne sont pas mineurs. Les États membres peuvent déterminer, en fonction du droit national et de la pratique nationale, ce qui constitue un fait mineur. La directive vise, par exemple, la création de réseaux zombies, c'est-à-dire l'acte d'établir un contrôle à distance d'un nombre important d'ordinateurs en les contaminant au moyen de logiciels malveillants dans le cadre de cyberattaques ciblées. Une fois créé, le réseau d'ordinateurs contaminés qui constitue le réseau zombie peut être activé à l'insu des utilisateurs dans le but de lancer une cyberattaque à grande échelle.

Point essentiel, la directive définit des circonstances aggravantes dans lesquelles les infractions visées sont passibles d'une peine d'emprisonnement maximale d'au moins cinq ans, à savoir :

- lorsqu'elles sont commises dans le cadre d'une organisation criminelle ;
- lorsqu'elles causent un préjudice grave ;
- lorsqu'elles sont commises contre le système d'information d'une infrastructure critique.

Convention de l'Union africaine de 2014 sur la cybersécurité et la protection des données

Conformément à cette Convention, adoptée en 2014, « chaque État partie s'engage à adopter les mesures législatives ou réglementaires qu'il jugera efficace considérant comme infraction criminelle

substantielle des actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes des technologies de l'information et de la communication et les données qu'ils traitent et des infrastructures réseau sous-jacentes […] ». (article 25).

Au nombre des dispositions concernant les prescriptions relatives à l'incrimination, celles qui sont le plus directement liées à la protection des infrastructures d'information critiques sont énoncées à l'article 29 (« Les infractions spécifiques aux technologies de l'information et de la communication »), sous les deux sous-rubriques « Atteintes aux systèmes informatiques » et « Atteintes aux données informatisées ».

Outre l'établissement d'infractions relatives aux atteintes directes aux systèmes informatiques, la Convention de l'Union africaine adopte une approche particulièrement préventive de la commission d'infractions cybercriminelles. À l'article 29 1) h), en particulier, les États parties s'engagent à « […] ériger en infraction pénale le fait sans droit, de produire, vendre, importer, détenir, diffuser, offrir, céder ou mettre à disposition un équipement, un programme informatique, tout dispositif ou donnée conçue ou spécialement adaptée pour commettre des infractions ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système informatique.

3.3 La rédaction de la législation pénale sur la protection des infrastructures critiques

Les autorités nationales sont tenues d'incorporer dans leur droit interne les éléments des infractions définies dans les conventions de lutte contre le terrorisme auxquelles leur pays est partie. De plus, elles doivent déterminer la mesure dans laquelle elles souhaitent ériger en infractions les actes commis à l'encontre des infrastructures critiques et qui dépassent le cadre des prescriptions énoncées dans ces conventions, prescriptions qui, comme on l'a vu dans la section précédente, ne couvrent que certains aspects de la question. Lorsque les autorités nationales envisageront d'introduire une législation complète sur les infrastructures critiques, il ne leur faudra pas oublier qu'il n'existe aucune définition des « infrastructures critiques » à l'échelon international. D'une manière générale, plusieurs options de rédaction peuvent s'offrir :

i) Incriminer les actes perpétrés à l'encontre de types particuliers d'infrastructure (approche par secteur) ;
ii) Incriminer les actes perpétrés à l'encontre d'infrastructures critiques en général (approche intersectorielle) ;
iii) Se fonder sur une législation pénale non spécifiquement axée sur les infrastructures critiques (approche indirecte).

Il convient de noter que les approches précitées ne sont pas mutuellement exclusives et qu'en pratique, les pays adoptent souvent un mélange des trois. Quelle que soit l'approche (ou la combinaison d'approches) retenue, les infractions pénales devraient être conçues dans le respect du principe de la légalité. Cela signifie que la responsabilité et les sanctions pénales devraient s'appuyer sur la promulgation préalable d'une interdiction énoncée avec suffisamment de précision et de clarté.

i) Approche par secteur

Les infractions relatives aux infrastructures critiques peuvent concerner certains domaines essentiels comme, entre autres, le nucléaire et le secteur des transports. Les actes visés peuvent être érigés en infraction, que le terrorisme soit ou non considéré comme un élément constitutif de l'infraction. Si la résolution 2341 (2017) demande aux États d'être en mesure d'établir la responsabilité pénale en cas d'actes terroristes, elle ne les empêche aucunement, cependant, d'étendre la portée des infractions visées en incriminant tout acte non lié à des motivations terroristes. Bien au contraire, le libellé auquel a recours la plupart des conventions relatives à la lutte contre le terrorisme va dans ce sens. Ainsi, en vertu de la Convention de 1970 pour la répression de la capture illicite d'aéronefs, les États parties sont tenus d'ériger en infraction le fait d'exercer le contrôle d'un aéronef (par violence ou menace, ou par toute autre forme d'intimidation), quelle que soit l'intention ou les motivations sous-jacentes du contrevenant.

Les pays de common law offrent plusieurs exemples de lois établies par secteur : par exemple, la loi sur la sécurité de l'aviation de 1994 des Fidji, la loi sur la répression des attentats terroristes à l'explosif de Sri Lanka de 1999 et la loi sur la protection des personnes jouissant d'une protection internationale du Royaume-Uni de 1999. Il arrive souvent qu'en cas d'approche par secteur, les infractions visées fassent partie de cadres normatifs plus larges ayant également pour objet de réglementer dans le détail divers aspects de tel ou tel secteur, comme les exigences et procédures d'autorisation. La loi japonaise sur la réglementation des matières, combustibles et réacteurs nucléaires en offre un exemple.

Cette approche présente l'avantage de permettre aux pays d'adapter leurs prescriptions en matière d'incrimination aux particularités de certains types d'infrastructure et de secteurs. Elle permet également de prévoir des sanctions qui reflètent mieux la perception du niveau « critique » de certains biens et les incidences attendues en cas de perturbations. En revanche, l'inconvénient majeur de cette approche, c'est qu'elle limite la portée de la loi pénale à une liste fermée de secteurs et de biens, en négligeant les autres.

ii) Approche intersectorielle

Plusieurs pays incriminent les actes dirigés contre les infrastructures critiques en les qualifiant directement d'infractions terroristes. Bien qu'en général les infractions terroristes relatives aux infrastructures critiques ne se limitent pas à certains secteurs en particulier, plusieurs pays dressent une liste non exhaustive d'exemples de types d'infrastructure concernés. Ainsi, la législation kényane entend par « acte terroriste » tout acte ou menace d'acte qui, notamment, perturbe un système électronique et interrompt ainsi la fourniture de services de communication, finances, transport ou autres services essentiels [ou] perturbe ou interrompt la fourniture de services essentiels ou d'urgence.

Dans la décision-cadre de l'Union européenne relative à la lutte contre le terrorisme[20], les actes dirigés contre les infrastructures critiques figurent bien en évidence parmi les éléments matériels des infractions terroristes sous la forme, notamment, du fait de causer « des destructions massives

[20] Décision-cadre de l'Union européenne du 13 juin 2002 relative à la lutte contre le terrorisme (2002/475/JHA), article premier.

à une installation gouvernementale ou publique, à un système de transport, à une infrastructure, y compris un système informatique, à une plateforme fixe située sur le plateau continental, à un lieu public ou une propriété privée susceptible de mettre en danger des vies humaines ou de produire des pertes économiques considérables », ou « la capture d'aéronefs et de navires ou d'autres moyens de transport collectifs ou de marchandises », ou « la perturbation ou l'interruption de l'approvisionnement en eau, en électricité ou toute autre ressource naturelle fondamentale ayant pour effet de mettre en danger des vies humaines ».

D'autre part, l'expression « infrastructures critiques », que l'on trouve dans la plupart des documents de stratégies et de politiques au niveau national, ne figure pas expressément dans les textes législatifs antiterroristes. Le plus souvent, il est fait référence aux notions d'« infrastructures publiques » ou de « services, installations ou systèmes essentiels », en général lorsque la destruction ou l'interruption du fonctionnement de ces derniers produit des pertes économiques considérables ou, entre autres incidences, met en danger des vies humaines.

Il est à noter que différents textes de loi érigeant en actes terroristes les attaques dirigées contre les infrastructures critiques veillent à prévoir des exemptions pour les actes commis dans le contexte de l'exercice légitime de certains droits civils, politiques ou sociaux. Ainsi, le Code criminel canadien exclut de la notion d'« activité terroriste » l'acte qui, s'il « perturbe gravement ou paralyse des services, installations ou systèmes essentiels, publics ou privés », est néanmoins commis « dans le cadre de revendications, de protestations ou de manifestations d'un désaccord ou d'un arrêt de travail qui n'ont pas pour but de provoquer l'une des situations mentionnées » [et relevant de la définition d'« activité terroriste »][21].

L'avantage d'une approche intersectorielle, c'est de fournir un cadre permettant de couvrir tous les domaines des infrastructures critiques, y compris ceux qui sont susceptibles d'être considérés comme tels à l'avenir. Si le droit pénal interne prévoit d'autres dispositions relatives à des secteurs particuliers, les textes législatifs en question s'appliqueront normalement comme une *lex specialis*. Le risque de cette approche est d'être imprécise, dans la mesure où le législateur pourra établir une série de sanctions indistinctement applicables à tous les secteurs. En pareils cas, les juges pourront adapter le niveau des sanctions aux circonstances avec une marge de manœuvre plus grande que si l'on avait opté pour une approche étroite par secteur.

[21] Code criminel, 83.01(1).

ÉTUDE DE CAS 28
Loi nº 33 de 2004 sur la protection de la démocratie constitutionnelle contre les activités terroristes et connexes (Afrique du Sud)

La définition sud-africaine du « terrorisme » et de l'« acte terroriste » fournit d'amples précisions sur les infrastructures critiques. Est ainsi considéré comme une « activité terroriste », notamment :

a) tout acte commis à l'intérieur ou à l'extérieur de la République, qui :
vi) vise à perturber ou à paralyser gravement des services, installations ou systèmes essentiels, ou la fourniture de tous services, installations ou systèmes, qu'ils soient publics ou privés, y compris mais sans s'y limiter :
aa) un système utilisé pour ou par un système électronique, y compris un système d'information ;
bb) un service ou système de télécommunication ;
cc) un service bancaire ou financier ou un système financier ;
dd) un système utilisé pour la fourniture de services publics essentiels ;
ee) un système utilisé pour ou par un service public essentiel ou un exploitant de transport ;
ff) une infrastructure essentielle ; ou
gg) tous services d'urgence essentiels, tels que les services de police, médicaux ou de protection civile ;
vii) engendre des pertes économiques considérables ou une déstabilisation importante de l'économie nationale d'un pays ; ou
viii) met la République dans une situation d'urgence publique grave ou d'insurrection générale, que les dommages visés aux paragraphes a) i) à vii) soient ou puissent être subis à l'intérieur ou à l'extérieur de la République, et que l'acte visé aux alinéas ii) à viii) ait été commis par quelque moyen ou méthode que ce soit ; et
b) qui vise, par sa nature ou son contexte, ou peut raisonnablement être considéré comme viser, en tout ou en partie, directement ou indirectement, à
menacer l'unité et l'intégrité territoriale de la République ;
intimider la population ou une partie d'entre elle, ou y susciter ou y faire naître des sentiments d'insécurité au regard de sa sécurité, y compris de sa sécurité économique, ou engendrer, causer ou propager des sentiments de terreur, peur ou panique au sein d'une population civile ; ou
à contraindre indûment, y compris par intimidation, à forcer, à obliger, à inciter ou à amener une personne, un gouvernement, l'ensemble de la population ou une partie d'entre elle, ou des organisations ou organismes nationaux ou internationaux, ou des organisations ou organismes intergouvernementaux, à accomplir ou à s'abstenir ou éviter d'accomplir un acte, ou à adopter une position particulière ou à y renoncer, ou à agir conformément à certains principes,

que la population ou la personne, le gouvernement, l'organisme, ou l'organisation ou institution visés aux alinéas ii) à iii), selon le cas, se trouve à l'intérieur ou à l'extérieur de la République ; et
c) qui est commis, directement ou indirectement, en tout ou en partie, au nom d'un motif, d'un objectif, d'une cause ou d'une entreprise politique, religieuse, idéologique ou philosophique individuelle ou collective […].

iii) Approche indirecte

Cette approche consiste à incriminer les actes dirigés contre des infrastructures critiques en invoquant des infractions pénales de référence comme, par exemple, le dommage aux biens, l'incendie criminel et la violation du droit de propriété.

Un des avantages de cette solution tient au fait que les pays peuvent s'appuyer sur un ensemble de base d'infractions bien établies en attendant l'adoption de cadres juridiques plus ciblés, ou pour combler les insuffisances de la nouvelle législation en matière d'infrastructures critiques. Elle peut aussi présenter un avantage pour les juges qui, dans de nombreux pays, maîtrisent souvent mieux l'application de ces infractions traditionnelles que celle des nouvelles dispositions relatives aux infrastructures critiques. Cette approche a néanmoins des inconvénients, dont l'absence de différenciation entre biens critiques et biens non critiques. De plus, l'interdiction d'appliquer les lois pénales par analogie soulève, à tout le moins, des doutes sérieux quant au fait de rendre applicables au cyberespace des infractions n'ayant été conçues que pour le monde physique (que l'on pense, par exemple, au recours aux infractions relatives à la violation du domaine de propriété dans le traitement de l'accès non autorisé à des systèmes informatiques)[22].

3.4 La portée de la législation pénale relative aux infrastructures critiques

Lors de la rédaction des infractions pénales relatives aux infrastructures critiques, une attention particulière devrait être accordée à leur champ d'application. Les autorités nationales devraient veiller à ce que leur législation pénale tienne dûment compte des scénarios suivants :

- Une attaque contre une infrastructure située sur le territoire de l'État a des effets importants sur un autre État. Un scénario de cette nature est très probable en cas d'actes perpétrés à l'encontre d'infrastructures d'information critiques. Prenons l'exemple d'un système de contrôle industriel situé dans un pays A qui gère l'approvisionnement en gaz dans un pays B : ce dernier, contrairement au pays A, enregistre des perturbations à l'issue du détournement du système de contrôle industriel ;

- À la suite d'une attaque contre une infrastructure critique située dans un pays A, son auteur présumé trouve refuge dans un pays B. Tous les traités universels de lutte contre le terrorisme font obligation aux pays d'établir leur juridiction extraterritoriale sur des actes commis à l'étranger dans au moins deux cas :

    - L'infraction a été commise par un de leurs ressortissants (principe de la nationalité active) ;
    - L'auteur présumé de l'infraction se trouve sur le territoire de l'État et n'est pas extradé vers un État en ayant fait la demande en raison de ce même acte (principe dit *aut dedere aut judicare*).

Certaines conventions relatives à la lutte contre le terrorisme énoncent des critères de compétence particuliers. Par exemple, dans le cas d'une infraction prévue par la Convention de 1970 pour la répression de la capture illicite d'aéronefs ou la Convention de 1971 pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, les juridictions nationales sont compétentes en cas d'infraction commise à bord d'un aéronef, si ce dernier atterrit sur le territoire de l'État alors que l'auteur présumé de ladite infraction se trouve toujours à bord et qu'aucun autre État partie ne demande pas son extradition à des fins de poursuite.

[22] D'un point de vue pratique, les enquêtes ayant trait à des infractions commises dans le cyberspace posent des problèmes particuliers quant à l'attribution des actes incriminés.

Dans les autres cas, les conventions relatives à la lutte contre le terrorisme prévoient l'exercice de compétences optionnelles, par exemple en cas d'infractions commises à l'étranger à l'encontre d'un ressortissant (principe de la nationalité passive). Les autorités nationales devraient envisager l'introduction de ces compétences supplémentaires et déterminer – pour ce qui touche aux cas ou aux domaines des infrastructures critiques non couverts par le cadre juridique international applicable – la portée adéquate des infractions y relatives les concernant.

3.5 La coopération internationale en matière pénale

Comme mentionné à la section 3.1, la nécessité pour les États d'incriminer les actes énoncés dans le cadre juridique universel contre le terrorisme est également essentielle à la facilitation de la coopération internationale en matière pénale. Dès lors que les infractions visées (c'est-à-dire en lien avec des infrastructures critiques) ont été introduites dans la législation pénale des États parties, les principaux obstacles juridiques à une bonne coopération peuvent être levés. Par exemple, l'obligation qui est faite ordinairement aux États de ne pouvoir accorder l'extradition (et, dans une moindre mesure, une assistance juridique mutuelle) que si l'acte considéré est érigé en infraction à la fois par l'État membre requis et l'État membre requérant sera automatiquement satisfaite si les deux États transposent fidèlement les dispositions d'un traité dans leurs législations pénales respectives.

Dans le même temps, la capacité des pays à engager des poursuites à l'encontre des contrevenants dépendra souvent de l'efficacité des canaux de coopération internationale en matière de répression, de restitution de fugitifs et d'échange d'éléments de preuve. Il est indispensable que les pays ayant l'intention de maximiser la protection de leurs infrastructures critiques du point de vue pénal tiennent compte du rôle des instruments universels de lutte contre le terrorisme en prévoyant des bases juridiques en matière d'extradition et d'assistance juridique mutuelle, soit en tant que complément ou à défaut d'accords bilatéraux ou régionaux à cet effet.

Sous l'angle répressif, Interpol définit dans son cadre stratégique pour la période 2017-2020 son premier objectif stratégique : « être la plaque tournante de l'information pour la coopération policière », objectif que l'organisation poursuit en reliant les Bureaux centraux nationaux de ses 192 pays membres par l'intermédiaire de ses canaux de communication sécurisés, parallèlement à d'autres organismes et partenaires autorisés dans le domaine de l'application de la loi, ainsi qu'en donnant accès à un ensemble de base de données criminelles.

Toute l'activité opérationnelle d'INTERPOL à l'appui de la coopération internationale entre ses pays membres en matière criminelle repose sur le réseau de communication policière de l'organisation, I-24/7. Depuis les vérifications de routine au passage des frontières jusqu'aux opérations ciblées menées dans les différents domaines de la criminalité comme depuis le déploiement d'équipes d'intervention spécialisées jusqu'à la recherche de fugitifs internationaux, I-24/7 est à la base de l'échange d'information entre les services de police du monde entier.

S'agissant de la lutte contre le terrorisme et des infrastructures critiques, la stratégie mondiale conduite par INTERPOL met l'accent sur l'importance fondamentale de la coopération

internationale entre les autorités responsables de l'application de la loi à l'échelle de la planète. Le mandat ainsi confié à INTERPOL en matière de lutte contre le terrorisme par cette stratégie consiste à donner à ses pays membres, au niveau répressif, les moyens et les possibilités de prévenir et d'entraver les activités terroristes grâce à l'identification des membres des réseaux concernés et de leurs affiliés, en s'attaquant aux principaux moteurs de leurs activités : déplacements et mobilité, présence en ligne, armes et matériels ainsi que financement.

Quel que soit le canal de coopération utilisé, les pays sont tenus de veiller au plein respect des normes en matière de procès équitable et de régularité des procédures. Cette obligation vaut non seulement dans le cadre des procédures nationales visant à établir la responsabilité pénale des personnes, mais aussi dans le cadre de celles engagées au nom d'autres pays en cas de restitution de fugitifs ou de transmission d'éléments de preuve.

4. PARTAGER DES INFORMATIONS ET DES EXPÉRIENCES

Résolution 2341 (2017) du Conseil de sécurité

Le Conseil de sécurité [...] :
4. *Demande aux États Membres d'étudier les moyens d'échanger des informations utiles et de prendre une part active à la prévention des attaques terroristes, à la protection contre ces attaques, à l'atténuation de leurs effets, à la préparation à de telles attaques, aux enquêtes et interventions menées en cas d'attaque et aux mesures de rétablissement d'un fonctionnement normal après une attaque terroriste visant ou pouvant viser des infrastructures critiques*
5. *Demande également aux États de créer ou de renforcer les partenariats nationaux, régionaux et internationaux avec les parties prenantes, tant publiques que privées, selon qu'il conviendra, de mettre en commun leurs informations et leurs données d'expérience aux fins des activités de prévention, de protection, d'atténuation des effets, d'enquête, d'intervention et de rétablissement d'un fonctionnement normal en cas de dégâts causés par des attaques terroristes visant des infrastructures critiques, notamment au moyen de formations communes et de l'utilisation ou de la mise en place des réseaux de communication ou d'alerte d'urgence pertinents*
7. *Engage l'Organisation des Nations Unies ainsi que les États Membres et les organisations régionales et internationales concernées qui ont élaboré leurs propres stratégies de protection des infrastructures critiques à collaborer avec tous les États et les organisations internationales, régionales, sous-régionales et autres organismes compétents pour dégager et mettre en commun de bonnes pratiques et mesures en matière de gestion du risque d'attaques terroristes contre des infrastructures critiques*

4.1 Partage de l'information dans le cadre des stratégies de protection des infrastructures critiques

Si toute stratégie en matière de protection des infrastructures critiques repose sur une structure de gouvernance, sa mise en œuvre nécessite un partage d'informations. Un partage adéquat de cette nature est essentiel pour protéger les infrastructures critiques à tous les niveaux et à toutes les étapes. Il s'agit d'un facteur clef sur lequel sont fondés les partenariats entre secteur public et secteur privé (voir section 4.5.2). La coordination entre les organismes nationaux repose sur le partage d'informations (voir chapitre 7). Enfin, l'ampleur et la qualité de la coopération internationale en matière d'infrastructures critiques dépendent de la capacité et de la volonté des États d'échanger des informations (voir chapitre 8).

4.2 Les dimensions du partage d'informations aux fins de la protection des infrastructures critiques

Lors de l'établissement des cadres opérationnels pour le partage d'informations, les stratégies de protection des infrastructures critiques et leurs plans de mise en œuvre devraient aborder trois questions fondamentales :

- quelles informations faudrait-il échanger et pourquoi ?
- de quelle manière une information relative à une tâche donnée sera-t-elle partagée ?
- entre qui l'information sera-t-elle partagée ?

Les informations peuvent être échangées au niveau stratégique, technique ou tactique. Elles peuvent par ailleurs être liées ou non à un problème particulier. Elles peuvent également faire l'objet d'un échange « en temps réel » dans le contexte d'une crise imminente ou en cours, lorsque le destinataire est censé prendre des mesures immédiates. Pour ce type d'informations, les plateformes de partage d'informations (et les dispositifs de sécurité qui y sont associés) sont structurées d'une tout autre manière que pour les informations visant à transmettre, notamment, des pratiques optimales ou des conseils stratégiques.

Le partage de l'information peut (et devrait) se faire entre différents types de parties prenantes :

- Entre entités publiques et exploitants d'infrastructures critiques (dans un secteur donné et entre secteurs);
- Entre exploitants d'infrastructures critiques (dans secteur donné et entre secteurs);
- Entre entités publiques.

4.2.1 Entre entités publiques et exploitants d'infrastructures critiques

Le processus de privatisation de plusieurs secteurs et sous-secteurs d'infrastructures critiques, tels que le gaz, les systèmes postaux et les services de télécommunication, qui s'est produit dans de nombreux pays, a fait passer plusieurs exploitations d'infrastructures critiques aux mains d'entreprises privées. Cette situation a, quant à elle, rendu nécessaire l'émergence de partenariats solides entre secteur public et secteur privé. L'échange d'informations aux fins de la protection des infrastructures critiques est une tâche essentielle qu'il convient d'accomplir dans le cadre de ces partenariats.

L'échange d'informations entre des organismes gouvernementaux et des exploitants d'infrastructures critiques devrait s'effectuer dans les deux sens et couvrir notamment :

Les menaces : par exemple, les forces de l'ordre et les services de renseignement devraient transmettre aux exploitants d'infrastructures critiques des informations sur les nouveaux types de menaces. Cela permettra de s'assurer que les exploitants procèdent à une évaluation des risques et prennent les mesures d'atténuation voulues. De même, les exploitants d'infrastructures critiques devraient communiquer aux organismes d'État compétents les résultats des évaluations qu'ils auront menées et des mesures d'atténuation qu'ils auront mises en place afin d'assurer une meilleure modulation des plans d'atténuation. Dans ce contexte, les notices mauves et orange d'INTERPOL présentent un intérêt particulier pour la diffusion d'informations urgentes au sein de la communauté policière mondiale et auprès du public. Si les notices mauves servent à solliciter ou à fournir des informations sur des modes opératoires, des objets, des dispositifs et des méthodes de dissimulation utilisés par des malfaiteurs, les notices orange, en revanche, sont utilisées pour alerter les services et entités concernés sur la menace grave et imminente pour la sécurité publique représentée par un événement, une personne, un objet ou certaines opérations ;

Les activités suspectes : les exploitants d'infrastructures critiques peuvent être invités à signaler les « indicateurs faibles », c'est-à-dire les situations inhabituelles qui, en soi, ne sont pas suffisamment graves pour déclencher l'alarme mais qui révèlent une menace imminente, lorsqu'elles sont examinées dans le contexte d'événements similaires ou lorsqu'un simple soupçon est corroboré par des informations émanant d'autres sources ;
Les données relatives à des événements antérieurs : les enseignements tirés d'événements antérieurs (concernant également ce qui a été fait ou non pour y faire face) peuvent donner d'importantes indications sur les moyens d'éviter que la même situation ne se reproduise, ce qui, par là même, jette les bases d'une gestion des risques plus efficace et de mesures de relèvement mieux adaptées.
Le tableau 7 résume les principaux types d'informations sur les infrastructures critiques que le secteur public pourrait échanger avec le secteur privé (et vice versa) pour faire face aux cybermenaces terroristes.

Tableau 7 : Types d'échange d'informations public-privé sur les cybermenaces terroristes

Informations du secteur public[23]	**Informations du secteur privé**
• Perspectives sur les capacités informatiques des principales organisations terroristes	• Informations sur les principales catégories d'actifs dans le secteur de l'énergie (par exemple, gaz, pétrole, électricité et énergies renouvelables ; indicateurs de fiabilité ; informations provenant des échanges commerciaux d'énergie)
• Informations sur les liens entre différents groupes terroristes et non terroristes	• Informations sur la vulnérabilité technique de matériel et logiciels informatiques spécifiques utilisés par les exploitants d'infrastructures énergétiques
• Indications sur les vecteurs d'attaques antérieures	• Informations anonymes sur les répercussions des attaques antérieures
• Indications sur les vecteurs potentiels d'attaques futures, mises en évidence par l'analyse de sites Web criminels clandestins	• Indications sur les besoins en matière de relèvement afin de faire face à différentes formes d'attaques
Source : OSCE 2013, p. 74.	• Enseignements tirés des schémas d'attaque dans d'autres secteurs d'infrastructures critiques et susceptibles de servir d'indicateurs d'alerte rapide pour le secteur de l'énergie

Le partage de l'information entre secteur public et secteur privé est souvent perçu comme un outil permettant d'abattre le mur entre ces deux mondes et de créer un véritable sentiment d'appartenance à une communauté autour des questions d'infrastructures critiques. La réalisation de cet objectif est d'autant plus importante que les secteurs privé et public ont tendance à se méfier

[23] Dans le tableau, le terme « secteur public » regroupe les « organismes gouvernementaux ».

l'un de l'autre et à ne pas échanger d'informations, notamment si celles-ci sont sensibles. Le secteur de l'énergie offre en la matière un exemple particulièrement intéressant de défi à relever. Selon l'OSCE, « dans le domaine de la sensibilisation aux questions de sécurité, on continue d'observer une grande différence entre la réalité de menaces potentielles d'attaques ciblées et la manière dont elles sont perçues. Cela tient principalement au fait que la plupart des attaques survenant dans les domaines de l'approvisionnement et de l'industrie énergétiques ne sont pas rendues publiques, car les exploitants des installations concernées ne souhaitent absolument pas que ces attaques soient divulguées. Cette façon d'envisager la question est à l 'origine d'une situation (les problèmes rencontrés étant perçus comme des événements isolés) qui ne fait que renforcer cette tendance à taire ce qui s'est passé. Dans certains pays, en revanche, le secteur privé est prié, incité et parfois obligé de signaler ces attaques » (OSCE 2013, p. 58).

Dans le contexte des cybermenaces, le partage d'informations précieuses peut inclure des renseignements sur :

- les vulnérabilités (par exemple, une faille exploitable dans un logiciel);
- les problèmes de cybersécurité rencontrés (par exemple, une attaque réussie contre les systèmes d'une entreprise);
- les mesures de défense (par exemple, des informations sur les retouches).

Dans ce contexte, le partage d'informations est capable de renforcer la sécurité et d'améliorer la cyberdéfense de manière considérable. Il peut être utile d'envisager de prendre des mesures pour encourager le partage d'informations au format électronique et réduire les risques. Par exemple, dans un premier effort pour faire face aux risques juridiques liés au partage d'informations électroniques, les États-Unis ont adopté la loi CISA (Cybersecurity Information Sharing Act)[24], qui prévoit, dans certaines circonstances, une exonération de responsabilité civile pour certaines activités de partage d'informations « menées conformément » aux dispositions de cette loi.

[24] Consolidated Appropriations Act of 2016, P.L. 114-113, Division N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2936, 6 U.S.C. §§ 1501-1510.

ÉTUDE DE CAS 29
Mesures d'incitation pour encourager le secteur privé à partager des informations dans le cadre de la stratégie de cybersécurité du Japon

La stratégie de cybersécurité du Japon vise à surmonter la réticence des entreprises à partager des informations avec les autorités publiques, lesquelles craignent de perdre leur crédibilité ou leur part de marché. Dans le cadre de cette stratégie, « pour dynamiser le partage d'informations, il est essentiel, d'une part, de soulager les exploitants d'infrastructures d'information critiques du fardeau que constitue la crainte de perdre leur crédit ou de ruiner la réputation de leur entreprise en livrant des informations à une partie intéressée et, d'autre part, de leur permettre au contraire de reconnaître les avantages qu'il y a à le faire. Le Gouvernement incitera les exploitants d'infrastructures d'information critiques à s'entendre sur la façon d'apporter des modifications appropriées aux renseignements à fournir, par exemple en dissimulant l'identité des informateurs et en précisant la portée et les limites de l'information à partager, et créera un environnement dans lequel la communication de renseignements ne fera subir aucune perte ni désavantage déraisonnable aux informateurs ».

Source : Japon 2015, p. 27.

4.2.2 Entre exploitants d'infrastructures critiques

La prestation des services les plus essentiels est possible grâce à des chaînes d'approvisionnement complexes qui nécessitent la participation de différentes entreprises œuvrant dans différents secteurs d'infrastructures et secteurs d'activités. Les dépendances inhérentes aux chaînes d'approvisionnement montrent qu'il importe d'avoir des canaux privé-privé appropriés pour faire circuler l'information entre les secteurs. Dans ce domaine, les échanges d'informations peuvent être de nature technique ou organisationnelle.

Il est également nécessaire pour les exploitants d'infrastructures critiques qui produisent ou fournissent le même type de biens ou de services dans le même secteur d'activité de mettre en place des dispositifs adéquats de partage de l'information. Cela est particulièrement vrai si l'on veut partager, notamment, des bonnes pratiques, des informations sur les méthodologies d'évaluation des risques, des mesures de protection en vigueur et des enseignements tirés à la suite de problèmes de sécurité. Il peut s'avérer utile pour les entreprises ayant une longue expérience de la protection des infrastructures critiques de transmettre leurs connaissances aux entreprises moins accoutumées aux cadres réglementaires et aux stratégies de conformité applicables. Dans le même temps, il faut reconnaître la difficulté intrinsèque résidant dans le fait d'assurer la fluidité des flux d'information entre des entreprises souvent concurrentes. C'est pourquoi les entreprises rechignent à coopérer, en particulier pour échanger des informations sensibles, de peur de perdre des parts de marché.

4.2.3 Entre entités publiques

La mise en place de mécanismes de partage d'informations entre organismes publics est essentielle, dans la mesure où ces derniers sont chargés de mettre en œuvre et de coordonner les actions liées à la protection des infrastructures critiques, aussi bien horizontalement que verticalement. À titre d'exemple, pour ce qui est du partage « horizontal » de l'information, on peut

citer le cas où plusieurs ministères sont responsables de secteurs différents et doivent œuvrer de concert pour résoudre des questions intersectorielles. On peut également citer le cas où les services de renseignement doivent fournir des informations aux autorités compétentes chargées de la protection des infrastructures critiques pour qu'elles puissent réaliser des évaluations des risques à l'échelle nationale. S'agissant des dispositifs de partage « vertical » de l'information, on peut citer l'exemple de ceux qui sont nécessaires à l'appui de la division du travail entre autorités municipales, régionales et nationales, en particulier (mais pas exclusivement) dans les États fédéraux.

Le partage de l'information entre entités publiques est un des aspects de l'action de coordination élargie entre organismes, qui est examinée plus en détail au chapitre 5.

ÉTUDE DE CAS 30
Sécuriser la circulation de l'information : le système de communication par satellite du Royaume-Uni (HITS)

La technologie peut considérablement aider les organismes à assurer la circulation de l'information essentielle en cas d'urgence. Au Royaume-Uni, cet objectif est poursuivi par le HITS. Mis au point par le Gouvernement britannique, le HITS est un système indépendant qui reste opérationnel en cas d'indisponibilité ou de dégradation des télécommunications fixes et mobiles classiques. Basé sur le réseau satellitaire militaire Skynet 5, il est accessible à la police et à d'autres membres de services d'urgence dans des sites fixes répartis dans tout le Royaume-Uni, et dispose d'unités transportables supplémentaires qui permettent de déployer le HITS n'importe où et n'importe quand selon les besoins. Assurant à la fois la transmission de voix et de données, ainsi que l'accès à Internet, le HITS joue un rôle essentiel en ce qu'il permet au dispositif de coordination dans les situations de crise une communication ininterrompue entre ses niveaux régionaux et nationaux pendant toute la durée d'un événement perturbateur.

Source : Cabinet Office du Royaume-Uni, à l'adresse : https://www.gov.uk/guidance/resilient-communications.

4.3 Conditions préalables à un partage efficace de l'information

L'expérience montre que l'efficacité du partage de l'information en matière de protection des infrastructures critiques dépend de deux facteurs fondamentaux :

- La capacité des principaux organismes à créer un climat de confiance entre les parties prenantes concernées ;
- La mise en place de niveaux de protection adéquats pour les informations sensibles dont le partage est encouragé ou rendu obligatoire en vertu d'accords de protection des infrastructures critiques.

Il est important que les personnes chargées d'élaborer des stratégies de protection des infrastructures critiques (et celles qui sont appelées à les mettre en œuvre) comprennent comment ces deux facteurs se recoupent. Si la confiance diminue lorsque l'information n'est pas protégée de manière adéquate, un niveau élevé de protection de l'information n'engendrera pas en soi une plus grande confiance entre les participants.

4.3.1 Confiance

L'instauration d'un véritable climat de confiance entre les participants à tel ou tel accord de partage d'informations peut prendre du temps et exige un engagement actif de la part de toutes les parties prenantes. Cependant, une fois la confiance établie, la qualité et la quantité des flux d'informations peuvent augmenter de manière significative.

Sur la base d'une enquête consacrée aux méthodologies employées en matière de protection des infrastructures critiques et portant principalement sur les pays européens, le manuel RECIPE a dressé une liste des principaux facteurs de réussite en matière de partage de l'information. Dans ce manuel de bonnes pratiques, il est en particulier indiqué que l'expérience a montré que la confiance s'établissait mieux lors de réunions de petite taille organisées en face à face. En règle générale, il y a des choses à faire et à ne pas faire. Habituellement, il est préférable de commencer par partager des informations à un niveau qui n'est pas trop détaillé. Il n'est pas toujours nécessaire de partager des informations trop spécifiques, par exemple des connaissances sur les infrastructures critiques et leur emplacement, ou des informations précises sur les vulnérabilités ou les problèmes de sécurité rencontrés. Plusieurs échanges d'information fructueux ont prouvé que le fait de commencer modestement aidait à établir le niveau de confiance voulu. Pour établir un climat de confiance, il faudrait que ce soient les mêmes personnes qui assistent aux réunions d'échange d'informations. Les participants devraient être nommés individuellement et être dotés d'un mandat et de responsabilités assez larges dans leur propre environnement. En général, aucun suppléant n'est autorisé. Les réunions de partage d'informations sont axées sur l'échange : toutes les organisations concernées doivent (en principe) fournir des informations. La personne qui communique des informations doit veiller à ce que leur contenu soit adéquat et à ce qu'elles soient fournies dans le bon contexte. Les informations communiquées devraient permettre à leurs destinataires de prendre les mesures appropriées dans leurs organisations respectives ou d'être alertés sur de nouvelles menaces. Avant tout, le fournisseur de renseignements en reste propriétaire et c'est lui qui décide de leur niveau de classification en fonction de leur degré de sensibilité. La plupart des échanges d'informations fructueux se font sur une base volontaire et reposent sur la confiance. Toutefois, il existe également quelques exemples d'échanges obligatoires dans le cadre desquels les informations relatives aux évaluations des risques et aux problèmes de sécurité rencontrés doivent être partagées, par exemple les rapports sur les perturbations importantes des réseaux de communication publics conformément à l'article 13a de la réglementation de l'Union européenne en matière de télécommunications. En cas d'approche obligatoire, il est souvent difficile de garantir la qualité des informations échangées. C'est la raison pour laquelle il est souligné également pour les approches obligatoires qu'une des clefs du succès de leur dispositif tient encore une fois au fait d'instaurer un climat de confiance et de favoriser un esprit de coopération volontaire. L'expérience montre que les outils d'échange d'informations électroniques sont surtout utiles à titre de compléments pour les communautés de partage d'informations déjà établies et fiables. Lorsqu'aucun climat de confiance n'est établi, il est très difficile d'en faire naître un qui soit fort dans l'environnement électronique (RECIPE 2011, p. 52).

4.3.2 Protection des informations sensibles

L'instauration d'un climat de confiance propice au partage d'informations repose sur la mise en place de cadres juridiques et opérationnels clairs qui soient propres à protéger la nature sensible des données partagées. En élaborant ces cadres avec l'objectif principal de faciliter la circulation d'informations aux fins de la protection des infrastructures critiques, il convient de toujours tenir compte de la nécessité de respecter les instruments applicables en matière de droit à la vie privée et de protection des données. En vertu de la Charte des droits fondamentaux de l'Union européenne, par exemple, les données à caractère personnel « doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification[25] ».

La directive 2008/114/CE du Conseil de l'Union européenne définit les « informations sensibles relatives à la protection des infrastructures critiques » comme suit : « informations sur une infrastructure critique qui, en cas de divulgation, pourraient être utilisées pour planifier et mettre en œuvre des actions visant à provoquer l'arrêt ou la destruction d'installations d'infrastructures critiques[26] ».

La même directive énonce un « principe de spécialité » selon lequel « les États membres, la Commission et les instances de surveillance compétentes veillent à ce que les informations sensibles relatives à la protection des infrastructures critiques européennes communiquées à d'autres États membres ou à la Commission ne soient pas utilisées à d'autres fins que la protection de ces infrastructures. [Cela] s'applique aussi aux informations échangées oralement durant les réunions au cours desquelles des questions sensibles sont examinées[27] ».

[25] Article 8.
[26] Article 2, paragraphe d).
[27] Article 9.

ÉTUDE DE CAS 31
Protection de renseignements sensibles sur la sûreté de l'aviation

L'Organisation de l'aviation civile internationale a élaboré des principes directeurs généraux sur la protection des informations relatives à la sûreté aérienne. La communication de ces dernières se limitera aux personnes qui en ont besoin dans l'exercice de leurs fonctions et qui sont donc autorisées à y avoir accès (principe dit du « besoin d'en connaître »). Des mesures de protection seront appliquées aux renseignements sensibles sur la sûreté de l'aviation, dont le degré de protection sera précisé par l'État ou les entités compétentes, en tenant compte des exigences nationales en matière de protection des informations sensibles établies par les autorités concernées. Il peut également être nécessaire d'appliquer des mesures de protection lors de l'identification, la classification, la réception, la conservation, la divulgation, la diffusion ou l'élimination d'informations sensibles en matière de sûreté aérienne.

Lorsque des renseignements de nature sensible sur la sûreté de l'aviation ne sont pas utilisés, ils seront conservés en lieu sûr afin d'empêcher tout accès non autorisé. Par exemple, l'utilisation d'armoires de sécurité, de pièces verrouillées ou de coffres-forts peut offrir davantage de protection, si celle-ci est jugée nécessaire. De même, il faut protéger les copies électroniques des documents d'information sensibles en matière de sûreté aérienne. Les États et les entités compétentes prendront des mesures pour veiller à ce que les personnes ayant accès à des informations sensibles en matière de sûreté aérienne ne les divulguent à aucune personne non autorisée. Il conviendra, par exemple, d'envisager de faire signer aux personnes autorisées un « accord de confidentialité » avant de leur donner accès à de telles informations.

À chaque fois que des États doivent échanger des informations en matière de sûreté aérienne, ils indiqueront clairement que celles-ci sont sensibles et feront part de toute exigence spécifique qu'ils auront concernant les mesures de protection à appliquer avant de partager de telles informations avec d'autres États. Les États qui reçoivent des informations sensibles en matière de sûreté aérienne appliqueront les mesures de protection requises pour empêcher toute utilisation ou divulgation non autorisée.

Source : Manuel de sécurité de l'Organisation de l'aviation civile internationale, Doc 8973-Distribution restreinte

En ce qui concerne les exploitants d'infrastructures critiques issus du secteur privé, ils ne partageront probablement des données sur des problèmes de sécurité ou des facteurs de vulnérabilité que s'ils reçoivent des assurances indiquant que la divulgation d'informations sensibles n'aura pas d'incidences négatives sur eux (par exemple, qu'elle ne donnera pas d'avantage compétitif à leurs concurrents, ou qu'elle ne sera pas utilisée contre eux par des organismes publics à des fins autres que la protection des infrastructures critiques).

Il n'est pas nécessaire de traiter toutes les informations relatives aux infrastructures critiques de manière confidentielle. De même, toutes les informations considérées comme « sensibles » ne doivent pas faire l'objet du même degré de protection. Les restrictions à la circulation des informations relatives aux infrastructures critiques peuvent prendre diverses formes et être plus ou moins rigoureuses selon les modalités et les objectifs propres à un certain type d'échange d'informations. La Nouvelle-Zélande, par exemple, a établi un principe de base selon lequel les problèmes de sécurité rencontrés doivent être traités au niveau de classification le plus bas

possible afin de permettre la diffusion rapide et efficace de l'information essentielle à tous les intervenants chargés d'atténuer les effets de ces problèmes.

Pour protéger les informations relatives aux infrastructures critiques, on peut commencer par adopter une législation fondée sur le principe selon lequel la divulgation inadéquate de données sensibles peut présenter des risques pour la sûreté nationale ou la sécurité publique. Au Canada, la loi de 2007 sur la gestion des urgences comprend une modification à la loi de 1985 sur l'accès à l'information en vue d'assurer la protection des renseignements sensibles fournis par les secteurs d'infrastructures critiques.

ÉTUDE DE CAS 32
Approches nationales en matière de protection des informations sensibles relatives aux infrastructures critiques : Australie et France

Australie :
Créé par le Gouvernement australien en 2003, le Trusted Information Sharing Network (TISN) est le principal mécanisme de concertation du pays en matière de partage d'informations entre les entreprises et le Gouvernement et d'initiatives de renforcement de la résilience. Il offre un environnement sécurisé dans lequel les propriétaires et les exploitants d'infrastructures critiques de sept groupes sectoriels se réunissent régulièrement pour partager de l'information et favoriser la coopération au sein de chaque secteur et entre secteurs afin de relever les défis posés à la sécurité et à la continuité des opérations. Les groupes sectoriels du TISN comprennent les secteurs bancaire et financier, les communications, l'énergie, l'alimentation, la santé, les transports et les services d'approvisionnement en eau. De plus, il existe des forums spécialisés (dits groupes d'intérêt intersectoriels) qui contribuent à l'étude ponctuelle des questions transversales et un groupe consultatif d'experts sur la résilience qui met fortement l'accent sur la résilience organisationnelle. Le conseil consultatif sur les infrastructures critiques (CIAC) fournit au TISN des conseils en matière de coordination et d'orientation stratégique. Il se compose des présidents de chacun des groupes du TISN, de hauts représentants et de hautes représentantes du Gouvernement australien issus des organismes compétents, et de hauts représentants des gouvernements des États et Territoires.

Source : Trusted Information Sharing Network, à l'adresse : https://tisn.gov.au/

France :
Les directives et plans établis en application du système national de sécurité des activités d'importance vitale (SAIV) sont classifiés au niveau Confidentiel Défense. Qu'il soit émetteur ou destinataire, l'exploitant d'infrastructures critiques veille à la destruction des documents classifiés dont il n'a plus à faire usage, notamment lorsque :
- un document classifié est révisé ou abrogé ;
- un « point d'importance vitale » est radié ;
- une « zone d'importance vitale » est radiée ;
- un exploitant perd la qualification « d'opérateur d'importance vitale » (OIV).

Un opérateur d'importance vitale peut ne pas vouloir faire apparaître certaines informations très sensibles touchant à la gestion des risques et des crises. Il doit, dans ce cas, justifier de l'existence de procédures ou de dispositions particulières en faisant référence à ses documents internes qui les prévoient. Les autorités administratives compétentes instruisant les plans de sûreté de l'opérateur peuvent interroger ce dernier si cela s'avère nécessaire à leur instruction. Elles peuvent prendre

connaissance des informations que l'opérateur souhaite ne pas divulguer, sans nécessairement en disposer.

Source : France 2014.

Sur le plan opérationnel, plusieurs méthodes et solutions permettent de protéger des informations sensibles en circulation. En règle générale, elles consistent en : i) des habilitations de sécurité et des vérifications des antécédents ; ii) des systèmes de codage par couleurs ; iii) des outils électroniques. Ces trois aspects sont souvent complémentaires.

i) Habilitations de sécurité et vérifications des antécédents

Les gouvernements peuvent accorder des habilitations de sécurité aux principales parties prenantes ayant besoin d'accéder à des renseignements sensibles relatifs aux infrastructures critiques. Selon la directive 2008/114/CE du Conseil de l'Union européenne, « toute personne traitant des informations classifiées en application de la présente directive pour le compte d'un État membre ou de la Commission est soumise à une enquête de sûreté adéquate[28] ».

Les plateformes d'échange d'informations peuvent également mettre en place des critères de sélection particuliers pour l'admission de nouveaux membres, découlant, par exemple, de la nécessité d'obtenir l'accord des participants déjà inscrits, ou sous la forme d'un examen des antécédents, de passer des entretiens avec les organismes publics en charge de la plateforme.

Dans certains cas, l'acceptation de membres des forces de l'ordre peut susciter une certaine réticence parce que l'on craint que la divulgation de certains types d'information ne déclenche une action de leur part, ce qui nuirait à la volonté des participants de partager les renseignements. Il est important que les stratégies de protection des infrastructures critiques tiennent compte de ces difficultés potentielles et trouvent des moyens de les surmonter.

ii) Systèmes de codage par couleurs

Ces systèmes reposent sur le principe selon lequel quiconque fournit une information doit déterminer dans quelle mesure cette dernière peut circuler. L'application de ce principe dans le cadre du « protocole par feu de signalisation » fait que l'émetteur de l'information attribue à ladite information l'une des quatre couleurs suivantes :

- *Rouge :* la distribution de l'information n'est possible qu'à des destinataires désignés ;
- *Orange* : sa distribution est limitée, l'émetteur devant déterminer les limites et les conditions du partage de l'information ;
- *Vert* : l'information peut être diffusée au sein d'une communauté donnée, mais ne peut pas être rendue publique (par exemple sur Internet), ni être diffusée hors de la communauté en question ;
- *Blanc* : distribution sans restriction.

[28] Article 9.

L'avantage de ce protocole réside dans sa convivialité et dans le fait de poser des limites clairement définies entre les responsabilités de l'émetteur et celles di destinataire.

iii) Outils électroniques

En vue de garantir le partage sécurisé de l'information, certaines plateformes utilisent des outils électroniques, tels que les réseaux externes, pour échanger des documents. Un réseau externe est un réseau de télécommunication qui utilise la technologie Internet et dont l'objectif est de faciliter les échanges entre une entité principale et plusieurs partenaires qui sont géographiquement éloignés. Les partenaires doivent s'identifier pour être autorisés à accéder aux informations diffusées sur le réseau.

ÉTUDE DE CAS 33
Passerelle d'information canadienne sur les infrastructures essentielles

L'un des objectifs de la stratégie nationale et du plan d'action sur les infrastructures essentielles est de faire progresser en temps opportun l'échange d'informations entre les partenaires d'infrastructures critiques et d'en améliorer la protection. Pour atteindre cet objectif, cette stratégie prévoit la création d'une passerelle d'information sur les infrastructures essentielles, un portail Web de partage d'informations sur les infrastructures critiques qui sera hébergé sur le domaine de Sécurité publique Canada.

Le plan d'action sur les infrastructures essentielles pour 2014-2017 tient compte du fait que plusieurs dispositifs de partage d'informations ont été mis en place dans le cadre du plan d'action initial et vise à tirer parti de ces réalisations en offrant davantage de possibilités d'échanger des informations par divers moyens, notamment des accords officiels, des mécanismes virtuels et physiques, et la création et la diffusion de produits d'information.

Selon le plan d'action pour 2014-2017, les principaux objectifs dans ce domaine sont les suivants :

Accroître l'adhésion et la participation des intervenants à la passerelle d'information canadienne sur les infrastructures essentielles et tirer parti des capacités de la passerelle d'améliorer l'échange d'informations et la collaboration sur des projets particuliers. Sécurité publique Canada est déterminée à tirer parti du lancement réussi de la passerelle en veillant à ce que ses membres soient issus des dix secteurs et représentent les autres intervenants clefs, en encourageant leur participation active et en favorisant l'utilisation de la passerelle par les réseaux et communautés de pratique sectorielles afin qu'ils échangent des renseignements et des pratiques optimales, et qu'ils travaillent ensemble sur des projets particuliers ;

Promouvoir des habilitations de sécurité parmi les intervenants du secteur privé afin de permettre l'échange accru d'informations sensibles. Certaines informations recueillies par la communauté canadienne de la sécurité et du renseignement sont de nature délicate et ne peuvent être communiquées qu'aux personnes possédant une habilitation de sécurité adéquate. Sécurité publique Canada s'est engagée à collaborer avec les principaux ministères et organismes fédéraux afin d'accroître le nombre d'intervenants du secteur privé dotés d'une habilitation de sécurité.

Sources : Passerelle d'information sur les infrastructures essentielles, à l'adresse : https://cigateway.ps.gc.ca/_layouts/pscbranding/trms-eng.pdf ; Plan d'action sur les infrastructures

essentielles pour 2014-2017, à l'adresse : www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-fra.pdf

5. POURVOIR À LA COORDINATION ENTRE LES INSTITUTIONS NATIONALES

Résolution 2341 (2017) du Conseil de sécurité
Paragraphe 6

Le Conseil de sécurité […] : *Demande instamment à tous les États de veiller à ce que tous leurs ministères, institutions et autres entités concernés collaborent étroitement et efficacement sur les questions de protection des infrastructures critiques contre les attaques terroristes*

5.1 Nécessité d'une approche interinstitutionnelle de la protection des infrastructures critiques

Diverses institutions publiques (organes législatifs, organismes de réglementation, etc.) fixent les nombreuses normes et règles de sûreté et de sécurité applicables aux différents secteurs des infrastructures critiques. Les renseignements relatifs au terrorisme, qui sont nécessaires pour évaluer les types et les niveaux de menaces pesant aujourd'hui sur ces infrastructures, sont souvent recueillis par plusieurs institutions rendant compte à différents ministères. Une gestion des crises et des mesures d'intervention efficaces supposent que plusieurs entités publiques (aux échelons local, municipal, régional et national) puissent jouer leur rôle sans heurt ni délai. En outre, il arrive souvent que plusieurs entités aient part à une même fonction de sécurité. C'est par exemple le cas dans le secteur de l'aviation, où l'autorité compétente, la direction de l'aéroport et les forces de l'ordre peuvent être conjointement responsables de la protection des aéroports, de l'aide à la navigation aérienne et des services de navigation aérienne.

Il est donc indispensable que l'ensemble des institutions concernées coordonnent leur action pour que les infrastructures critiques soient correctement protégées. Les stratégies élaborées à cette fin doivent faire le lien entre les diverses institutions nationales chargées d'une façon ou d'une autre de la protection des infrastructures critiques. La coordination devrait devenir une réalité, et les parties prenantes telles que les ministères (des communications, de l'économie, de la sécurité, des affaires gouvernementales, de la justice, de l'intérieur et de la défense, par exemple), les instances régionales et les organismes de réglementation collaborer sur les plans stratégique, tactique et opérationnel. Atteindre cet objectif général n'est toutefois pas toujours aisé. La qualité de l'action d'ensemble menée en faveur de la protection des infrastructures critiques risque de pâtir fortement de l'emploi d'une terminologie et d'un jargon différents par les diverses entités prenant part aux activités de prévention, de protection et d'intervention, ainsi que du manque d'uniformisation des procédures et des moyens de communication. En outre, il a été observé que, dans certains cas, les pouvoirs publics avaient tendance à avoir des préoccupations divergentes s'agissant de la protection des infrastructures critiques. Certains souscrivent aux forces du marché, tandis que d'autres sont fermement convaincus que l'État a un rôle législatif à jouer. Des divergences qui peuvent faire gravement obstacle à la coopération à l'heure de mobiliser le secteur privé (OSCE 2013, p. 68).

ÉTUDE DE CAS 34
Le Groupe de travail fédéral-provincial-territorial canadien sur les infrastructures essentielles

Dans le cadre de sa stratégie nationale et de son plan d'action sur les infrastructures essentielles, le Canada a créé, outre des réseaux sectoriels et un Forum national intersectoriel, un Groupe de travail fédéral-provincial-territorial sur les infrastructures essentielles. Cette entité offre un exemple de coordination verticale entre services dans un système de gouvernement fédéral. Ses principaux objectifs sont les suivants :

- appuyer la mise en œuvre de la Stratégie dans les gouvernements fédéral, provinciaux et territoriaux ;
- offrir une orientation et participer à l'avancement et à la mise en œuvre du Plan d'action ;
- constituer un centre d'échanges des gouvernements sur les questions liées aux infrastructures essentielles à l'intention des cadres supérieurs responsables de la gestion des urgences aux échelons fédéral, provincial et territorial ;
- faciliter le réseautage fédéral-provincial-territorial en vue d'appuyer l'échange d'information, la gestion des risques, la planification en matière d'infrastructures essentielles et les exercices ;
- cibler les problèmes liés aux infrastructures essentielles qui relèvent de la compétence des régions et des administrations ;
- favoriser la compréhension mutuelle des risques et interdépendances liés aux infrastructures essentielles ;
- encourager la participation aux exercices visant à mettre à l'essai les plans de travail propres à chaque secteur et à cibler les nouveaux risques ;
- fournir une orientation quant aux défis actuels et futurs liés aux infrastructures essentielles ;
- déterminer quels liens existent entre les programmes et initiatives des gouvernements fédéral, provinciaux et territoriaux, et faciliter l'échange d'information et des pratiques exemplaires.

Toutes les provinces et tous les territoires peuvent désigner des membres pour participer au Groupe de travail, selon leurs besoins et les ressources disponibles. Aucune décision n'est prise sans que l'information n'ait été diffusée à tous et que tous les membres n'aient pu communiquer leurs commentaires. Le Groupe de travail est coprésidé par un représentant du Secteur de la gestion des mesures d'urgence et de la sécurité nationale de Sécurité publique Canada, et par un représentant d'une province ou d'un territoire désigné par consensus.

La section suivante traite des principaux éléments conceptuels et institutionnels nécessaires pour que les organismes concernés mènent une action coordonnée dans des situations de crise. Les sections ultérieures offrent un aperçu des principaux obstacles auxquels se heurte la coordination interinstitutions de manière générale ainsi que des outils essentiels pour les surmonter, notamment les formations et exercices conjoints et les solutions d'interopérabilité.

5.2 Coordination entre les institutions dans les situations de crise

Un aspect important de la coordination interinstitutions est la capacité de toutes les parties prenantes d'agir rapidement et efficacement en cas de crise. La notion de gestion des crises a été présentée à la section 2.6.2. Une fois que les structures et dispositifs principaux de gestion des crises ont été définis, les stratégies de protection des infrastructures critiques doivent garantir

qu'ils fonctionneront sans heurt en cas de besoin. La fluidité et la rapidité de la prise de décision supposent que certaines conditions élémentaires soient remplies, notamment les suivantes :

- La répartition claire des rôles et des responsabilités, et donc la prise de décision au niveau le plus bas possible tout en garantissant la coordination au niveau le plus haut requis. Selon toute vraisemblance, pour que les exploitants d'infrastructures critiques soient étroitement associés à la gestion des crises, plusieurs conditions doivent être remplies. La compréhension des rôles, responsabilités, capacités et compétences de chacun est un travail de longue haleine qui demande du temps, une coopération humaine et l'apprentissage du jargon des autres (RECIPE 2011, p 82).
- La compréhension totale des conséquences des perturbations touchant les infrastructures critiques, notamment de leurs effets en chaîne. À cet égard, il a été noté que, dans la plupart des États, la gestion des crises était principalement axée sur une perturbation unique des infrastructures critiques et sur ses conséquences potentielles (par exemple, une perturbation touchant l'alimentation en eau potable), plutôt que sur une défaillance en chaîne ou sur une défaillance de mode commun (par exemple, une forte tempête perturbant le fonctionnement de plusieurs infrastructures critiques en même temps). Il est recommandé de se préparer aux conséquences de défaillances de mode commun et de défaillances en chaîne qui toucheraient plusieurs infrastructures critiques en même temps (RECIPE 2011, p. 81).
- La désignation dans toutes les institutions concernées de responsables de la coordination disponibles à tout moment.
- La mise en place de systèmes de gestion de l'information propres à renforcer l'efficacité de la collecte, de l'analyse et de la diffusion des données à l'appui de la prise de décision par une ou plusieurs institutions, ainsi que l'information du public. Les dispositifs de communication devraient être conçus de manière à réduire au minimum le risque de recevoir des instructions contradictoires. De plus, les systèmes de gestion de l'information devraient, dans l'idéal, se doubler de lignes de communication sécurisées (voir section 4.3 sur les questions de sécurité et de protection des données dans le cadre de l'échange d'informations).

ÉTUDE DE CAS 35
La gestion de crise lors de l'attentat de Londres en 2005

Le 7 juillet 2005, quatre bombes ont explosé dans les transports londoniens, faisant cinquante-deux morts parmi les usagers. Les circonstances de l'attentat ont rendu la coordination des secours particulièrement difficile. Comme l'a souligné la coroner dans son rapport d'enquête sur les événements, trois des explosions s'étant produites dans des tunnels, les témoins oculaires étaient peu nombreux. D'autre part, les communications dans les tunnels étaient limitées. Enfin, les perturbations à grande échelle causées par les explosions ont entraîné une avalanche d'appels qui a submergé les exploitants radio et saturé toutes les communications radiophoniques et téléphoniques. Il a fallu du temps pour discerner les renseignements les plus importants et les plus significatifs et les démêler de la pléthore d'informations reçues (qui sont venues s'ajouter aux demandes habituelles traitées au quotidien par les services de secours et du métro londonien) afin que les institutions concernées puissent intervenir en conséquence.

La coroner a constaté un certain nombre d'insuffisances s'agissant de l'intervention d'urgence et formulé plusieurs recommandations. Plus précisément, d'après son rapport, les éléments de preuve ont révélé non seulement des déficiences des systèmes de communication alors en place, mais également certains malentendus entre les services de secours quant aux questions élémentaires que sont leurs rôles et opérations respectifs. Ainsi, certains secouristes n'ont pas compris que les premiers membres du service d'ambulance de Londres (London Ambulance Service) présents sur place avaient l'obligation d'intervenir en tant qu'agent-ambulancier en charge de l'incident plutôt que d'aider à soigner les victimes, ni mesuré l'importance de ce rôle. Chacun des secouristes a mis du temps et eu du mal à établir la nature des incidents et les moyens nécessaires et d'importantes différences ont été relevées dans la manière dont chacun s'est efforcé de résoudre des problèmes communs, comme par exemple l'usage des radios alors qu'il existait un risque de déclencher des dispositifs secondaires. Les éléments de preuve montrent donc qu'il convient de revoir l'étendue et le contenu des formations interinstitutions, lesquelles sont indispensables pour limiter la confusion et favoriser une meilleure connaissance des rôles respectifs des services de secours.

Dans son rapport, la coroner a notamment constaté que si l'offre en formation interinstitutions à l'intention des équipes de direction était grande (sous la forme d'exercices de simulation théorique ou en conditions réelles), les éléments indiquaient que ce n'était pas le cas pour les secouristes « de première ligne » chargés d'intervenir dans les minutes qui suivent un événement grave, dans le chaos et la confusion d'un massacre.

D'autres recommandations ont porté sur les points suivants : la formation interinstitutions relative aux incidents graves à l'intention du personnel de première ligne ; les protocoles de partage d'informations relatives aux alertes d'urgence entre la régie des transports londoniens (Transport for London) et les services de secours ; la création et la dotation en effectifs de points de rendez-vous ; les procédures de communication et de confirmation d'informations relatives à une coupure du courant de traction dans le métro londonien ; la mise à disposition de matériel de premiers secours et de civières dans les stations et les rames de métro ; les procédures de triage dans les situations où les victimes sont nombreuses ; les soins d'urgence de la nature de ceux qui sont dispensés par les services médicaux d'urgence par hélicoptère (London Air Ambulance) et les équipes d'intervention médicale urgente (Medical Emergency Response Incident Teams).

Dans son rapport, le médecin légiste a également évoqué des questions telles que la réglementation de l'approvisionnement en peroxyde d'hydrogène ; la question de la coopération réelle entre les agences ; la communication et le partage d'information ; l'utilisation des stations de radio de base dite AIRWAVE (TETRA) et leur capacité d'utilisation en cas d'incident majeur, notamment de manière transparente vis-à-vis des différents intervenants d'urgence.

Source: Enquêtes du médecin légiste sur les attentats à la bombe de Londres du 7 juillet 2005, le 6 mai 2011, à

5.3 Exercices et formations conjoints

Dans le cadre de la protection des infrastructures critiques, il est admis par tous que les exercices et formations interinstitutions sont essentiels pour atteindre au minimum les objectifs suivants :

- parvenir à une compréhension commune des procédures et méthodes applicables ;

- clarifier les rôles et responsabilités de chacun dans les cycles de protection des infrastructures critiques ;
- donner au personnel la confiance en soi nécessaire pour appliquer les instructions et règles de protection relatives aux infrastructures critiques (indispensable dans les phases de tension d'une crise réelle) ;
- recenser les insuffisances et apporter toute modification nécessaire pour qu'une situation d'urgence réelle connaisse une heureuse issue ;
- veiller à la fiabilité et à la compatibilité de tous les équipements de communication destinés à servir lors d'un incident.

ÉTUDE DE CAS 36
Cyber Europe

Dirigé par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), Cyber Europe est une série d'exercices de gestion des incidents et crises de cybersécurité à l'intention des secteurs public et privé des États membres de l'Union européenne et de l'Association européenne de libre-échange. Les exercices consistent en des simulations d'incidents de cybersécurité à grande échelle qui dégénèrent en véritables crises de cybersécurité, et offrent aux équipes chargées de la sécurité informatique, de la continuité des opérations et de la gestion des crises la possibilité d'analyser des incidents de cybersécurité d'une grande technicité et de traiter des situations complexes.

Les exercices Cyber Europe ont débuté en 2010 et sont organisés tous les deux ans. L'édition 2016 a réuni plus de 1 000 participants. La prochaine édition se tiendra en 2018.

Source : ENISA, consultable à l'adresse suivante : www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

Les formations interinstitutions peuvent être facultatives ou obligatoires, selon les circonstances. Les exercices organisés par les pays prennent différentes formes selon l'objectif recherché, le nombre d'entités et de participants concernés, les moyens disponibles et d'autres facteurs.

ÉTUDE DE CAS 37
Formation, exercices et entraînements prévus dans le Code ISPS

Le Code international pour la sûreté des navires et des installations portuaires (Code ISPS) prévoit des formations et exercices obligatoires, entre autres mesures nécessaires pour que les parties concernées comprennent mieux les tâches et les responsabilités qui leur incombent en matière de sûreté (sections 13 et 18 du Code).

Les exercices, en particulier, doivent être effectués à des intervalles appropriés. S'agissant des exercices portant sur la sûreté du navire, il doit être tenu compte « du type de navire, des changements de personnel du navire, des installations portuaires où le navire doit faire escale et d'autres conditions pertinentes » (Section 13.3.). S'agissant des exercices portant sur la sûreté de l'installation portuaire, il doit être tenu compte « des types d'opérations effectuées par l'installation portuaire, des changements dans la composition du personnel de l'installation portuaire, du type de navires que dessert l'installation portuaire et autres circonstances pertinentes » (Section 18.3).

Dans tous les cas, il doit être tenu compte, pour les exercices et entraînements, des recommandations énoncées dans la partie B du Code ISPS.

L'Institut ukrainien d'études stratégiques a dressé un inventaire des types d'exercices les plus courants et de leurs principaux emplois (Ukraine 2017, p. 110). On peut notamment citer les exercices ci-après :

- *Les séminaires* : il s'agit de donner des orientations générales sur les stratégies, les plans, les politiques, les procédures et les protocoles déjà en place, les moyens disponibles et les notions.
- *Les exercices de simulation théorique* : il s'agit d'ouvrir un débat sur une situation d'urgence hypothétique. Ces exercices sont utiles pour faciliter la compréhension des notions, recenser les points forts et les points à améliorer et faire évoluer les idées.
- *Les simulations (jeux)* : il s'agit d'étudier les conséquences des décisions prises par les joueurs et de leurs actions. Ce type d'exercice prend souvent la forme d'une compétition entre deux équipes ou plus qui s'affrontent dans des situations de la vie réelle.
- *Les exercices d'entraînement* : il s'agit de former le personnel à de nouveaux équipements, de valider des procédures ou des pratiques et d'entretenir les capacités existantes. L'idée est d'enseigner ou de perfectionner des compétences par la répétition des tâches.
- *Les exercices à grand déploiement (conditions réelles)* : il s'agit de présenter aux participants des scénarios qui reproduisent des situations réelles et de leur demander d'agir et de réagir en temps réel.

Il est important de noter que certains des exercices cités ci-dessous, en particulier ceux qui supposent la participation d'un grand nombre de personnes et reposent sur des simulations de situations réelles complexes, exigent une planification minutieuse et souvent des mois, voire des années, de préparation.

ÉTUDE DE CAS 38
Ukraine : « Coherent resilience 2017 »

Organisé par l'OTAN, « Coherent resilience 2017 » est un exercice de simulation théorique visant à renforcer la résilience des infrastructures énergétiques critiques en Ukraine. Il s'agissait notamment de :

- Vérifier les procédures de prévention, de protection et d'intervention relatives aux incidents liés au secteur de l'énergie ;
- Faciliter la coopération entre départements s'agissant du renforcement de la résilience du système électrique national, notamment l'action internationale visant à trouver une solution aux nouveaux problèmes qui se posent en matière de sécurité.
- L'exercice a réuni vingt entités étatiques, soit plus de cent participants qui ont pris part à sa planification et à son exécution, dans quatre filières : cybersécurité et terrorisme, gestion des crises, communications stratégiques et intervention internationale. Parmi les participants figuraient, entre autres, des agents des institutions étatiques et ministères compétents dans le domaine de l'énergie, des services de secours et des services de sécurité nationale ainsi que des militaires, des policiers et d'autres institutions et organismes chargés de protéger le secteur critique de l'énergie électrique et de renforcer sa résilience.

Les différents scénarios étaient conçus de façon à encourager les participants à :

- Analyser les faiblesses des infrastructures énergétiques critiques en s'appuyant sur des risques et des menaces définis ;
- Établir les conséquences d'une défaillance des infrastructures énergétiques critiques, d'un attentat contre celles-ci ou de dégâts qui leur seraient causés et les répercussions de tels incidents sur des aspects connexes de la société ;
- Évaluer la coopération et la coordination entre les institutions, les organismes et les organisations dont dépendent les services d'urgence et examiner les plans qu'ils ont mis en place ;
- Mettre à l'essai les mécanismes de gestion des crises, notamment la planification des interventions d'urgence civiles et militaires en réponse à des situations causées par des moyens mixtes avant, pendant et après un conflit.

Source : Ukraine 2017.

5.4 Promotion de procédures et de solutions interopérables

L'interopérabilité est une notion essentielle à la coordination interinstitutions. Elle peut être soit opérationnelle et fonctionnelle, soit technique, deux aspects qui sont définis dans la Stratégie de résilience aux incidents chimiques, biologiques, radiologiques, nucléaires et à l'explosif pour le Canada comme suit :

1) « L'interopérabilité opérationnelle et fonctionnelle est l'aptitude à travailler efficacement de concert. Précisément, c'est l'aptitude de différentes administrations ou disciplines à fournir des services à d'autres administrations ou à d'autres disciplines de façon coordonnée, ou à en recevoir, et à les utiliser pour fonctionner plus efficacement de concert en cas d'urgence. D'un point de vue pratique, l'interopérabilité opérationnelle signifie que le personnel de différentes administrations ou différents services fonctionne comme une équipe au sein d'une structure de commandement et de contrôle commune. »

2) « L'interopérabilité technique est l'aptitude à communiquer et à échanger de l'information ainsi qu'à intégrer de l'équipement et des capacités techniques. C'est l'aptitude des systèmes à fournir de l'information interactive dynamique et à échanger des données entre les éléments de

commandement, de contrôle et de communications afin de planifier, de coordonner, d'intégrer et d'exécuter les opérations d'intervention. » (Canada 2005).

Dans le cadre de la coordination interinstitutions, il semble tout particulièrement important de pouvoir s'appuyer sur des procédures interopérables s'agissant des transmissions lors des interventions d'urgence. À cet égard, le constat suivant a été établi : si cette question est un sujet de préoccupation depuis presque aussi longtemps que les secouristes et autres agents de la sécurité publique communiquent au moyen de radios, ce n'est qu'après l'attaque terroriste commise le 11 septembre 2001 contre le World Trade Center qu'elle a cessé d'être une préoccupation de longue date pour devenir une priorité nationale. L'une des plus grandes tragédies de la catastrophe qui s'est produite ce jour-là est à déplorer parce qu'il a été impossible d'avertir efficacement les équipes de lutte contre les incendies que les tours étaient sur le point de s'effondrer et qu'il fallait évacuer immédiatement les lieux. De nombreux experts s'accordent à dire que le décès de 343 pompiers est en premier chef imputable à cette défaillance de leur système radio, qui ne leur a pas permis de bien communiquer avec les autres organismes ou ne serait-ce qu'entre eux selon qu'ils étaient équipés de modèles de radio plus ou moins récents (Federal Signal 2013).

L'utilisation de systèmes interopérables est essentielle, non seulement pour permettre aux policiers et aux autres intervenants (pompiers, secouristes, ambulanciers, etc.) de communiquer entre eux pour coordonner leur action, mais aussi pour les aider à rationaliser les ressources dans le cadre de la budgétisation et de la planification des activités de secours en cas de catastrophe et de reprise après sinistre.

5.5 Surmonter les obstacles culturels

Bien que l'adoption de solutions interopérables et de procédures rationalisées ou uniformisées puisse contribuer dans une large mesure à briser les cloisonnements et à favoriser la coordination interinstitutions, il n'en reste pas moins que la protection des infrastructures critiques dépend des opérations quotidiennes de personnes ayant des compétences techniques et des expériences professionnelles très diverses. Les différences de mentalité peuvent s'ancrer dans des différences de terminologie, de méthode et d'organisation du travail.

Dans quelle mesure les différences culturelles entre les acteurs de la protection des infrastructures critiques peuvent-elles faire obstacle à une collaboration optimale ? Cette question a fait l'objet d'une attention particulière en Suède, pays dont la démarche s'agissant de la résilience des infrastructures critiques et, plus généralement, de la sécurité de tous, consiste à mobiliser l'ensemble de la société. Ainsi, une étude consacrée à la résilience face aux catastrophes a permis d'étudier isolément un certain nombre de relations professionnelles prenant place dans le cadre de la protection des infrastructures critiques et d'analyser les problèmes culturels associés à chacune d'elles. Cette étude a révélé, par exemple, qu'il existait des différences entre les professionnels de la sûreté et ceux de la sécurité dans la manière de traiter les informations. Si les professionnels de la sécurité sont habitués à traiter des informations classifiées dans des cercles restreints, le personnel chargé de la sûreté a tendance à se fier à des sources publiques et à ne pas voir l'intérêt des informations confidentielles. Toutefois, à l'heure où les menaces deviennent plus

complexes et où il peut être difficile, dans un premier temps, d'établir si un événement relève d'un accident d'apparence normale ou d'une attaque terroriste, une coopération solide entre les forces de police et les secouristes, par exemple, doit être instaurée bien en amont (Lindberg & Sundelius 2013, p. 1301).

Si certaines différences de comportement correspondent à la fracture qui existe entre militaires et civils, l'étude révèle des obstacles plus prononcés dans le cadre de la coordination entre civils, ce qui s'explique principalement par le fait que les rôles et responsabilités dans la sphère complexe que représente le domaine civil sont souvent établis moins clairement, quand ils ne se chevauchent pas. Au fur et à mesure de l'évolution des menaces, des règles et des procédures peuvent faire défaut ou devenir obsolètes. Les domaines de compétence peuvent se compléter ou se concurrencer, selon les points de vue. Une certaine résistance peut parfois se faire sentir face aux initiatives de coordination, ce qui peut s'expliquer en partie par le fait que les interactions visant à modifier les comportements peuvent se révéler extrêmement délicates chez des professionnels fiers de leur travail (Lindberg & Sundelius 2013, p. 1300 et1301).

Dans les autres pays, les expériences et les perceptions peuvent varier considérablement selon les structures institutionnelles, sociales et économiques dans lesquelles s'inscrivent les différentes professions. Sans nécessairement chercher à uniformiser des comportements profondément ancrés, chaque pays souhaitera peut-être faire mieux connaître ces problèmes et y trouver des solutions (en en discutant ouvertement et régulièrement dans le cadre des formations conjointes, par exemple) pour veiller à ce qu'ils ne viennent pas compromettre l'action de longue haleine qui, moyennant beaucoup de temps et de ressources, continue d'être menée pour parvenir à la résilience des infrastructures critiques.

6. RENFORCER LA COOPERATION INTERNATIONALE POUR PROTEGER LES INFRASTRUCTURES CRITIQUES

Résolution 2341 (2017) du Conseil de sécurité
Paragraphes 8 et 9

Le Conseil de sécurité […]

Affirme que la coopération économique et les initiatives de développement aux niveaux régional et bilatéral contribuent de manière essentielle à assurer la stabilité et la prospérité régionales et, à cet égard, demande à tous les États d'envisager de renforcer leur coopération afin de protéger les infrastructures critiques, notamment les projets de connectivité régionale et les infrastructures transfrontières connexes, contre les attaques terroristes, selon qu'il conviendra, par des moyens bilatéraux et multilatéraux, de mise en commun des informations, d'évaluation des risques et de maintien de l'ordre ;
Demande instamment aux États qui sont en mesure de le faire de contribuer de façon efficace et ciblée au renforcement des capacités, à la formation et à la fourniture d'autres ressources, à des services d'assistance technique, à des transferts de technologie et aux programmes nécessaires afin que tous les États puissent atteindre l'objectif de protection des infrastructures critiques contre les attaques terroristes ;

6.1 Les dimensions de la coopération internationale en matière de protection des infrastructures critiques

L'une des manifestations les plus visibles de la mondialisation est l'internationalisation des chaînes d'approvisionnement, que ce soit pour la fourniture de produits et de services essentiels ou non essentiels. En conséquence, les interdépendances et les interconnexions des infrastructures critiques dépassent les frontières. Les risques qui pèsent sur les infrastructures critiques des pays peuvent provenir de pays voisins (en particulier dans le cas d'infrastructures physiques partagées) ou très éloignés (notamment en cas de cyberattaques). En cas de crise informatique, il peut même arriver qu'une situation d'urgence se produisant dans un pays ne puisse être traitée que dans un autre pays, sans que celui-ci soit directement touché.

Les scénarios possibles illustrant la nécessité d'intégrer fermement la coopération internationale dans les stratégies de protection des infrastructures critiques des pays comprennent notamment les situations suivantes :

- Deux pays ou plus partagent la même infrastructure (infrastructures critiques transfrontières) ;
- Une infrastructure critique située dans un pays dépend, en totalité ou en partie, de produits, de services, de technologies, etc. fournis par un autre pays ;
- Les perturbations ou les anomalies liées au fonctionnement d'une infrastructure critique située dans un pays produisent des effets dans d'autres pays.

Les niveaux actuels de coopération internationale en matière de protection des infrastructures critiques varient considérablement en fonction des besoins et des perceptions des pays. La coopération peut être plus ou moins étendue selon les types d'accords en place, la proximité des pays et le niveau d'intégration économique.

Lorsqu'ils envisagent de créer ou de renforcer des partenariats transfrontières dans le domaine de la protection des infrastructures critiques, les pays devraient prendre en compte plusieurs éléments. Comme en témoignent les études de cas présentées dans les sections suivantes, les efforts de coopération internationale sont généralement axés sur la mise en commun des informations, la gestion des crises et les activités conjointes. Les aspects quelque peu oubliés sont le maintien de l'ordre et la coopération judiciaire en matière pénale à l'échelle internationale. Ces formes de coopération internationale ne servent peut-être pas exclusivement les objectifs relatifs à la protection des infrastructures critiques, mais elles jouent un rôle essentiel dans l'action que mènent les États en cas d'attentats terroristes perpétrés contre des infrastructures critiques. Dans la mesure où la résolution 2341(2017) du Conseil de sécurité exige l'établissement des responsabilités pénales, l'application effective de sanctions est indissociable de la nécessité pour les pays de s'appuyer sur des canaux efficaces de coopération internationale dans le domaine de la justice pénale.

Dans ce contexte, le système I-24/7 d'INTERPOL offre une plateforme mondiale permettant aux forces de l'ordre de communiquer. Ce système relie les fonctionnaires chargés de l'application de la loi des 192 pays membres d'INTERPOL et permet aux utilisateurs autorisés de partager en toute sécurité des informations de police sensibles et urgentes avec leurs homologues dans le monde entier, 24 heures sur 24 et 365 jours par an. I-24/7 est le réseau qui donne accès aux différentes bases de données criminelles d'INTERPOL. Les utilisateurs autorisés peuvent faire des recherches et des recoupements en quelques secondes en accédant directement aux bases de données contenant des informations sur les criminels présumés ou les personnes recherchées, les documents de voyage perdus ou volés, les véhicules automobiles volés, les empreintes digitales, les profils génétiques, les documents administratifs volés et les œuvres d'art volées. Le réseau I-24/7 ayant été installé dans tous les Bureaux centraux nationaux, INTERPOL s'emploie actuellement à en élargir accès au-delà de ces bureaux, afin de permettre à des agents travaillant en première ligne, tels que les agents de l'immigration et les douaniers, d'en bénéficier.

Étude de cas 39
Échange international d'informations sur les menaces dans le domaine de l'aviation civile

Dans le secteur de l'aviation, l'échange de renseignements sur les menaces constitue une dimension importante de la mise en commun des informations.
Le Manuel de sûreté de l'OACI (Doc 8973 – Diffusion restreinte) recommande l'établissement de lignes de communication, tant officielles qu'informelles, entre les responsables de la sûreté aérienne des États, afin de faciliter l'échange rapide d'informations, y compris concernant toute augmentation du niveau de menace. Le partage d'informations sur les techniques utilisées pour tenter de porter atteinte à la sécurité, l'expérience acquise dans l'utilisation du matériel de sécurité et les pratiques opérationnelles présentent également un intérêt considérable.

Des procédures officielles régissant l'échange d'informations entre les responsables désignés, ainsi qu'une liste de numéros de téléphone, d'adresses postales, de numéros de télex et de télécopie, d'adresses électroniques et d'adresses du service fixe aéronautique, devraient être disponibles pour faciliter la communication lorsque survient un fait grave. Les États devraient élaborer des procédures relatives à l'analyse et à la diffusion d'informations sur les menaces et veiller à ce que les exploitants des aéronefs et des aéroports prennent les mesures voulues pour contrer les menaces identifiées. Il conviendrait de diffuser les informations au moment où les personnes concernées en ont besoin pour s'acquitter efficacement de leurs fonctions, conformément au principe du besoin d'en connaître.

Les États disposant de ressources limitées pour faire face à des menaces imminentes ou à des actes d'intervention illicite devraient envisager de négocier une aide juridique et procédurale avec les États voisins qui sont mieux équipés pour recueillir et diffuser des informations sur les menaces et les incidents.

Il convient de satisfaire, chaque fois que nécessaire, les demandes d'un État concernant la mise en place de mesures de sûreté spéciales pour un vol donné. Pour veiller à ce que ces demandes reçoivent l'attention voulue, les États devraient recenser les procédures applicables et dresser la liste des représentants des pouvoirs publics, des exploitants d'aéronefs et des exploitants aéroportuaires qui devraient être informés des menaces. En outre, les paramètres des mesures spéciales de sûreté, la responsabilité des coûts supplémentaires et les délais d'intervention devraient être négociés avec les exploitants d'aéronefs ou les aéroports concernés.

Les communications urgentes peuvent être facilitées par le Réseau de points de contact en sûreté de l'aviation, créé par l'OACI pour la communication de menaces imminentes dirigées contre les opérations d'aviation civile, en application des vues exprimées par le Groupe Lyon-Rome contre la criminalité et le terrorisme du G8. Conformément à la résolution A39-18 de l'Assemblée intitulée « Exposé récapitulatif de la politique de l'OACI relative à la sûreté de l'aviation », les États qui ne l'ont pas déjà fait sont instamment priés de participer au réseau OACI de points de contact en sûreté de l'aviation. L'objectif de ce réseau est de fournir des informations sur les points de contact internationaux en sûreté de l'aviation au sein de chaque État, qui sont désignés comme l'autorité compétente pour envoyer et recevoir à n'importe quel moment des communications au sujet de menaces imminentes, des demandes urgentes en matière de sûreté ou des directives à l'appui des dispositions de sûreté, afin de contrer une menace imminente. Les points de contact devraient être disponibles à tout moment, participer au processus d'évaluation de la menace et être proches des instances qui prennent des décisions concernant les procédures de sûreté aérienne.

Source : OACI, Manuel de sûreté, Doc 8973 – Diffusion restreinte.

6.2 Grandes initiatives transfrontières

Au cours des dernières années, on a mieux pris conscience du fait que les interdépendances des infrastructures critiques ne s'arrêtaient pas aux frontières nationales, ce qui a facilité la conclusion de plusieurs accords et partenariats internationaux. Compte tenu du poids économique des pays concernés et de la grande complexité des réseaux d'infrastructures qui les relient, la présente section est consacrée au cadre de l'Union européenne et aux accords de coopération mis en place entre le Canada et les États-Unis.

6.2.1 Union européenne

L'action menée pour faire en sorte que les 27 États membres de l'Union européenne élaborent une stratégie globale en matière de protection des infrastructures critiques a commencé en 2005. À la demande du Conseil européen, la Commission a adopté un livre vert contenant des propositions pour l'établissement d'un programme de protection des infrastructures critiques. Les réactions reçues ont mis en évidence la valeur ajoutée d'un cadre communautaire dans ce domaine. En avril 2007, le Conseil a déclaré que c'était aux États membres qu'incombait en dernier ressort la gestion des dispositifs de protection des infrastructures critiques sur leur territoire national. Dans le même temps, il s'est félicité des efforts déployés par la Commission en vue d'élaborer une procédure à l'échelle européenne aux fins du recensement et du classement des infrastructures critiques européennes. L'approche actuelle de l'Union européenne est consacrée dans une directive de 2008 aux termes de laquelle une infrastructure critique européenne est « une infrastructure critique située dans les États membres dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins. L'importance de cet impact est évaluée en termes de critères intersectoriels. Cela inclut les effets résultant des dépendances intersectorielles par rapport à d'autres types d'infrastructures » (art. 2.b).

De manière déterminante, cette directive se concentre sur le secteur de l'énergie et sur celui des transports. En outre, elle vise à compléter, et non à remplacer, les mesures sectorielles existant au niveau communautaire et dans les États membres. Dans les cas où des mécanismes communautaires sont déjà en place, ils devraient continuer à être utilisés et ainsi à contribuer à la mise en œuvre globale de la directive.

Le processus de désignation des infrastructures critiques européennes suit plusieurs étapes, qui imposent les obligations suivantes à chaque État membre :

- Informer les autres États membres de la présence sur son territoire d'une infrastructure critique européenne potentielle susceptible de les affecter, et engager avec eux des discussions bilatérales ou multilatérales ;
- Désigner cette infrastructure en tant qu'infrastructure critique européenne après accord avec les États membres concernés ;
- Informer chaque année la Commission du nombre d'infrastructures critiques européennes désignées comme telles par secteur et du nombre d'États membres concernés par chacune d'entre elles ;
- Informer le propriétaire/opérateur de l'infrastructure de la désignation de celle-ci comme infrastructure critique européenne ;
- Veiller à ce que les infrastructures classées comme infrastructures critiques européennes soient dotées d'un plan de sécurité d'opérateur et à ce que ce plan soit régulièrement réexaminé ;
- Veiller à ce que chaque infrastructure critique européenne soit dotée d'un correspondant pour la sécurité qui exerce la fonction de point de contact entre le propriétaire/opérateur de l'infrastructure et l'autorité compétente de l'État membre ;
- Réaliser une évaluation de la menace pesant sur les sous-secteurs d'infrastructures critiques européennes dans un délai d'un an à compter de la désignation d'une

infrastructure critique située sur son territoire comme infrastructure critique européenne au sein de ces sous-secteurs ;
- Présenter à la Commission, tous les deux ans, des données génériques synthétisées sur les types de risques, menaces et vulnérabilités rencontrés dans chacun des secteurs d'infrastructures critiques européennes comptant une infrastructure critique européenne désignée comme telle ;
- Désigner un point de contact pour la protection des infrastructures critiques européennes chargé de coordonner les questions liées à la protection des infrastructures critiques européennes tant au niveau national qu'avec les autres États membres et la Commission.

En 2013, une évaluation de l'état de l'application de la directive de 2008 a révélé une situation mitigée. Bien que l'établissement d'un cadre de protection des infrastructures critiques à l'échelle de l'Union européenne ait été clairement reconnu comme une priorité, un certain nombre de difficultés ont été mises en lumière. En particulier, il a été observé que moins de 20 infrastructures critiques européennes avaient été désignées et qu'en conséquence, très peu de nouveaux plans de sécurité d'opérateur avaient été élaborés. Certaines infrastructures critiques ayant clairement une dimension européenne, telles que les principaux réseaux de transport d'énergie, ne sont pas prises en compte. Bien qu'elle ait contribué à favoriser la coopération européenne dans le domaine de la protection des infrastructures critiques, la directive a principalement encouragé les échanges bilatéraux entre les États membres plutôt que la mise en place d'un cadre européen de coopération. L'approche par secteur de la directive représente également un défi pour plusieurs États membres, car dans la pratique, l'analyse de criticité n'est pas limitée par des frontières sectorielles et répond plutôt à une approche par système ou par service (hôpitaux ou services financiers, par exemple) (Commission européenne, 2013 bis).

En 2013, la Commission européenne a donc proposé d'orienter l'action menée en faveur de la protection des infrastructures critiques dans une nouvelle direction, plus pragmatique, qui consisterait essentiellement à passer d'une approche sectorielle à une approche systémique. Cette nouvelle approche commence par l'exécution un projet pilote visant à évaluer les risques et les vulnérabilités de quatre infrastructures critiques européennes et les mesures mises en œuvre pour protéger ces infrastructures critiques, à savoir : 1) le réseau de transport d'électricité de l'Union européenne ; 2) le réseau de transport de gaz de l'Union européenne ; 3) EUROCONTROL ; et 4) GALILEO (programme européen de navigation mondiale par satellite).

La Commission européenne espère que la phase pilote fournira les indicateurs nécessaires pour faciliter l'élaboration d'un cadre de protection des infrastructures critiques à l'échelle de l'Union européenne. Ce cadre serait fondé sur les résultats obtenus et les lacunes recensées lors de l'évaluation des quatre infrastructures critiques européennes et viserait à fournir des outils utiles pour améliorer la protection et la résilience, notamment par la mise en place de mesures renforcées d'atténuation des risques, de préparation et d'intervention (...). L'étape suivante pourrait consister à mettre en œuvre cette approche dans les régions où les États membres souhaitent coopérer les uns avec les autres. Par exemple, on pourrait mettre en place un dispositif de résilience pour l'ensemble des infrastructures de transport critiques situées autour de la mer Baltique et un programme sur les criticités de la chaîne d'approvisionnement dans la région du Danube (Commission européenne, 2013 bis).

Étude de cas 40
AIRPOL et RAILPOL

La collaboration transfrontière en matière de protection des infrastructures critiques dans les pays européens ne se limite pas au cadre fixé par la directive de 2008. Elle se développe également dans des instances qui, bien que n'étant pas exclusivement consacrées à la protection des infrastructures critiques, jouent un rôle très important dans la réalisation de cet objectif. Dans le secteur des transports, les activités mises en œuvre dans le cadre d'AIRPOL et de RAILPOL offrent deux exemples pertinents.

Créé en 2011, AIRPOL est un organe de coordination des services répressifs actifs dans les aéroports européens. Sa mission est de renforcer la sécurité globale dans le domaine de l'aviation civile par les moyens suivants :

- Assurer un traitement efficace et efficient des questions de maintien de l'ordre et de protection des frontières concernant les aéroports et l'aviation ;
- Contribuer à une harmonisation plus poussée de l'application des mesures dans ce domaine.

Les travaux d'AIRPOL s'articulent autour de trois types d'activités :

- Établissement d'un réseau permanent et opérationnel, axé sur la mise en commun de pratiques optimales, de renseignements et d'informations de portée générale, visant à permettre de futurs échanges de personnel dans plusieurs domaines ;
- Coordination d'actions transfrontières à fort impact ;
- Réalisation de missions consultatives en tant qu'organe représentatif constitué de spécialistes.

RAILPOL est un réseau international regroupant les organisations de police ferroviaire des États membres de l'Union européenne. Son objectif est de renforcer et d'intensifier la coopération internationale entre services de police ferroviaire en Europe, de prévenir les menaces et de garantir l'efficacité des mesures de lutte contre la criminalité transfrontière. RAILPOL est composé de représentants des organisations responsables des missions de police ferroviaire dans les États membres de l'Union européenne.

6.2.2 Coopération entre le Canada et les États-Unis

Non seulement la frontière canado-américaine est la plus longue du monde, mais plus de 90 % de la population canadienne vit dans un rayon de 160 km de cette frontière. En outre, plusieurs raffineries, centrales nucléaires, grandes usines et autres infrastructures critiques sont situées près de la frontière. L'une des conséquences majeures est l'existence de fortes dépendances et d'un grand nombre d'infrastructures transfrontières dont la protection dépend largement des initiatives de coopération bilatérale.

Le principal outil de coopération transfrontière en matière de protection des infrastructures critiques est le Plan d'action Canada-États-Unis de 2010. Bien que le Plan s'appuie sur les accords de coopération sectorielle en vigueur entre les deux pays, l'adoption d'une approche intégrée a été encouragée afin de répondre aux principales nécessités suivantes :

- Renforcer la collaboration avec le secteur privé de part et d'autre de la frontière ;

- Prévenir les doubles emplois qui sont inévitables lorsque l'on suit des approches exclusivement sectorielles ;
- Améliorer la rapidité et la précision des communications avec les intervenants du secteur des infrastructures critiques, aussi bien au niveau national qu'au niveau transfrontière.

Le Plan d'action Canada-États-Unis s'articule autour de trois objectifs : i) établissement de partenariats visant à renforcer la résilience des infrastructures critiques ; ii) échange d'informations ; et iii) gestion des risques.

i) Établissement de partenariats visant à renforcer la résilience des infrastructures critiques

La méthode employée pour atteindre cet objectif consiste à exploiter les structures organisationnelles et les structures de partenariat existantes. L'une de ces structures est le Groupe consultatif sur la gestion des urgences (GCGU), qui a été établi dans le cadre de l'Accord de coopération Canada-Etats-Unis en matière de gestion des urgences (2008) pour assurer une surveillance centrale à l'appui des activités communes de gestion des urgences. L'un des groupes de travail créé dans le cadre du GCGU s'occupe spécialement des infrastructures critiques et a été chargé de fournir des directives et une continuité à l'appui du Plan d'action Canada-Etats-Unis.

Au titre de cet objectif, le Plan d'action prévoit également de fournir des mécanismes et des occasions aux conseils de coordination du gouvernement et des secteurs des États-Unis et aux réseaux sectoriels canadiens afin qu'ils travaillent ensemble en vue d'améliorer la collaboration transfrontalière propre aux secteurs. De plus, une unité d'analyse des risques pour les infrastructures essentielles du Canada et des États-Unis a été mise en place dans le cadre du Plan d'action afin d'élaborer et de réaliser des produits analytiques de collaboration pouvant s'appliquer au-delà des frontières.

ii) Partage de l'information

Au titre de cet objectif, les deux pays se sont notamment engagés à travailler ensemble pour :

- Concevoir des mécanismes et des protocoles compatibles en vue de protéger et de communiquer les renseignements sensibles sur les infrastructures critiques ;
- Déterminer les besoins en matière d'information des secteurs privé et public à l'appui de l'élaboration de produits analytiques utiles ;
- Assurer un échange d'informations efficace pendant et après la survenue de faits ayant une incidence sur des infrastructures critiques.

iii) Gestion des risques

Au titre de cet objectif, les deux pays s'engagent à travailler ensemble afin d'évaluer les risques et d'élaborer des plans pour les secteurs prioritaires. Des sous-activités seront déterminées après un examen approfondi des priorités axées sur le risque de chaque pays et la définition des secteurs d'intérêt mutuel.

6.2.3 **INTERPOL**

En mars 2016, INTERPOL a rédigé une note de renseignement sur la menace croissante que les systèmes de drones font peser sur les infrastructures critiques et sur d'autres sites sensibles, qui a été adressée à tous ses pays membres. La note concluait que les systèmes de drones devenant plus populaires, moins chers et plus faciles à acquérir et à utiliser, ce n'était qu'une question de temps avant qu'ils ne soient employés plus largement à des fins néfastes. Elle indiquait également que les entités de répression du monde entier n'étaient pas équipées pour faire face à la menace posée par les systèmes de drones. En effet, selon certaines sources, l'État islamique d'Iraq et du Levant a utilisé des drones comme dispositifs de dispersion d'engins explosifs et à des fins de surveillance en Iraq et en Syrie. Il est recommandé dans la note que les services de répression envisagent, s'ils ne le faisaient pas déjà, d'utiliser les systèmes de drones comme multiplicateurs de force, non seulement pour combattre les drones utilisés à des fins néfastes, mais aussi pour faciliter les enquêtes, en particulier celles concernant les attentats à la bombe, la gestion des risques liés aux substances chimiques, bactériologiques, radiologiques, nucléaires et explosives et aux matières dangereuses, le maintien de l'ordre, la gestion des situations d'urgence, les secours en cas de catastrophe et d'autres activités quotidiennes de police.

En parallèle, il convient de souligner qu'INTERPOL assure la présidence du groupe de travail de l'Équipe spéciale de lutte contre le terrorisme sur la protection des infrastructures critiques y compris les cibles vulnérables, Internet et la sécurité du tourisme. Dans ce cadre, plusieurs entités internationales et pays membres ont souligné que l'utilisation de drones par des terroristes et des criminels représentait une menace croissante et qu'ils ne disposaient pas des capacités opérationnelles ou du cadre juridique appropriés pour y faire face.

En réponse, en octobre 2017, le Centre d'innovation et la Direction de la lutte contre le terrorisme d'INTERPOL ont organisé la première réunion du Groupe de travail sur le cadre d'enquête et d'analyse scientifique relatif aux drones, qui a réuni 42 participants venus de 20 pays. Les participants étaient principalement issus des forces de l'ordre, et 16 % d'entre eux venaient du secteur privé et du milieu universitaire. Le Groupe de travail a permis d'échanger des informations sur les questions d'actualité et les nouvelles tendances liées à l'utilisation des drones, notamment la menace des drones dans les prisons, l'emploi des drones à des fins terroristes, les mesures de lutte contre les drones, les outils de police scientifique, la criminalistique appliquée aux drones, etc.

INTERPOL a l'avantage de pouvoir offrir une plateforme de coopération policière neutre à l'échelle mondiale, réunissant des spécialistes, des représentants des gouvernements, des professionnels et des représentants du milieu universitaire et du secteur privé, afin d'aider les pays membres à lutter contre cette nouvelle menace. En outre, ce programme constituera l'initiative phare d'INTERPOL et sa contribution à la communauté internationale dans le cadre de sa présidence du groupe de travail de l'Équipe spéciale de lutte contre le terrorisme sur la protection des infrastructures critiques.

Le Programme devrait être lancé par le Complexe mondial INTERPOL pour l'innovation, basé à Singapour, et mis en œuvre en étroite collaboration avec le Centre d'innovation, sous la supervision de la Direction de la lutte contre le terrorisme et de la Sous-direction des substances chimiques,

bactériologiques, radiologiques, nucléaires et explosives et des cibles vulnérables. En outre, il marquera l'aboutissement des efforts ponctuels menés jusqu'ici par le Centre d'innovation et permettra de répondre aux prérogatives relatives à la mission et au mandat de la Direction de la lutte contre le terrorisme concernant la protection des infrastructures critiques (voir Stratégie de lutte antiterroriste mondiale d'INTERPOL, axe d'action 4.6 : « Renforcer les moyens dont disposent les pays membres pour protéger leurs infrastructures critiques et leurs cibles vulnérables contre les attaques terroristes, qu'il s'agisse d'attentats physiques ou de cyberattaques ».

6.2.4 Autres initiatives

Ces dernières années, un nombre croissant d'initiatives ont été lancées pour prendre en compte la dimension transfrontière de la protection des infrastructures critiques, tant au niveau sous-régional qu'interrégional.

À titre d'exemple d'initiative sous-régionale, on peut citer le programme Nordic emergency management cooperation (coopération nordique en matière de gestion des urgences). En 2009, la coopération a été renforcée dans le cadre de cette plateforme opérationnelle, à laquelle participent le Danemark, la Finlande, l'Islande, la Norvège et la Suède. L'initiative est structurée autour de plusieurs groupes de travail, qui sont tenus de faire rapport chaque année aux ministères compétents. En 2011, un nouveau groupe de travail a été créé pour examiner les vulnérabilités et les perspectives de mise en commun des capacités opérationnelles dans le domaine cybernétique. Les domaines de coopération concernent notamment les services de sauvetage, les exercices de simulation et l'éducation, la préparation face aux menaces de nature chimique, biologique, radiologique ou nucléaire, les portails de crise, le recrutement de volontaires, la recherche-développement, la prévention tactique des incendies, le transport aérien stratégique en cas de catastrophe, le transport aérien stratégique et le soutien fourni par le pays hôte.

Au niveau interrégional, la question de la protection des infrastructures critiques a fait l'objet de réunions annuelles de spécialistes entre l'Union européenne et les États-Unis, et entre l'Union européenne et le Canada. Comme indiqué dans le document de travail de la Commission de 2013, ces réunions ont principalement porté sur la nécessité de renforcer la coopération en partageant les connaissances, les meilleures pratiques et les informations concernant la protection des infrastructures critiques, ainsi que sur l'élaboration d'une trousse à outils mondiale pour la sécurité des infrastructures. Les prochaines réunions seront axées sur certains thèmes considérés comme ayant une importance croissante pour la protection des infrastructures critiques à l'échelle internationale, à savoir : les interdépendances extérieures, l'interconnexion des infrastructures critiques, les effets en cascade potentiels à l'échelle mondiale et l'interdépendance des infrastructures physiques et des cyberinfrastructures (Commission européenne, 2013 *bis*, p. 6).

6.3 Assistance technique et financière transfrontière

Non seulement la protection des infrastructures critiques nécessite des ressources pour la mise en œuvre de ses différentes phases et dimensions, mais elle exige également des niveaux élevés d'expertise dans plusieurs domaines. La protection des infrastructures critiques a beau être une priorité partagée par tous les pays, les ressources et les compétences multidisciplinaires

nécessaires ne sont pas facilement accessibles dans tous les pays. C'est pourquoi, dans sa résolution 2341 (2017), le Conseil de sécurité a demandé instamment aux États qui étaient en mesure de le faire « de contribuer de façon efficace et ciblée au renforcement des capacités, à la formation et à la fourniture d'autres ressources, à des services d'assistance technique, à des transferts de technologie et aux programmes nécessaires afin que tous les États puissent atteindre l'objectif de protection des infrastructures critiques contre les attaques terroristes ».

Dans cet esprit, dans le domaine de l'aviation civile, l'OACI engage les États disposant de ressources limitées pour faire face aux menaces imminentes à envisager de négocier une aide juridique et procédurale avec les États voisins qui sont mieux équipés pour recueillir et diffuser des informations sur les menaces et les incidents[29].

L'Union européenne fournit un cadre juridique sur l'aide technique et financière transfrontière apportée aux pays tiers dans le domaine de la gestion des crises[30]. Les objectifs visés sont les suivants :

- Dans une situation de crise ou de crise émergente, contribuer rapidement à la stabilité en prévoyant une réaction efficace conçue pour aider à préserver, établir ou restaurer les conditions essentielles pour permettre la mise en œuvre effective des politiques et des actions extérieures de l'Union [...] ;
- Contribuer à prévenir les conflits et à garantir une capacité et un degré de préparation suffisants en vue de faire face aux situations d'avant crise et d'après crise et de consolider la paix ;
- Répondre aux menaces spécifiques qui pèsent sur la paix ainsi que sur la sécurité et la stabilité internationales aux niveaux mondial et transrégional.

Fait important, l'aide technique et financière susmentionnée peut couvrir en particulier « le soutien aux mesures nécessaires pour entamer la réhabilitation et la reconstruction d'infrastructures essentielles, de logements, de bâtiments publics et de biens économiques et de capacités de production fondamentales, ainsi qu'à d'autres mesures destinées à relancer l'activité économique, à créer de l'emploi et à établir les conditions minimales nécessaires à un développement social durable ».

Au-delà du type d'assistance à la gestion des crises proposé dans le cadre de l'instrument normatif susmentionné, les pays peuvent également envisager d'aider les pays à planifier des initiatives de renforcement de la résilience des infrastructures critiques. Cette aide pourrait notamment se matérialiser par des transferts de connaissances et de savoir-faire concernant les différents cycles de la protection des infrastructures critiques, de l'évaluation des risques à la mise en place d'un cadre de gouvernance adapté. Dans le même ordre d'idées, en ce qui concerne les infrastructures d'information critiques, le processus Meridian a proposé que des ressources et des connaissances soient transmises aux pays où les politiques et les activités étaient moins développées, lesquels

[29] Manuel de sûreté (Doc 8973 – Diffusion restreinte).
[30] Règlement (UE) n °230/2014 instituant un instrument contribuant à la stabilité et à la paix, consultable à l'adresse suivante : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0230&from=FR.

pourraient apprendre, par l'intermédiaire du guide ou de pays partenaires, des approches organisationnelles ou des procédures utiles ainsi que les pièges à éviter. De cette façon, ces pays pourraient avancer plus vite dans leurs travaux concernant la protection des infrastructures d'information critiques que s'ils ne bénéficiaient d'aucun accompagnement. Pour un pays qui est en avance sur les autres dans le domaine de la protection des infrastructures d'information critiques, être un guide apporte aussi des avantages. Le pays partenaire peut poser des questions qui n'ont pas encore été envisagées par le pays guide. De plus, le renforcement de la protection des infrastructures d'information critiques dans le pays partenaire permet de nouer un lien plus sûr dans le cyberespace. Parallèlement, avant de s'adresser à un partenaire potentiel, les pays guides devraient s'assurer auprès des ministères et organismes nationaux concernés que toutes les mesures de coordination et les autorisations nécessaires ont été mises en place. Il est cependant possible de commencer par des discussions informelles pour établir la compatibilité et les intérêts mutuels, avant que chaque pays décide de mettre en place un partenariat plus officiel (GFCE-Meridian 2016, p. 53).

7. INITIATIVES INTERNATIONALES PAR SECTEUR

Le présent chapitre donne un aperçu d'un certain nombre d'initiatives clefs prises par les organismes des Nations Unies dans différents secteurs relevant des infrastructures critiques. L'objectif n'est pas d'être exhaustif, qu'il s'agisse de la liste des secteurs concernés ou de l'énumération des initiatives décrites, mais bien plutôt d'aiguiller le lecteur vers des ressources et des outils susceptibles de le guider dans la conception de plans sectoriels avisés de protection des infrastructures critiques dans le cadre de stratégies nationales plus larges.

7.1 Secteur maritime

Organisme chef de file international dans le domaine, l'Organisation maritime internationale s'occupe des questions de protection des infrastructures critiques, notamment contre les attentats terroristes, dans le cadre des initiatives qu'elle prend pour sécuriser l'industrie maritime civile, qui comprend à la fois le secteur maritime et le secteur portuaire. En ce qui concerne ces derniers, si les ports sont, « pour de nombreux pays, des infrastructures essentielles, […]en l'absence de lois, de politiques et d'orientations nationales et locales claires permettant de coordonner les activités de toutes les parties prenantes […], les interventions en matière de sécurité dans les ports sont pour le moins fragmentées. Une stratégie préventive fondée sur l'analyse des risques et bien coordonnée est essentielle pour assurer l'efficacité des régimes de sécurité des ports et des installations portuaires, qu'il s'agisse de […] lutter contre le vol […] ou d'empêcher les terroristes […] d'y avoir accès »[31]. Pour remédier à ces problèmes, « l'OMI a mis au point toute une série de directives, d'outils d'auto-évaluation et de matériel didactique pour assurer la protection des ports, des navires et des installations offshore ». Les menaces continuant d'évoluer, « les ripostes […] ne se concentrent plus sur la lutte contre le terrorisme, mais l'accent est désormais mis sur des mesures à caractère anticipatif visant à [le] prévenir […]. L'un des principaux défis à la mise en œuvre efficace des mesures de sécurité […] et d'application de la loi dans le secteur maritime est [qu'elles] sont considérées comme […] relevant de différentes entités – […] la marine, la garde côtière, la police […] – qui se font concurrence pour des ressources limitées, et non [une problématique] multi-institutions ».

Le programme mondial de l'OMI sur la sûreté maritime, en particulier, a pour mission de concevoir et d'exécuter des projets de coopération technique dont l'objet principal est d'apporter un soutien aux États aux fins de la mise en œuvre, de la vérification, de la conformité et de l'application des différents cadres juridiques et opérationnels de l'OMI. L'un de ces cadres, des plus importants dans le domaine, est le Code international pour la sûreté des navires et des installations portuaires (ISPS). Composé de deux sections, le Code ISPS contient, dans une partie à caractère obligatoire (Partie A), des prescriptions détaillées relatives à la sûreté maritime et portuaire à l'intention des gouvernements des Parties à la Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS), des autorités portuaires et des compagnies maritimes, et, dans une partie à caractère non obligatoire (Partie B), un ensemble de recommandations sur les dispositions à

[31] Intervention du représentant de l'OMI, procès-verbal de la 7882e séance du Conseil de sécurité, à l'adresse : https://undocs.org/fr/S/PV.7882.

prendre pour satisfaire à ces mêmes prescriptions. Les principaux objectifs du Code ISPS consistent à[32] :

- créer un cadre international qui favorise la coopération entre les gouvernements contractants, les organismes publics, les administrations locales et les secteurs maritime et portuaire afin d'évaluer et de détecter les menaces potentielles pour la sûreté des navires et des installations portuaires utilisés dans le cadre du commerce international, et de mettre en œuvre des mesures de sûreté préventives face à ces menaces ;
- déterminer le rôle et les responsabilités respectifs de tous les acteurs dont la mission est d'assurer la sûreté maritime au sein des ports et à bord des navires, aux échelles nationale, régionale et internationale ;
- veiller à ce que les renseignements liés à la sûreté maritime sont rassemblés et échangés de façon rapide et efficace aux échelles nationale, régionale et internationale ;
- fournir une méthode d'évaluation de la sûreté du port et du navire propre à faciliter l'élaboration de plans et procédures de sûreté pour le navire, la compagnie et les installations portuaires, lesquels doivent impérativement être utilisés pour répondre aux différents niveaux de sûreté des navires ou des ports ;
- veiller à ce que des mesures de sûreté maritime adaptées et proportionnées soient en place à bord des navires et dans les ports.

Pour faire face à toute menace potentielle pour la sûreté, les pays, les autorités portuaires et les compagnies maritimes doivent, en vertu du Code ISPS, désigner respectivement des agents de sûreté de l'installation portuaire, des agents de sûreté du navire et des agents de sûreté de la compagnie, lesquels ont pour mission d'élaborer et de mettre en œuvre des plans de sûreté adaptés efficaces.

Outre le Code ISPS, le programme de l'OMI pour la sûreté maritime repose sur un certain nombre d'autres instruments relatifs à la sûreté maritime, qui ont été réunis en 2012 dans un recueil intitulé « Guide pour la sûreté maritime et le Code ISPS », qui vise à mettre à la disposition des parties prenantes un document de synthèse complet contenant des recommandations en matière de sûreté.

7.2 Secteur des transports aériens

L'**Organisation de l'aviation civile internationale (OACI)** est une institution spécialisée des Nations Unies créée par les États en 1944 pour gérer et administrer la Convention relative à l'aviation civile internationale (Convention de Chicago)[33].

L'OACI œuvre de concert avec les 192 États signataires de la Convention et des groupes du secteur à l'établissement d'un consensus sur des normes et pratiques recommandées (SARP) et des politiques en matière d'aviation civile internationale servant de base à un secteur de l'aviation civile sûr et efficace, dont le développement soit économiquement durable et écologiquement responsable. Les États membres de l'OACI utilisent ces SARP et politiques pour s'assurer que leurs opérations et réglementations locales d'aviation civile sont conformes aux normes mondiales, ce

[32] *Source* : OMI, Sûreté maritime et piraterie, à l'adresse : www.imo.org/fr/ourwork/security/pages/maritimesecurity.aspx.
[33] Doc 7300/9.

qui permet au réseau mondial de transport aérien d'exploiter plus de 100 000 vols par jour, en toute sécurité et avec efficacité dans toutes les régions du monde.

Outre qu'elle s'efforce essentiellement d'établir entre ses États membres et l'industrie un consensus sur les SARP et politiques internationales, et parallèlement à de nombreux autres programmes et priorités, l'OACI : coordonne l'assistance et le renforcement des capacités pour les États, en appui à de nombreux objectifs de développement de l'aviation ; produit des plans mondiaux pour coordonner les progrès stratégiques multilatéraux dans les domaines de la sécurité et de la navigation aérienne ; suit de nombreuses mesures de performance du secteur du transport aérien et en rend compte ; et effectue des audits des capacités de supervision de l'aviation civile des États dans les domaines de la sûreté et de la sécurité.

L'objectif stratégique relatif à la sûreté et à la facilitation de l'aviation civile est mis en œuvre suivant les grands axes ci-après :

- initiatives de politique générale ;
- audits destinés à vérifier les capacités des États Membres en matière de supervision des activités relatives à la sûreté des transports aériens ;
- aide au renforcement des capacités et formation destinée à améliorer les capacités connexes des États ;
- élaboration et mise en œuvre de la Stratégie pour un programme OACI d'identification des voyageurs (TRIP) ;
- gestion du répertoire de clefs publiques (RCP) de l'OACI.

Le travail de l'OACI dans le secteur repose sur un certain nombre de traités relatifs à la sûreté de l'aviation. Adoptés sur une période de plus de cinquante ans, ils sont généralement considérés comme faisant partie intégrante du cadre juridique universel de lutte contre le terrorisme :

- Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs de 1963, et son Protocole supplémentaire de 2014 ;
- Convention pour la répression de la capture illicite d'aéronefs de 1970, et son Protocole supplémentaire de 2010 ;
- Convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile de 1971 ;
- Protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale de 1988, et son Protocole supplémentaire de 2010 ;
- Convention sur le marquage des explosifs plastiques et en feuilles aux fins de détection de 1991 ;
- Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale de 2010 ;
- Protocole portant amendement de la Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs de 2014.

Le document fondateur pour ce qui est de la collaboration des États, du secteur, des parties prenantes et de l'OACI dans l'objectif commun de rendre l'aviation plus sûre dans le monde entier

est le Plan pour la sûreté de l'aviation dans le monde. Approuvé en 2017 par le Conseil de l'OACI, il définit cinq résultats prioritaires :

- renforcer la sensibilisation et la réponse au risque ;
- développer une culture de sûreté et des capacités humaines en la matière ;
- améliorer les ressources technologiques et encourager l'innovation ;
- renforcer la supervision et l'assurance de la qualité ;
- accroître la coopération et l'appui.

L'OACI a mis au point un outil fondamental, le *Manuel de sûreté de l'aviation*[34], conçu pour aider les États à mettre en œuvre les normes et pratiques recommandées figurant à l'Annexe 17 (Sûreté) à la Convention relative à l'aviation civile internationale (Convention de Chicago)[35]. Publiée en 2017, la version la plus récente du Manuel contient des directives nouvelles et révisées, dont celles consacrées à la sûreté des zones terrestres des aéroports, au contrôle du personnel et des véhicules et aux cybermenaces pesant contre les systèmes aériens critiques revêtent un intérêt particulier au regard de la protection des infrastructures critiques.

Autre outil utile, l'Énoncé du contexte de risque à l'échelle mondiale, publié annuellement, est un document évolutif destiné à fournir aux États les informations les plus pertinentes sur l'état des menaces et des risques. Il présente une analyse des menaces mondiales contre l'aviation civile, des informations sur l'évolution récente des tactiques terroristes et une analyse technique de menaces particulières pesant sur la sûreté aérienne. Dans la dernière version, il est indiqué que certains groupes terroristes continuent de rechercher des méthodes novatrices de dissimulation d'engins explosifs improvisés afin de contourner les mesures de sûreté en vigueur.

Consciente qu'il est urgent et important de protéger contre les cybermenaces les éléments critiques que sont l'infrastructure, les systèmes informatiques et les données de l'aviation civile, l'Assemblée de l'OACI, à sa trente-neuvième session, a demandé que soit menée une action coordonnée en vue de mettre sur pied à l'échelle mondiale une capacité de résilience acceptable en la matière. À cette fin, la résolution A39-19 intitulée « Cybersécurité dans l'aviation civile »[36] définit les mesures que les États et les autres parties prenantes doivent prendre dans le cadre de la collaboration horizontale et transversale pour lutter contre les menaces pesant sur l'aviation civile.

Le Programme d'identification des voyageurs (TRIP) de l'OACI a été approuvé en 2013 par l'Assemblée de l'Organisation à sa trente-huitième session. La stratégie y relative, qui met l'accent sur une conception intégrée des méthodes de gestion de l'identification des voyageurs afin d'optimiser la sûreté et la facilitation des opérations, devrait permettre aux États d'être mieux à

[34] Doc 8973. Le *Manuel* est en accès restreint. Sa diffusion est limitée aux autorités de l'aviation civile des États et, sur demande, à d'autres entités chargées de la mise en œuvre des mesures de sûreté aérienne, telles que les exploitants d'aéroports et d'aéronefs, ou d'autres entités validées par une autorité nationale compétente. Le *Manuel de sûreté de l'aviation* est accessible par voie électronique aux utilisateurs dûment autorisés, sur le site Web : https://drm.icao.int/.

[35] L'Annexe 17 (Sûreté) comprend notamment les normes et pratiques recommandées pour la sûreté de l'aviation internationale. Elle est revue et modifiée en permanence en fonction des menaces nouvelles et des progrès technologiques qui ont une incidence sur l'efficacité des mesures visant à prévenir les actes d'intervention illicite.

[36] Résolution A39-19, octobre 2016, doc 10075, sect. VII.24 (https://www.icao.int/Meetings/a39/Documents/Resolutions/10075_fr.pdf).

même d'identifier distinctement chaque personne en fournissant à leurs autorités des outils d'identification et des éléments d'orientation efficaces. Ce cadre devrait permettre d'améliorer sensiblement la sûreté de l'aviation et d'en faciliter le fonctionnement en conjuguant les différents éléments relatifs à la gestion de l'identification et en mettant à profit le rôle moteur joué par l'OACI dans le domaine des Documents de voyage lisibles à la machine (DVLM). La stratégie repose sur cinq éléments étroitement imbriqués : la preuve d'identité, les DVLM, la délivrance et le contrôle des documents de voyage, les systèmes et outils d'inspection et l'interopérabilité des applications. Les spécifications techniques permettant l'interopérabilité des documents de voyage à l'échelle mondiale figurent dans le document 9303, intitulé « Documents de voyage lisibles à la machine ».

L'infrastructure critique liée aux voyages comprendrait l'infrastructure cybernétique et physique, qui permet la délivrance des documents de voyage, et les systèmes de contrôle aux frontières, qui comportent les systèmes et outils d'inspection et les applications interopérables utilisées pour le traitement du passage des voyageurs aux frontières. L'infrastructure de sécurisation des éléments d'identification joue un rôle essentiel en amont dans l'infrastructure critique liée aux voyages.

On trouvera à l'adresse suivante de nombreux documents d'orientation sur le programme TRIP élaborés avec le concours des experts techniques du Groupe consultatif technique : www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

En vue d'encourager la participation des États au répertoire de clefs publiques (RCP) de l'OACI, l'Amendement nº 26 de l'Annexe 9 (Facilitation) à la Convention ajoute à l'Annexe la nouvelle Pratique recommandée 3.35.5, qui vise les États membres de l'OACI utilisant des systèmes de contrôle frontalier automatisé (CFA). Cette nouvelle pratique recommandée encourage les États concernés à se servir des informations qui figurent dans le RCP pour valider les passeports électroniques, en établissant des correspondances biométriques entre la reconnaissance faciale du passager et la photographie figurant dans son passeport.

7.3 Secteur des technologies de l'information

La protection des infrastructures d'information critiques contre les risques liés à la cybersécurité est un objectif prioritaire de l'Union internationale des télécommunications (UIT). Le Plan d'action de Buenos Aires, adopté à la Conférence mondiale de développement des télécommunications de 2017, avait notamment pour objectif de « promouvoir le développement d'infrastructures et de services, et notamment instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC » (objectif 2)[37].

Les travaux de l'UIT sont en prise directe avec l'amélioration de la résilience des infrastructures d'information critiques (puis des infrastructures critiques tout court) contre les cyberattaques, quelle qu'en soit l'origine. Ses activités s'articulent autour de trois grands axes : i) la normalisation ; ii) la sensibilisation ; iii) le développement des capacités. Les initiatives saillantes menées dans chaque domaine sont présentées ci-après.

[37] Le rapport final de la Conférence est disponible à l'adresse : www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_fr.pdf.

i) Normalisation

Les travaux de normalisation sont effectués par un certain nombre de commissions d'études techniques au sein desquelles des représentants des membres de l'UIT élaborent des recommandations (normes) se rapportant à différents domaines des télécommunications internationales. La Commission d'études 17 (CE 17), en particulier, se propose de développer la confiance et la sécurité dans le cadre de l'utilisation des technologies de l'information et de la communication, afin de renforcer la sécurité dans les infrastructures, les services et les applications de réseau. Plus de 350 normes[38] (recommandations UIT-T et suppléments) ont été adoptées jusqu'à présent au sein de cette commission d'études.

Les domaines actuels de travail de la CE 17 comprennent notamment les questions suivantes : cybersécurité, gestion de la sécurité, architectures et cadres de la sécurité, gestion d'identité, sécurité des applications et aspects de l'informatique en nuage liés à la sécurité, services pour l'Internet des objets (IoT), systèmes de transport intelligents, mégadonnées, technologie du grand livre ouvert, etc. L'une des principales références, en matière de normes de sécurité, est la Recommandation UIT-T X.509 relative à l'authentification électronique sur les réseaux publics, considérée comme une innovation sans précédent pour la conception des applications relatives aux infrastructures à clefs publiques.

ii) Sensibilisation

L'Indice de cybersécurité dans le monde mis au point par l'UIT est un outil sans précédent. Conçu avant tout comme outil de sensibilisation, il vise à mesurer l'engagement des pays en faveur de la cybersécurité. Les performances de chaque pays sont évaluées dans cinq domaines : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités et coopération.

Des questionnaires sont établis pour évaluer l'engagement des pays dans chacun de ces grands domaines. Ces questions sont ensuite pondérées, en concertation avec un groupe d'experts, pour permettre de calculer un score global au titre de l'Indice. La troisième édition de l'Indice est actuellement en cours d'élaboration[39].

iii) Développement des capacités

Dans ce domaine, l'UIT aide les États Membres à mettre en place des équipes nationales d'intervention en cas d'incident informatique (CIRT). Il s'agit de centres de liaison nationaux chargés de coordonner dans les meilleurs délais une réponse efficace aux cyberattaques. L'objectif de l'UIT est d'aider les pays tout au long du processus de mise en place des CIRT, depuis l'évaluation de leur état de préparation jusqu'aux phases de planification et de mise en œuvre, sur la base du

[38] Les recommandations UIT-T élaborées par la Commission d'études 17 de l'UIT-T sont accessibles au public à l'adresse : http://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=17.

[39] Les versions antérieures peuvent être consultées à l'adresse : https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

principe de la collaboration continue. Par ailleurs, l'UIT organise régulièrement des cyberexercices régionaux en vue de renforcer la collaboration entre CIRT nationales de la même région.

7.4 Secteur des armes classiques

Dans sa résolution 2370 (2017), le Conseil de sécurité a souligné la « valeur […] des mesures visant à assurer la sécurité physique et la gestion des stocks d'armes légères et de petit calibre, qui constituent des moyens importants de contribuer à mettre fin à l'approvisionnement des terroristes en armes »[40].

Il a, au paragraphe 7 en particulier, souligné « qu'il import[ait] que les États Membres prennent des mesures appropriées […] pour prévenir […] les pillages de stocks nationaux par des terroristes ou l'acquisition par eux d'armes légères et de petit calibre provenant de ces stocks, et […] qu'il import[ait] d'aider les États de ces régions à surveiller et contrôler les stocks d'armes légères et de petit calibre, afin d'empêcher les terroristes d'en acquérir ».

Dans le cadre de la protection des infrastructures critiques, assurer la sécurité physique et la gestion des stocks d'armes classiques revêt une importance critique à double titre. Premièrement, cela réduit le risque d'une utilisation de ces armes contre des infrastructures critiques telles que les systèmes de transport, les édifices publics et toute autre installation jugée essentielle par les pays concernés. Deuxièmement, ces stocks peuvent être considérés en soi comme des infrastructures critiques de par le rôle déterminant qu'ils jouent dans la politique de défense des pays.

Le régime juridique international relatif aux armes classiques se compose d'un ensemble d'instruments internationaux et régionaux qui, tout en fournissant aux États un solide cadre juridique et opérationnel pour le renforcement de leur propre régime juridique, ne constituent pas nécessairement un ensemble d'outils homogène. À titre d'exemple, le Protocole contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions (Protocole relatif aux armes à feu)[41] traite de cette question sous l'angle de la justice pénale, dans le but d'offrir aux pays des mesures de lutte face au caractère transnational de ce phénomène et à ses liens avec la criminalité organisée. D'autres instruments traitant de sujets analogues abordent la question sous l'angle du désarmement, du trafic ou encore du développement et mettent davantage l'accent sur les mesures visant à réduire l'accumulation, la prolifération ou le détournement des armes à feu ainsi que leur utilisation à des fins abusives. Par conséquent, il importe que les autorités des États se familiarisent avec un cadre juridique international à caractère hétérogène et veillent à sa pleine mise en œuvre.

On trouvera dans la liste ci-après une compilation non exhaustive des traités internationaux et autres instruments de référence traitant de la question sous ses différents angles.

[40] Ce type de mesures était déjà envisagé dans le Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects, au titre duquel les gouvernements sont convenus d'améliorer leur législation nationale concernant les armes légères, le contrôle des importations et des exportations, et la gestion des stocks et à coopérer et s'entraider (https://www.un.org/disarmament/fr/convarms/armes-legeres/).

[41] Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée.

Organisation des Nations Unies

Traités

- Protocole contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions (Protocole relatif aux armes à feu), additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée (2001) ;
- Traité sur le commerce des armes (2013).

Autres instruments

- Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects (2001) ;
- Instrument international visant à permettre aux États de procéder à l'identification et au traçage rapides et fiables des armes légères et de petit calibre illicites (2005).

Afrique

Traités

- Protocole relatif au contrôle des armes à feu, des munitions et d'autres matériels connexes dans la région de la Communauté de développement de l'Afrique australe (2001) ;
- Protocole de Nairobi pour la prévention, le contrôle et la réduction des armes légères dans la région des Grands Lacs et la Corne de l'Afrique (2004) ;
- Convention de la Communauté économique des États de l'Afrique de l'Ouest sur les armes légères et de petit calibre, leurs munitions et autres matériels connexes (2006) ;
- Convention de l'Afrique centrale pour le contrôle des armes légères et de petit calibre, de leurs munitions et de toutes pièces et composantes pouvant servir à leur fabrication, réparation et assemblage (Convention de Kinshasa) (2010).

Autres instruments

- Déclaration de Bamako sur la position africaine commune sur la prolifération, la circulation et le trafic illicites des armes légères – instrument politiquement contraignant (2000) ;
- Stratégie de l'Union africaine sur le contrôle de la prolifération, de la circulation et du trafic illicites des armes légères et de petit calibre (2011) ;
- Plan d'action pour la mise en œuvre de la Stratégie de l'Union africaine sur le contrôle de la prolifération, de la circulation et du trafic illicites des armes légères et de petit calibre.

Amériques

Traités

- Convention interaméricaine contre la fabrication et le trafic illicites d'armes à feu, de munitions, d'explosifs et d'autres matériels connexes (CIFTA) (1997)

Autres instruments

- Plan andin pour prévenir, combattre et éliminer le trafic illicite d'armes légères sous tous ses aspects – instrument politiquement contraignant (2003) ;
- Règlements-types de la Commission interaméricaine de lutte contre l'abus des drogues – Règlement-type du contrôle des mouvements internationaux des armes à feu et de leurs pièces détachées et composants ainsi que des munitions ; Règlement-type du contrôle des courtiers en armes à feu et en pièces détachées, composants et munitions connexes ;
- Code de conduite des États d'Amérique centrale en matière de transfert d'armes, de munitions, d'explosifs et d'autres éléments connexes (2006).

Asie-Pacifique

Instruments

- Plan-cadre de Nadi (Cadre juridique visant un rapprochement des méthodes de maîtrise des armements) ;
- Plan d'action de l'ASEAN pour la lutte contre la criminalité transnationale (Association des nations de l'Asie du Sud-Est) (1999).

Europe

Organisation pour la sécurité et la coopération en Europe

- Plan d'action de l'OSCE relatif aux armes légères et de petit calibre (Document FSC. DEC/2/10) ;
- Manuel OSCE des meilleures pratiques concernant les munitions conventionnelles (2008) ;
- Principes de l'OSCE relatifs au contrôle du courtage des armes légères et de petit calibre, Forum pour la coopération en matière de sécurité, Décision n° 8/04 (2004) ;
- Éléments standard des certificats d'utilisateur final et des procédures de vérification pour les exportations d'ALPC, Forum pour la coopération en matière de sécurité, décision n° 5/04 (2004) ;
- Manuel des meilleures pratiques relatives aux armes légères et de petit calibre (2003) ;
- Principes régissant les transferts d'armes classiques, Série « Programme d'action immédiate », n° 3 (DOC.FSC/3/96) (1993) ;
- Document de l'OSCE sur les armes légères et de petit calibre (2000, republié en 2012) ;
- Décision n° 11/08 sur l'introduction de meilleures pratiques pour prévenir les transferts déstabilisants d'armes légères et de petit calibre par la voie du transport aérien et sur un questionnaire associé (2008).

Union européenne

- Action commune du Conseil du 12 juillet 2002 relative à la contribution de l'Union européenne à la lutte contre l'accumulation et la diffusion déstabilisatrices des armes légères et de petit calibre ;
- Position commune 2003/468/PESC du Conseil de l'Union européenne sur le contrôle du courtage en armements ;

- Position commune 2008/944/PESC du Conseil de l'Union européenne définissant des règles communes régissant le contrôle des exportations de technologie et d'équipements militaires ;
- Règlement (UE) n ° 258/2012 du Parlement européen et du Conseil du 14 mars 2012 portant application de l'article 10 du protocole des Nations unies contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la convention des Nations unies contre la criminalité transnationale organisée (protocole relatif aux armes à feu) et instaurant des autorisations d'exportation, ainsi que des mesures concernant l'importation et le transit d'armes à feu, de leurs pièces, éléments et munitions (Journal officiel de l'Union européenne, L 94, 2012) ;
- Code de conduite de l'Union européenne en matière d'exportation d'armements (1998) ;
- Stratégie de l'Union européenne de lutte contre l'accumulation illicite et le trafic d'armes légères et de petit calibre et de leurs munitions (2005).

7. 5 Secteurs chimique, biologique, radiologique et nucléaire (CBRN)

La perspective que des acteurs non étatiques, y compris des groupes terroristes et leurs partisans, aient accès à des armes de destruction massive et des matières connexes et les utilisent constitue une grave menace contre la paix et la sécurité internationales. Conscient de l'ampleur du problème, le Secrétaire général de l'ONU a placé la prévention au cœur même de son programme de paix et de sécurité. Dans sa résolution 70/291 portant sur le cinquième examen de la Stratégie antiterroriste mondiale des Nations Unies (prévue par la résolution 60/288), l'Assemblée générale a également demandé à tous les États Membres « d'empêcher les terroristes d'acquérir des armes de destruction massive [et] leurs vecteurs [...], et (encouragé) la coopération entre les États Membres ainsi qu'entre ceux-ci et les organisations régionales et internationales compétentes afin de renforcer les capacités nationales dans ce domaine ». Le Conseil de sécurité de l'ONU s'est également prononcé en ce sens, notamment par sa résolution 2325 du 15 décembre 2016, dans laquelle il a appelé tous les États Membres à renforcer leurs régimes nationaux de non-prolifération dans le cadre de l'application de la résolution historique 1540 (2004).

i) Bureau de lutte contre le terrorisme

En juin 2017, par sa résolution 71/291, l'Assemblée générale a créé le Bureau de lutte contre le terrorisme, lequel regroupe le Bureau de l'Équipe spéciale de lutte contre le terrorisme et le Centre de lutte contre le terrorisme. Depuis 2006, le Groupe de travail de l'Équipe spéciale sur la prévention des attentats terroristes à l'arme de destruction massive et les interventions en cas d'attentat a facilité l'échange interactif de connaissances et le partage d'informations sur les activités existantes et les plans d'urgence des entités des Nations Unies et des organisations internationales en matière de prévention et d'intervention en cas d'attaque à l'arme de destruction massive ou aux matières connexes. Depuis 2013, le Centre de lutte contre le terrorisme appuie le projet du Groupe de travail sur les moyens d'assurer l'interopérabilité interorganisations et la coordination des communications en cas d'attaques chimiques et/ou biologiques. Le projet consiste à évaluer la manière dont le système des Nations Unies et les organisations internationales interviendraient collectivement en cas d'attentat à l'arme ou aux matières

chimiques et biologiques, ainsi que le niveau de coordination prévu entre les différentes entités pour faciliter la fourniture rapide d'une assistance aux États touchés.

En 2018, le Centre de lutte contre le terrorisme a commencé à axer ses activités relatives aux attentats à l'arme de destruction massive et à l'arme chimique, biologique, radiologique ou nucléaire autour de quatre objectifs stratégiques : 1) faire mieux comprendre la menace que représente l'utilisation de ce type d'armes dans les attaques terroristes ; 2) élargir les activités de renforcement des capacités pour soutenir la prévention, la préparation et l'intervention dans les États Membres conformément à la Stratégie antiterroriste mondiale des Nations Unies, notamment dans les domaines du contrôle des frontières et des douanes, du contrôle stratégique du commerce, du trafic et de la sécurité des infrastructures critiques ; 3) établir des partenariats pour contribuer au renforcement actuel des capacités de la communauté internationale ; 4) améliorer la visibilité et appuyer la mobilisation de ressources supplémentaires.

ii) Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI)

Dans le cadre de l'Initiative relative aux centres d'excellence pour la réduction des risques chimiques, biologiques, radiologiques et nucléaires de l'Union européenne, l'UNICRI a aidé plusieurs États Membres de l'ONU à élaborer des plans d'action nationaux dans le domaine de la sécurité chimique, biologique, radiologique et nucléaire dans lesquels sont mis en évidence les principaux risques et les priorités nationales de renforcement des capacités. Lesdits plans d'action couvraient divers aspects de la prévention des risques CBRN (accidentels ou non) et de la lutte contre ceux-ci, notamment la sûreté et la sécurité des infrastructures critiques.

En outre, l'UNICRI a géré la mise en œuvre d'un projet multirégional dans le cadre de l'Initiative relative aux centres d'excellence CBRN de l'Union européenne (projet 19) intitulé « Élaboration de procédures et de lignes directrices destinées à créer des systèmes sécurisés de gestion de l'information et des mécanismes sécurisés d'échange de données sur les matières chimiques soumises à un contrôle réglementaire, et à les améliorer ». Ce projet, qui a été mis en œuvre de 2013 à 2015, visait à renforcer les capacités nationales en matière de gestion sécurisée de l'information et d'échange de données sur les matières et installations CBRN, en créant une équipe d'experts composée de spécialistes éminents des secteurs public et privé.

iii) Organisation internationale de police criminelle (INTERPOL)

En 2010, à l'occasion de sa quatre-vingtième session, l'Assemblée générale d'INTERPOL a pris la décision stratégique[42] de lancer un vaste programme de prévention des attentats terroristes de type CBRNE et d'intervention en cas d'attaque, afin d'appuyer l'action de ses 192 pays membres. En 2016, la Stratégie de lutte antiterroriste mondiale d'INTERPOL a consolidé la mission de l'Organisation dans le domaine CBRNE et a défini un axe d'action consacré aux armes et matériaux au titre duquel INTERPOL aidera les pays membres à identifier, suivre et intercepter le trafic illicite d'armes et de substances nécessaires aux activités terroristes. La Stratégie définit en outre les principales mesures que doit prendre la Sous-direction CBRNE et cibles vulnérables en vue d'aider

[42] AG-2011-RES-10

les pays membres à prévenir les menaces mondiales CBRNE émanant d'acteurs non étatiques et à y faire face :

- *Mesure 4.3* : Faciliter l'échange de renseignements entre les pays membres sur les sujets et modes opératoires liés aux incidents chimiques, biologiques, radiologiques et nucléaires et aux attaques perpétrées au moyen d'engins explosifs improvisés ;
- *Mesure 4.4* : Renforcer les capacités de prévention et d'intervention des pays membres face aux attaques chimiques, biologiques, radiologiques et nucléaires et aux attaques perpétrées au moyen d'engins explosifs improvisés en mettant en place des programmes de contre-mesures ;
- *Mesure 4.5* : Concevoir et coordonner des opérations interinstitutions transfrontalières fondées sur le renseignement pour intercepter les matières chimiques, biologiques, radiologiques et nucléaires ainsi que les composants d'engins explosifs improvisés faisant l'objet d'un trafic ;
- *Mesure 4.7* : Maintenir et renforcer des partenariats stratégiques à l'échelle mondiale sur les questions chimiques, radiologiques et nucléaires et en matière d'explosifs.

Dans le cadre de la mise en œuvre des mesures susmentionnées – et en vertu du Statut d'INTERPOL[43] – l'Organisation se concentre exclusivement sur la lutte contre les menaces CBRNE émanant d'acteurs non étatiques. En conséquence, INTERPOL se garde d'aborder les questions liées à la prolifération d'armes de destruction massive parrainée par des États, qui sont traitées en profondeur par d'autres mécanismes juridiques et institutionnels internationaux. Toutefois, l'éventail des acteurs non étatiques couvre non seulement les groupes terroristes, les individus agissant seuls (« loups solitaires ») et d'autres criminels en leur qualité d'utilisateurs finaux potentiels, mais également tout individu impliqué dans le trafic de matières CBRNE et de leurs différentes composantes. Les fournisseurs, les intermédiaires, les acheteurs et les réseaux de contrebande relèvent tous de la compétence d'INTERPOL.

INTERPOL est progressivement devenue l'une des organisations internationales principales pour ce qui est de l'action mondiale contre le terrorisme CBRNE étant donné que la communauté internationale a pris conscience du rôle pivot joué par les services de détection et de répression pour prévenir la menace CBRNE émanant d'acteurs non étatiques et y faire face. En outre, l'Organisation a intégré tous les grands cadres multinationaux et établi des liens étroits avec tous les partenaires internationaux concernés, en concrétisant l'approche interinstitutions à l'échelle mondiale.

Dans le cadre de ses activités dans le domaine CBRNE, INTERPOL se réfère naturellement à la résolution 1540 du Conseil de sécurité de l'ONU étant donné que celle-ci mentionne explicitement la question des acteurs non étatiques. Depuis qu'elle est active dans ce domaine, INTERPOL entretient une correspondance officielle avec le Comité 1540, dans laquelle sont décrites les modalités de leur collaboration actuelle et par laquelle sont désignés des points de contact respectifs. Plus récemment, INTERPOL a joué un rôle actif dans l'examen approfondi de l'état

[43] L'article 3 du Statut d'INTERPOL consacre le principe directeur de neutralité selon lequel il est interdit à l'Organisation de se livrer à toute activité ou intervention dans des questions ou affaires présentant un caractère politique, militaire, religieux ou racial.

d'avancement de l'application de la résolution en 2016. De manière plus générale, INTERPOL agit comme organisation de coopération chargée d'assister le Comité 1540 et la plupart de ses activités dans le domaine CBRNE favorisent directement ou indirectement l'application de la résolution.

INTERPOL entretient des relations de travail étroites avec le Bureau des affaires de désarmement de l'ONU, notamment en contribuant aux activités de renforcement des capacités du fichier d'experts appartenant au mécanisme d'enquête du Secrétaire général sur l'utilisation alléguée d'armes chimiques, bactériologiques (biologiques) ou à toxines.

Au sein d'INTERPOL, les équipes spécialisées se concentrent sur la prévention de trois formes de terrorisme :

- Le terrorisme radiologique et nucléaire
- Le bioterrorisme
- Le terrorisme chimique et les attentats à l'explosif

Les activités d'INTERPOL vont de l'analyse de données à l'organisation de conférences internationales et d'opérations sur le terrain, en passant par la tenue d'ateliers de formation et d'exercices de simulation. La méthodologie d'INTERPOL pour lutter contre la menace CBRNE repose sur trois piliers principaux :

i. Mise en commun et analyse des renseignements : outre l'évaluation et l'analyse de la menace, l'Organisation publie régulièrement un rapport analytique (INTERPOL CBRNE Monthly Digest) qu'elle partage avec ses pays membres et d'autres abonnés et dans lequel sont résumées les informations obtenues auprès de sources en accès libre en ce qui concerne tous les aspects de la criminalité et du terrorisme CBRNE afin de dresser une perspective analytique sur des problématiques particulières ;
ii. Renforcement des capacités et formation : l'Organisation aide ses pays membres à renforcer leurs capacités, leurs compétences et leurs connaissances afin de contrer la menace CBRNE. Elle s'emploie à :
    - aider les services de détection et de répression à acquérir une meilleure connaissance des substances chimiques, biologiques, radiologiques, nucléaires et explosives ;
    - organiser des séances de formation pour renforcer les capacités des forces de l'ordre ;
    - élaborer des méthodes de prévention destinées aux pays membres.

    Soutien logistique et appui aux enquêtes : INTERPOL peut fournir, sur demande, un appui opérationnel à ses pays membres en y dépêchant une cellule de crise. En cas d'attaque terroriste, des spécialistes des substances chimiques, biologiques, radiologiques, nucléaires et explosives peuvent être déployés dans ces équipes. En outre, l'Organisation mène diverses opérations, initiatives et projets pour aider les services de répression du monde entier à combattre le trafic de substances CBRNE.

7.5.1 Secteur chimique

Dans le cadre du mandat de l'Organisation pour l'interdiction des armes chimiques (OIAC), la protection des infrastructures critiques passe par la promotion de bonnes pratiques de gestion du dispositif de sécurité pour les sites et activités chimiques. En 2016, l'Organisation a élaboré un

guide des meilleures pratiques qui recueille et détaille les informations reçues de 16 États membres (OIAC 2016).

L'approche de l'OIAC consiste notamment à aborder les questions de sécurité (c'est-à-dire en prenant des mesures contre les rejets « délibérés » de produits chimiques toxiques) parallèlement aux questions de sûreté (c'est-à-dire en prenant des mesures pour faire face aux rejets « non délibérés »). Dans ce domaine, l'OIAC a pour objectifs prioritaires de veiller à ce que les pays abordent les dimensions de sûreté et de sécurité suivantes :

- *Prévention* : compréhension et mise en œuvre de mesures visant à réduire le risque qu'un accident chimique ou un incident de sécurité ne survienne, notamment le vol de produits chimiques à des fins abusives ou le rejet malveillant de produits chimiques dans l'environnement ;

- *Détection* : systèmes et activités qui favorisent la détection précoce d'un rejet ou d'une perte chimique et confirmation de l'utilisation d'un produit chimique à la suite d'un rejet soupçonné (accidentel ou malveillant). Des éléments de signalisation des risques devraient être intégrés aux systèmes de détection.
- *Intervention* : à la fois au niveau de l'installation et au niveau national en cas d'accident chimique ou d'incident lié à la sécurité chimique. Les activités d'intervention comprennent la mobilisation, l'équipement et la formation des intervenants de première ligne, comme les pompiers, le personnel compétent en cas de présence de matières dangereuses, les services médicaux d'urgence et la police.

De 2009 à 2016, plus de 1400 participants issus de plus de 130 États membres ont bénéficié de programmes de renforcement des capacités sur la gestion intégrée des risques chimiques encadrés par le Secrétariat technique de l'OIAC. Les activités reposent sur les normes fixées par la réglementation internationale (principalement la Convention sur les armes chimiques) et les réglementations nationales. Parmi les instruments et initiatives internationaux existants, l'OIAC a mis en évidence les suivants car ils comportent des éléments utiles sur les questions de sûreté et de sécurité chimiques :

- La résolution 1540 (2004) du Conseil de sécurité, qui oblige les États, entre autres, à s'abstenir d'apporter un appui, quelle qu'en soit la forme, à des acteurs non étatiques qui tenteraient de mettre au point, de se procurer, de fabriquer, de posséder, de transporter, de transférer ou d'utiliser des armes nucléaires, chimiques ou biologiques ou leurs vecteurs. Cet instrument porte essentiellement sur les éléments de la dimension préventive de la gestion des risques de sécurité chimique ;
- La Convention de Bâle, qui traite des mouvements transfrontières de déchets dangereux. La Convention vise à prévenir le rejet de produits chimiques toxiques dans l'environnement et les mesures d'application peuvent quant à elles permettre de manipuler les produits chimiques avec précaution et de réduire le volume de produits chimiques dans les transports et dans le système de gestion des déchets, à l'appui des meilleures pratiques en matière de sécurité et de sûreté chimiques ;

- La Convention de Stockholm, dont l'objectif est de réduire la production et l'utilisation de polluants organiques persistants. Les règlements et les pratiques optimales adoptés pour mettre en œuvre la Convention contribuent à améliorer la gestion des risques de sécurité et de sûreté chimiques ;
- La Convention de Rotterdam, qui encadre l'étiquetage et la manipulation de produits chimiques dangereux, en particulier ceux qui font l'objet d'un commerce international. Y figurent des normes et des directives à l'appui des pratiques de sécurité de la chaîne d'approvisionnement ;
- La Directive Seveso (I, II et III), instruments de l'Union européenne visant à améliorer la sûreté des sites contenant de grandes quantités de substances dangereuses ;
- Le Système général harmonisé de classification et d'étiquetage des produits chimiques (SGH), une norme établie par l'ONU afin de remplacer les nombreux systèmes de classification et d'étiquetage des matières dangereuses auparavant utilisés dans le monde. Bien que d'application volontaire, plusieurs pays l'ont rendu obligatoire au niveau national ;
- L'initiative Responsible Care, une initiative de l'industrie chimique mondiale visant, entre autres, à améliorer la sécurité des produits et des activités du domaine et à fournir une assistance et des conseils pour encourager la gestion responsable des produits chimiques par tous ceux qui les gèrent et les utilisent le long de la chaîne de production[44] ;
- L'Organisation internationale de normalisation (ISO), qui a établi un certain nombre de normes en matière de sécurité et de sûreté des produits chimiques, en particulier la norme 31000 pour la gestion du risque, la norme 28000 pour la gestion de la sûreté de la chaîne d'approvisionnement, la norme 14000 pour la gestion environnementale et la norme 9000 pour la gestion de la qualité.

Un atelier d'experts sur la coordination internationale en matière de sécurité chimique a été organisé par l'OIAC en 2017 afin d'examiner tout particulièrement la question de la menace terroriste posée par les acteurs non étatiques[45]. Les participants ont dressé un aperçu général visant à faire le point sur la coopération et la coordination internationales en cours en matière de sécurité chimique, à recenser les lacunes et à débattre des activités à venir, notamment les futurs mécanismes de coordination. L'une des principales recommandations était la création d'un mécanisme de coordination internationale permettant aux principaux acteurs internationaux qui soutiennent le développement des capacités mondiales en matière de sécurité chimique de discuter des priorités et des méthodologies, de mobiliser leurs ressources respectives, de collaborer si nécessaire pour répondre aux besoins de chaque État et de mieux faire connaître les besoins et l'assistance en matière de sécurité chimique. À l'issue de l'atelier, les participants ont également adopté une recommandation primordiale au sujet de l'établissement d'un modèle de méthodologie en matière de sécurité chimique.

[44] http://www.cefic.org/Responsible-Care

[45] Atelier d'experts sur la coordination internationale en matière de sécurité chimique, tenu le 7 décembre 2017, voir lien suivant : https://www.opcw.org/fileadmin/OPCW/Protection-Against-CW/OPCW_Chemical_Security_Workshop_-_Informal_Summary_-_October_2017_-_for_release.pdf

7.5.2 Secteur nucléaire

La protection des matières nucléaires et autres matières radioactives et des installations associées contre les attaques terroristes et autres dangers est un objectif prioritaire de l'Agence internationale de l'énergie atomique (AIEA). Les initiatives que celle-ci prend dans ce domaine s'inscrivent dans le cadre du programme de sécurité nucléaire, qui traite de toutes les questions relatives à la prévention, la détection et l'intervention en cas de vol, sabotage, accès non autorisé, cession illégale ou autres actes malveillants mettant en jeu des matières nucléaires et autres substances radioactives ou les installations associées. Un ensemble d'instruments internationaux sous-tendent les bases juridiques du programme, notamment les suivants :

- La Convention sur la protection physique des matières nucléaires et son amendement de 2005 ;
- Le Code de conduite sur la sûreté et la sécurité des sources radioactives ;
- Les résolutions 1325 (2000), 1540 (2004) et 2325 (2016) du Conseil de sécurité ;
- La Convention internationale pour la répression des actes de terrorisme nucléaire.

Les publications de la collection Sécurité nucléaire de l'AIEA complète les instruments susmentionnés en fournissant des pratiques optimales, des guides techniques, des manuels de formation, entre autres, à l'intention des États Membres.

On peut notamment mentionner le Guide d'application intitulé « Établissement de l'infrastructure de sécurité nucléaire pour un programme électronucléaire » (AIEA 2013). Celui-ci fournit des orientations techniques sur la mise en place d'une infrastructure de sécurité nucléaire, y compris un cadre juridique, réglementaire et institutionnel et une stratégie nationale de sécurité nucléaire. Sa raison d'être réside dans la nécessité de « veiller à ce que des matières nucléaires et autres matières radioactives ne tombent pas entre les mains de parties susceptibles de les utiliser aux fins d'actes criminels ou terroristes et pour empêcher les actes de sabotage contre des installations et les activités associées, y compris en cours de transport ».

Le 13 septembre 2017, le Conseil des gouverneurs de l'AIEA a approuvé le Plan sur la sécurité nucléaire pour 2018-2021 (AIEA 2017). Les objectifs énoncés dans le Plan sont les suivants :

- contribuer aux efforts mondiaux en vue d'une sécurité nucléaire efficace en préparant des orientations exhaustives sur la sécurité nucléaire, et sur demande, en encourageant leur utilisation au moyen d'examens par des pairs et de services consultatifs, ainsi que de la création de capacités, notamment la formation théorique et pratique ;
- faciliter l'adhésion aux instruments juridiques internationaux applicables et leur mise en œuvre, ainsi que le renforcement de la coopération et de la coordination internationales en matière d'assistance ;
- jouer le rôle principal et renforcer la coopération internationale en matière de sécurité nucléaire afin de répondre aux priorités exprimées par les États Membres à travers les décisions et résolutions des organes directeurs de l'Agence.

Les activités envisagées dans le cadre du Plan visent essentiellement à aider les pays qui en font la demande à mettre en place des régimes nationaux de sécurité nucléaire durables et efficaces ainsi qu'à promouvoir le respect des instruments internationaux pertinents. Le Plan énumère notamment un ensemble de programmes et de sous-programmes prioritaires d'intervention à mettre en œuvre au moyen d'activités d'assistance technique et de renforcement des capacités, dans les domaines suivants :

Gestion de l'information
- Évaluation des besoins et des priorités en matière de sécurité nucléaire
- Partage d'informations
- Sécurité de l'information, sécurité informatique et services informatiques

Sécurité nucléaire des matières et des installations associées
- Approches de la sécurité nucléaire pour l'ensemble du cycle du combustible nucléaire
- Renforcement de la sécurité des matières nucléaires au moyen de la comptabilisation et du contrôle
- Renforcement de la sécurité des matières radioactives et des installations associées
- Sécurité nucléaire du transport des matières nucléaires et autres matières radioactives

Sécurité nucléaire des matières non soumises à un contrôle réglementaire
- Infrastructure institutionnelle couvrant les matières non soumises à un contrôle réglementaire
- Architecture de détection et d'intervention pour la sécurité nucléaire
- Conduite des opérations sur le lieu d'un délit impliquant des matières radioactives et criminalistique nucléaire

Élaboration de programmes et coopération internationale
- Coopération internationale sur des réseaux et des partenariats pour la sécurité nucléaire
- Programmes de formation théorique et pratique pour la mise en valeur des ressources humaines
- Coordination des services d'orientation et de conseil en matière de sécurité nucléaire

RÉFÉRENCES

Ackerman 2007, Assessing terrorist motivations for attacking critical infrastructures, Centre for Nonproliferation Studies, Institut d'études internationales de Monterey, disponible à l'adresse suivante : https://e-reports-ext.llnl.gov/pdf/341566.pdf

Arie H.2017, Japan's Approach to Tackling Cybersecurity Challenges, disponible à l'adresse suivante : www.japanindustrynews.com/2017/01/japans-approach-tackling-cybersecurity-challenges/

Australie-Nouvelle-Zélande 2015, National Guidelines for Protecting Critical Infrastructure from Terrorism, Australia-New Zealand Counter-Terrorism Committee, disponible à l'adresse suivante : www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf

Canada 2005, Stratégie et Plan d'action de résilience aux incidents chimiques, biologiques, radiologiques, nucléaires et à l'explosif pour le Canada, disponible à l'adresse suivante : https://www.securitepublique.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/chmcl-blgcl-rdlgcl-fr.aspx

Clemente 2013, Cyber Security and Global Interdependence: What Is Critical?, Chatham House, février 2013, disponible à l'adresse suivante : www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf

Coroner's Inquests into the London Bombings of 7 July 2005, 6 mai 2011, disponible à l'adresse suivante : http://image.guardian.co.uk/sys-files/Guardian/documents/2011/05/06/rule43-report.pdf

DECT 2017, Physical Protection of Critical Infrastructure against Terrorist Attacks, Trends Report, Direction exécutive du Comité contre le terrorisme, disponible à l'adresse suivante : www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf

Commission européenne 2005, Livre Vert sur un programme européen de protection des infrastructures critiques, COM (2005) 576 final

Commission européenne 2013, Stratégie de cybersécurité de l'Union européenne, JOIN (2013) 1 final, disponible à l'adresse suivante : https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_fr.pdf

Commission européenne 2013 bis, Working Document on a New Approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures More Secure, SWD(2013) 318 final, disponible à l'adresse suivante :

https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

Commission européenne 2017, Plan d'action visant à améliorer la protection des espaces publics, le 18.10.2017, COM (2017) 612 final, disponible à l'adresse suivante : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017DC0612&from=EN

Federal Signal 2013, The basis of interoperability for emergency communications, Thought Paper, disponible à l'adresse suivante : www.fedsig.com/sites/default/files/news/pdf/The%20bais%20of%20Interoperability%20for%20Emergency%20Communications.pdf

France 2014, Instruction générale interministérielle relative à la sécurité des activités d'importance vitale, Secrétariat général de la défense et de la sécurité nationale (N°6600/SGDSN/PSE/PSN), disponible à l'adresse suivante : http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

Allemagne 2009, National Strategy for Critical Infrastructure Protection, Federal Ministry of the Interior, disponible à l'adresse suivante : http://ccpic.mai.gov.ro/docs/Germania_cip_stategy.pdf

2015, rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (Doc. A/70/174), disponible à l'adresse suivante : http://undocs.org/fr/A/70/172.

GFCE-Meridian 2016, Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers, disponible à l'adresse suivante : www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

Japon 2015, Cyber Security Strategy, disponible à l'adresse suivante : www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

AIEA 2013, Établissement de l'infrastructure de sécurité nucléaire pour un programme électronucléaire – Guide d'application, disponible à l'adresse suivante : https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1591_F_web.pdf

AIEA 2017, Plan sur la sécurité nucléaire pour 2018-2021, doc. GC (61)/24, disponible à l'adresse suivante : https://www-legacy.iaea.org/About/Policy/GC/GC61/GC61Documents/French/gc61-24_fr.pdf

Kolesnikova 2017, Challenges for PPP in time of new types of security threats, World Security Report, disponible à l'adresse suivante : www.worldsecurity-index.com/

Lindberg & Sundelius 2013, Whole-Of-Society Disaster Resilience: The Swedish Way, dans "The McGraw-Hill Homeland Security Handbook" (2e édition)/[ed] David Kamien, New York: McGraw-Hill, disponible à l'adresse suivante : www.msb.se/Upload/Nyheter_press/McGraw-

Hill%20Homeland%20Security%20Handbook,%20Helena%20Lindberg%20and%20Bengt%20Sundelius.pdf

McAfee 2011, In the Dark: Critical Industries Confront Cyberattacks, deuxième rapport annuel de McAfee sur les infrastructures critiques, disponible à l'adresse suivante : www.mcafee.com/in/about/news/2011/q2/20110419-01.aspx

Michel-Kerjan 2018, Financial Protection of Critical Infrastructure : Uncertainty, Insurability and Terrorism Risk, Institut Veolia Environnement, disponible à l'adresse suivante : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.1268&rep=rep1&type=pdf

NIPC 2002, Terrorist Interest in Water Supply and SCADA Systems, Bulletin d'information 02-001, 30 janvier.

NIPP 2013, Partnering for Critical Infrastructure Security and Resilience, Département de la sécurité du territoire, 2013, p. 15, disponible à l'adresse suivante : https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

OCDE 2008, Recommandation du Conseil sur la protection des infrastructures d'information critiques, C(2008)35, disponible à l'adresse suivante : https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0361

OSCE 2013, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, 2013, disponible à l'adresse suivante : www.osce.org/atu/103500?download=true

OIAC 2016, Needs and Best Practices on Chemical Safety and Security Management, disponible à l'adresse suivante : www.opcw.org/fileadmin/OPCW/ICA/ICB/OPCW_Report_on_Needs_and_Best_Practices_on_Chemical_Safety_and_Security_ManagementV3-2_1.2.pdf

RECIPE 2011, Good Practices Manual for CIP Policies for Policy Makers in Europe, disponible à l'adresse suivante : https://repository.tudelft.nl/search/tno/?q=title%3A%22RECIPE%20%3A%20Good%20practices%20manual%20for%20CIP%20policies%2C%20for%20policy%20makers%20in%20Europe%22

Shea 2003, Critical Infrastructure: Control Systems and the Terrorist Threat, Congressional Research Service, disponible à l'adresse suivante : https://fas.org/irp/crs/RL31534.pdf

Sinai 2016, New Trends in Terrorism's Targeting of the Business Sector, The Mackenzie Institute, disponible à l'adresse suivante : http://mackenzieinstitute.com/new-trends-in-terrorisms-targeting-of-the-business-sector/#reference-27

Suède 2014, Guide to Increased Security in Industrial Information and Control Systems, Civil Contingencies Agency, disponible à l'adresse suivante : https://www.msb.se/RibData/Filer/pdf/27473.pdf

Suède 2016, National Risk and Capability Assessment, Civil Contingency Agency, disponible à l'adresse suivante : www.msb.se/Upload/Forebyggande/Krisberedskap/National%20risk%20and%20capability%20assessment%202016%20-%20Summary%20English.pdf

Pays-Bas 2018, Resilient Critical Infrastructure, National Coordinator for Security and Counterterrorism, Ministère de la justice et de la sécurité, disponible à l'adresse suivante : https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf

Ukraine 2017, Developing the Critical Infrastructure Protection System in Ukraine, Institut national d'études stratégiques, disponible à l'adresse suivante : http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf

UNISDR 2009, Terminologie pour la prévention des risques de catastrophe, disponible à l'adresse suivante : https://www.unisdr.org/files/7817_UNISDRTerminologyFrench.pdf

UP KRITIS 2014, Public-Private Partnership for Critical Infrastructure Protection – Basis and Goals, disponible à l'adresse suivante : www.upkritis.de

Vishwanath 2015, The Water Wars Waged by the Islamic State, Stratfor, disponible à l'adresse suivante : www.stratfor.com/weekly/water-wars-waged-islamic-state

ANNEXE I – PRATIQUES NATIONALES EN MATIERE DE PROTECTION DES INFRASTRUCTURES ESSENTIELLES CONTRE LES ATTAQUES TERRORISTES [46]

Country	Title	Type	Description	Year	Web address
Australie	Résilience des infrastructures essentielles : Plan	Stratégie/Document de politique générale	Vise à soutenir le fonctionnement continu de CI face à tous les dangers. Les principaux résultats visés par la stratégie sont les suivants : 1. Un partenariat solide et efficace entre les entreprises et les gouvernements ; 2. amélioration de la gestion des risques de l'environnement d'exploitation ; 3. compréhension et gestion efficaces des questions stratégiques ; et 4. Une compréhension et une application mûres de la résilience organisationnelle. Le document décrit les activités principales qui seront entreprises au niveau national pour atteindre ces résultats.	2015	https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF
Australie	Lignes directrices nationales pour la protection des infrastructures essentielles contre le terrorisme	Stratégie/Document de politique générale	Compléter la stratégie de résilience des infrastructures essentielles en fournissant un cadre pour une approche nationale de la protection des infrastructures essentielles contre le terrorisme.	2015	https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf
Australie	Stratégie australienne de cybersécurité	Stratégie/Document de politique générale	Cette stratégie de cybersécurité présente la philosophie et le programme du gouvernement australien visant à relever le double défi de l'ère numérique, à savoir faire progresser et protéger les intérêts de l'Australie en ligne. Cette stratégie définit cinq thèmes d'action pour la cybersécurité en Australie au cours des quatre prochaines années jusqu'en 2020 : un cyber-partenariat national, des cyberdéfenses puissantes, une responsabilité et une influence mondiales, une croissance et une innovation, une nation cyber-intelligente.	2016	https://cybersecuritystrategy.pmc.gov.au/index.html

[46] Les documents affichés dans cette annexe ne constituent pas une liste complète des ressources gouvernementales existantes dans CIP. Les matériaux ont été sélectionnés sur la base de leur pertinence, de leur accès ouvert et complet sur le Web, de leur représentation géographique et de la disponibilité des traductions en anglais.

Belgique	Loi du 1er juillet 2011 sur la sécurité et la protection des infrastructures essentielles	Instrument normatif	Conjointement avec l'arrêté royal du 2 décembre 2011 relatif aux infrastructures essentielles dans le sous-secteur du transport aérien, cette loi constitue la transposition de la directive 2008/114 / CE du Conseil du 8 décembre 2008.	2011	https://centredecrise.be/sites/default/files/loi_du_1er_juillet_2011_sur_les_ic_0.pdf
Canada	Cadre de gestion des urgences pour le Canada	Stratégie/Document de politique générale	Établit une approche commune pour les diverses initiatives de gestion des urgences fédérales, provinciales et territoriales (FPT). Le cadre vise à permettre la consolidation du travail collaboratif FPT et à garantir des actions plus cohérentes et complémentaires entre les différentes initiatives gouvernementales FPT. Il souligne les éléments clés de la gestion des urgences. Le cadre introduit également de nouveaux termes et révise les définitions existantes pour des termes en évolution tels que « tous risques » et « résilience » afin de refléter les développements contemporains dans le domaine de la gestion des urgences.	2011	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/mrgnc-mngmnt-frmwrk-eng.pdf
Canada	Stratégie de cybersécurité	Stratégie/Document de politique générale	Vise à renforcer les systèmes informatiques et les secteurs des infrastructures essentielles en s'appuyant sur trois piliers : la sécurité des systèmes gouvernementaux ; Établir des partenariats pour sécuriser des systèmes informatiques essentiels en dehors du gouvernement fédéral ; Aider les Canadiens à être en sécurité en ligne.	2010	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
Canada	Stratégie nationale pour les infrastructures essentielles	Stratégie/Document de politique générale	Sur la base des principes du cadre de gestion des urgences, la stratégie propose que les gouvernements fédéral, provinciaux et territoriaux et les secteurs d'infrastructures essentielles collaborent afin de renforcer la résilience des infrastructures essentielles au Canada. La collaboration se réalise à travers l'établissement de partenariats reposant sur les mandats et les responsabilités existants. Pour favoriser ces partenariats, la stratégie décrit les mécanismes permettant d'améliorer l'échange d'informations et la protection de l'information et identifie l'importance d'une approche de gestion des risques.	2009	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

Canada	Plan d'action pour les infrastructures essentielles (2014-2017)	Stratégie/Document de politique générale	S'appuie sur le plan d'action initial de 2010 en définissant davantage les mesures à prendre pour chacun des objectifs énoncés dans la Stratégie nationale sur les infrastructures essentielles.	2014	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf
Canada	Centre de réponse aux incidents cybernétiques (CCRIC)	Centre de coordination	Le CCRIC est le centre national de coordination chargé de réduire les cyber-risques auxquels sont exposés les systèmes et services clés du Canada. Le CCRIC collabore avec le Département de Sécurité publique Canada en partenariat avec les provinces, les territoires, les municipalités, les organisations du secteur privé et leurs homologues internationaux. Il coordonne la réponse nationale à tout incident grave de cybersécurité.		www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx
Canada / Etats-Unis d'Amérique	Accord de coopération concernant la gestion des urgences	Accord international	Établit les principes de la coopération bilatérale mutuelle en cas d'urgence. Il crée le groupe consultatif canado-américain.	2008	www.treaty-accord.gc.ca/text-texte.aspx?id=105173
Canada / Etats-Unis d'Amérique	Cadre pour la circulation des biens et des personnes à la frontière pendant et après une urgence	Document stratégique / politique	Énonce les principes de communication et de gestion des frontières en cas d'incident (y compris les actes explicitement terroristes) qui contribuent à une perturbation importante des frontières.		www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cnd-ntd-stts-frmwrk-en.aspx
Canada/ Etats-Unis d'Amérique	Plan d'action pour les infrastructures essentielles	Stratégie/Document de politique générale	Vise à traiter plus efficacement une série de problèmes liés aux infrastructures essentielles transfrontalières et à travailler conjointement pour échanger des informations / les meilleures pratiques, identifier les interdépendances et mener des actions communes.	2010	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx
Canada / Etats-Unis d'Amérique	Accord de coopération concernant la gestion des urgences	Accord international	Établit les principes de la coopération bilatérale mutuelle en cas d'urgence. Il crée le groupe consultatif canado-américain	2008	www.treaty-accord.gc.ca/text-texte.aspx?id=105173
Canada / Etats-Unis d'Amérique	Accord de coopération concernant la gestion des urgences	Stratégie/Document de politique générale	Énonce les principes de communication et de gestion des frontières en cas d'incident (y compris les actes explicitement terroristes) qui		www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cnd-ntd-

			contribuent à une perturbation importante des frontières.		stts-frmwrk-en.aspx
Canada/ Etats-Unis d'Amérique	Plan d'action sur les infrastructures essentielles	Stratégie/Document de politique générale	Vise à traiter plus efficacement une série de problèmes liés aux infrastructures essentielles transfrontalières et à travailler conjointement pour échanger des informations / les meilleures pratiques, identifier les interdépendances et mener des actions communes.	2010	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx
Chine	Règlement sur la sécurité et la protection de l'infrastructure d'information essentielle (Brouillon)	Instrument normatif	Premier projet de loi nationale visant à définir la politique de la Chine en matière de protection des infrastructures essentielles en matière d'information.	2017	https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/ (Unofficial English translation)
France	Décret No 2007-585 du 23 avril 2007 relatif à certaines dispositions réglementaires de la première partie du code de la défense	Instrument normatif	Modifie le code de la défense en introduisant un ensemble d'articles établissant le cadre institutionnel de la protection des activités d'importance vitale (voir articles R. 1332-1 à 1332-42).	2007	https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B3D2B93BA4D5B3162AC56B149F71F4EC.tplgfr30s_3?cidTexte=JORFTEXT000000615627&dateTexte=20070424
France	Livre Blanc – Défense et sécurité nationale	Stratégie/Document de politique générale	Présente les principes de base pour la protection des infrastructures essentielles dans le cadre plus large de l'approche française en matière de sécurité nationale	2013	http://www.livreblanc defense etsecurite.gouv.fr/pdf/the_white_paper_defence_2013.pdf
France	Instruction générale interministérielle relative à la sécurité des activités d'importance vitale (n°6600/SGDSN/PSE/PSN	Instrument normatif	Adoptée par le Secrétariat général à la défense et à la sécurité nationale, cette instruction contient des dispositions relatives à la mise en œuvre de l'architecture institutionnelle de la France en matière de protection des infrastructures essentielles.	2014	http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

	du 7 janvier 2014)				
France	Stratégie nationale pour la sécurité numérique	Stratégie/Document de politique générale	Définit les objectifs stratégiques et l'approche institutionnelle visant à assurer la résilience de la France contre les menaces cybernétiques, y compris les menaces contre les infrastructures essentielles en matière d'information.	2015	https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
France	Plan Vigipirate	Stratégie/Document de politique générale	Prévoit 300 mesures couvrant 13 domaines d'action principaux tels que les transports, la santé et les réseaux. Les mesures peuvent être activées en fonction de l'évolution de la menace et des vulnérabilités. Sur la base de l'évaluation de la menace terroriste faite par les services de renseignement, le Secrétariat général à la défense et à la sécurité nationale émet des lignes directrices déterminant les mesures à prendre par les acteurs concernés en matière de vigilance, de prévention et de protection contre les menaces d'action terroriste. Les opérateurs d'infrastructure doivent traduire les mesures du plan VIGIPIRATE dans leurs propres plans de sécurité.	2015	http://www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd_0.pdf
Allemagne	Stratégie nationale pour la protection des infrastructures essentielles	Stratégie/Document de politique générale	Résume les buts et objectifs de l'Administration Fédérale et son approche politico-stratégique. La stratégie est également le point de départ pour consolider les résultats obtenus jusqu'à présent et pour les développer davantage compte tenu des défis nouveaux.	2009	https://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile
Allemagne	Protection des infrastructures essentielles - Concept de protection de base - Recommandations pour les entreprises	Lignes directrices/ Manuel pratique	Elaboré par le ministère Fédéral de l'Intérieur, l'Office fédéral de la protection de la population et des catastrophes et l'Office fédéral de la police criminelle, doté de l'expertise du monde des affaires, le document fournit aux entreprises allemandes des recommandations relatives à la sécurité intérieure.	2006	https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/Baseline%20Protection%20Concept.pdf?__blob=publicationFile
Allemagne	Stratégie de cybersécurité de l'Allemagne	Stratégie/Document de politique générale	Fournit les axes de la politique nationale en matière de cybersécurité.	2011	https://www.cio.bund.de/SharedDocs/

					Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
Allemagne	Plan national de protection des infrastructures d'information	Stratégie/Document de politique générale	Vise à la protection intégrale des infrastructures essentielles en matière d'information en Allemagne en fixant trois objectifs stratégiques : prévention, préparation, durabilité.	2005	http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf
Allemagne	Plan de mise en œuvre du plan national de protection des infrastructures d'information	Stratégie/Document de politique générale	Le plan de mise en œuvre est une directive de sécurité informatique destinée aux opérateurs d'infrastructure de confiance. Il vise à faciliter la prise de décisions politiques et la coopération nationale et internationale. Il est recommandé aux entreprises de mettre en place un niveau de sécurité informatique adéquat.		https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation%20Plan.pdf?__blob=publicationFile
Allemagne	UP Kritis - Partenariat public-privé pour la protection des infrastructures essentielles	Stratégie/Document de politique générale	Aperçu des réalisations et nouvelle vision du programme allemand de partenariat public-privé en matière de protection des infrastructures essentielles.	2014	https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile
Japon	Eléments politiques de base sur les infrastructures essentielles en matière d'information	Stratégie/Document de politique générale	Établi pour servir de base à la politique relative aux mesures de sécurité de l'information concernant les infrastructures essentielles du Japon.	2015	https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_engv3_r1.pdf

Japon	Stratégie de cybersécurité	Fiche descriptive	Établit les priorités et les objectifs nationaux en matière de cybersécurité et consacre une section à la protection des infrastructures essentielles en matière d'information.	2015	https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf
Japon	Stratégie nationale de sécurité	Stratégie/Document de politique générale	Établit les approches fondamentales du pays en matière de sécurité nationale et ses objectifs. Bien qu'il ne se réfère pas directement aux infrastructures essentielles, la Stratégie prévoit le renforcement des mesures ayant un impact direct sur les infrastructures essentielles, telles que le renforcement de la sécurité maritime et de la cybersécurité, les capacités de renseignement, etc.	2013	http://www.mofa.go.jp/fp/nsp/page1we_000081.html
Japon	Loi fondamentale sur la cybersécurité	Acte normatif	La première loi spécifique à la cybersécurité adoptée par les pays du G7. Cette loi prescrit, outre les obligations en matière de cybersécurité de l'État et des autorités locales, les obligations en matière de cybersécurité des opérateurs d'infrastructure de confiance, des universités et d'autres établissements d'enseignement ou de recherche du secteur économique. La loi envisage qu'à l'avenir, des obligations plus spécifiques pour les exploitants du secteur soient définies par des lois plus spécifiques.	2014	http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=02&id=2760
Malaisie	Portail - CNII	Centre de coordination	Portail en ligne dans lequel les exploitants d'infrastructures essentielles travaillent ensemble en partageant des informations sur les problèmes de sécurité. Il fournit des informations sur la politique nationale en matière de cybersécurité, qui vise à réduire les risques pesant sur l'infrastructure nationale d'information essentielles (CNII) dans dix secteurs essentielles.		https://cnii.cybersecurity.my/main/index.html
Pays-Bas	Resilient Critical Infrastructure	Brochure explicative / Fiche descriptive	Préparée par le Coordonnateur national pour la sécurité et la lutte contre le terrorisme, la fiche d'information illustre le changement intervenu en 2014 dans l'approche suivie par le gouvernement dans sa politique en matière de protection de l'information et des politiques.	2018	https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf

Nouvelle-Zélande	Manuel sur le système de sécurité nationale	Stratégie/Document de politique générale	Présente les arrangements de la Nouvelle-Zélande concernant à la fois la gouvernance de la sécurité nationale et la réaction à une crise de sécurité nationale potentielle, émergente ou réelle. Le document est divisé en quatre sections : • Partie 1 : Le système de sécurité nationale ; • Partie 2: structures de gouvernance de la sécurité nationale; • Partie 3: Réponse à un événement potentiel, émergent ou réel. • Partie 4 : Annexes annexes.	2016	www.dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf
Nouvelle-Zélande	Stratégie de cybersécurité	Stratégie/Document de politique générale	Établit les priorités et les objectifs nationaux en matière de cybersécurité et consacre une section à la protection des infrastructures essentielles en matière d'information.	2015	www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf
Nouvelle-Zélande	Centre national de cybersécurité	Centre de coordination	Établi en 2011, ce centre a pour objectif de fournir des conseils de sécurité spécialisés et un soutien aux organisations et systèmes d'information les plus importants de Nouvelle-Zélande. Cela inclut les ministères, les principaux producteurs d'économie, les exportateurs spécialisés, les instituts de recherche et les exploitants d'infrastructures nationales essentielles. Le NCSC aide ces entités à protéger leurs réseaux des types de menaces qui dépassent généralement la capacité des outils disponibles sur le marché et des menaces susceptibles d'affecter le fonctionnement efficace de l'administration publique ou des secteurs économiques clés.	2011	https://www.ncsc.govt.nz/
Nouvelle-Zélande	Stratégie de cybersécurité : rapport annuel du plan d'action	Document politique / Rapport	Appuie la stratégie en matière de cybersécurité en définissant des mesures concrètes pour protéger les systèmes informatiques du pays.	2015	www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf
Nouvelle-Zélande	Stratégie de cybersécurité : rapport annuel du plan d'action	Document politique / Rapport report	Il s'agit du premier rapport annuel sur la mise en œuvre des objectifs énoncés dans la stratégie et le plan d'action de 2015 en matière de cybersécurité.	2016	www.dpmc.govt.nz/sites/default/files/2017-06/nzcss-action-plan-annual-

					report-2016.pdf
Pologne	Programme national de protection des infrastructures essentielles	Stratégie/Document de politique générale	Présente les concepts de base de la protection des infrastructures essentielles en Pologne et la répartition des tâches entre les parties prenantes sur la base des principes juridiques et des définitions contenus dans la loi de 2007 sur la gestion des crises.	2015	http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf
Pologne	Stratégie de sécurité nationale	Stratégie/Document de politique générale	Identifie les intérêts nationaux et les objectifs stratégiques dans le domaine de la sécurité. Dans sa section « Actions de protection », la stratégie de sécurité nationale mentionne explicitement la protection des infrastructures essentielles.	2014	https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf
Russie	Loi sur la sécurité des infrastructures essentielles en matière d'information	Normative instrument	Etablit les fondements et les principes de base pour assurer la sécurité des infrastructures essentielles russes, y compris les fondements du fonctionnement du système étatique de détection, de prévention et de liquidation des conséquences des cyberattaques contre les ressources informatiques de la Fédération de Russie. Il s'agit d'un système unifié, distribué dans tout le pays et doté des capacités et des ressources nécessaires pour détecter, prévenir et liquider les conséquences des cyberattaques et réagir aux cyber-incidents. La loi fédérale définit le mécanisme de prévention des cyber incidents liés à des éléments importants des infrastructures essentielles en matière d'information. Il définit les pouvoirs des organes de l'Etat pour assurer la sécurité des infrastructures essentielles en matière d'information, ainsi que les droits et obligations des différents acteurs dans ce domaine.	2017	http://en.kremlin.ru/acts/news/55146
Sénégal	Stratégie nationale de cybersécurité	Stratégie/Document de politique générale	Comprend les éléments suivants : -une évaluation du contexte stratégique de la cybersécurité au Sénégal, y compris des menaces actuelles et futures ; - vision du gouvernement sur la cybersécurité et objectifs stratégiques à atteindre ; Principes généraux, rôles et responsabilités susceptibles de renforcer ladite stratégie ; -le cadre logique pour sa mise en œuvre.	2017	www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf

			L'objectif stratégique 2 porte spécifiquement sur « le renforcement des systèmes d'information essentiels à la protection des infrastructures et des systèmes d'information de l'État du Sénégal».		
Singapour	Stratégie nationale de cybersécurité	Stratégie/Document de politique générale	Définit les priorités de Singapour en matière de sécurité et la stratégie adoptée pour lutter contre le terrorisme. Le document établit l'architecture de la sécurité nationale, qui organise les diverses agences autour des trois piliers essentiels de la sécurité que sont la politique, les opérations et le développement des capacités, ainsi que le rôle de coordination d'un secrétariat de coordination de la sécurité nationale.	2004	https://www.nscs.gov.sg/public/download.ashx?id=1031
Singapour	Stratégie de cybersécurité	Stratégie/Document de politique générale	Définit la vision, les objectifs et les priorités de Singapour en matière de cybersécurité, notamment sur le renforcement de la résilience des infrastructures essentielles en matière d'information.	2016	https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecurity strategy.pdf
Singapour	Agence de cybersécurité	Centre de coordination	Supervise la stratégie de cybersécurité du pays. Le Centre fait partie du bureau du Premier ministre et est géré par le ministère des Communications et de l'Information. L'un de ses objectifs est de protéger des secteurs essentielles tels que l'énergie, l'eau et les banques.		https://www.csa.gov.sg/
Singapour	Projet de loi sur la protection des infrastructures	Instrument normatif	Introduit dans le cadre de la stratégie antiterroriste du Ministère de l'intérieur visant à protéger les bâtiments abritant des services essentiels ou à fort trafic humain. Il vise à garantir que des mesures de sécurité adéquates sont mises en place afin de dissuader les agresseurs et de les en empêcher, ainsi que de minimiser les pertes et les dommages résultant d'une attaque.	2017	file:///Users/SM/Downloads/Infrastructure%20Protection%20Bill.pdf
Singapour	Projet de loi sur la cybersécurité	Instrument législatif	Le projet de loi poursuit quatre objectifs : - Fournir un cadre pour la réglementation des infrastructures essentielles en matière d'information permettant de formaliser les obligations des propriétaires d'infrastructures essentielles en matière d'information en assurant leur cybersécurité. - Donner à la Cyber Security Agency (CSA) les pouvoirs nécessaires pour	2017	https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en

			gérer les menaces et les incidents liés à la cybersécurité et y faire face. - Établir un cadre pour le partage d'informations de cybersécurité avec et par le CSA et la protection de ces informations. - Établir un cadre d'agrément «allégé » pour les fournisseurs de services de cybersécurité.		
Espagne	Loi No 8/2011 instituant des mesures de protection à l'égard des établissements de crédit (en espagnol)	Instrument normatif	Vocation de la loi à coordonner les actions de tous les organismes publics et à promouvoir la collaboration et la participation des propriétaires et des exploitants d'infrastructure de crédit. La loi transpose dans la législation nationale les mesures incluses dans la directive 2008/114 / CE, en particulier l'identification et la classification des infrastructures essentielles européennes.	2011	http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf
Espagne	Décret royal 704/2011 portant approbation du règlement relatif à la protection des infrastructures essentielles (en espagnol)	Instrument normatif	Mise en œuvre des dispositions-cadres contenues dans la loi 8/2011.	2011	http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf
Espagne	Centre national sur la protection des infrastructures essentielles et la cybersécurité	Centre de coordination	Organe ministériel chargé de promouvoir, de coordonner et de superviser toutes les activités confiées par le ministère de l'Intérieur en matière de PIC sur le territoire national.	2007	http://www.cnpic.es/index.html
Espagne	Stratégie de sécurité nationale (en espagnol)	Document stratégique / politique	Les menaces pesant sur l'IC sont pleinement intégrées au document en tant que menaces à la sécurité nationale.	2017	http://www.cnpic.es/Biblioteca/Eventos/Estrategia_Seguriad_Nacional_2017.pdf
Espagne	Stratégie nationale de cybersécurité (en espagnol)	Document stratégique / politique	Définit les objectifs et les approches de la stratégie espagnole, parmi lesquels ceux qui sont pertinents pour la protection des infrastructures en matière d'information.	2013	https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Suède	Plan d'action ''for the Protection of Vital Societal Functions and Critical Infrastructures"	Document stratégique / politique	Préparé par l'Agence suédoise de protection civile, le plan d'action crée des conditions permettant à toutes les fonctions sociales essentielles et aux infrastructures essentielles de mettre en œuvre un travail de sécurité systématique dans leurs opérations aux niveaux local, régional et national d'ici 2020.	2014	https://www.msb.se/RibData/Filer/pdf/27412.pdf
Suède	Guide pour une sécurité accrue des systèmes d'information et de contrôle industriels	Stratégie/Document de politique générale	Préparé par l'Agence suédoise de protection civile, le guide contient 17 recommandations de base pour accroître la sécurité et, grâce à sa large diffusion, a atteint son statut de Norme dans l'industrie suédoise. Les recommandations sont basées sur des normes, pratiques et méthodes de travail reconnues sur le plan international.	2014	https://www.msb.se/RibData/Filer/pdf/27473.pdf
Suède	Évaluation nationale des risques et des capacités	Stratégie/Document de politique générale	Présentée chaque année par « the Civil Contingency Agency » au gouvernement, l'Évaluation fournit un terrain stratégique pour l'orientation et le développement ultérieur des contingents civils.	2016	https://www.msb.se/en/Prevention/National-risk-and-capability-assessment/
Suisse	Stratégie nationale pour les PIC (Protection des infrastructures essentielles) 2018-2022	Stratégie/Document de politique générale	Adoptée par l'Office fédéral de la protection de la population, elle actualise la stratégie initiale publiée en 2012 en fixant des objectifs plus ambitieux pour ses parties prenantes. La stratégie révisée est censée traduire le travail accompli en un processus institutionnalisé, le fixer dans la législation et le compléter sur une base ad hoc.	2017	https://www.babs.admin.ch/fr/aufgabenbabs/ski.html
Suisse	Stratégie nationale de protection contre les cyber-risques	Stratégie/Document de politique générale	Par cette stratégie, le Conseil fédéral, en étroite collaboration avec les milieux d'affaires et les exploitants d'infrastructures essentielles, cherche à réduire les cyber-risques auxquels tous ces acteurs sont quotidiennement exposés. La stratégie comprend 16 mesures à mettre en œuvre jusqu'en 2017. Une nouvelle stratégie entrera en vigueur en 2018.	2012	https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html
Royaume-Uni	Stratégie de sécurité nationale	Stratégie/Document de politique générale	Expose les piliers et les objectifs de la vision du pays en matière de protection de la sécurité nationale. Le document consacre une section aux infrastructures essentielles.	2015	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/

					52309_Cm_9161_NSS_SD_Review_web_only.pdf
Royaume-Uni	Centre pour la protection des infrastructures nationales	Centre de coordination	Fournit des conseils en matière de protection et de sécurité aux entreprises et aux organisations à l'échelle de l'infrastructure nationale. Les conseils visent à réduire la vulnérabilité des établissements de crédit face au terrorisme et à d'autres menaces.	2007	https://www.cpni.gov.uk/
Royaume-Uni	Centre national de cybersécurité	Centre de coordination	Fournit des conseils et du soutien aux secteurs public et privé sur la façon d'éviter les menaces à la sécurité informatique.	2016	https://www.ncsc.gov.uk/
Royaume-Uni	Plan de sécurité et de résilience du secteur pour l'année 2017	Stratégie/Document de politique générale	Définit la résilience de l'infrastructure la plus importante du Royaume-Uni face aux risques identifiés dans l'évaluation nationale des risques. Élaborés chaque année, des plans sont soumis aux ministres pour les alerter sur les vulnérabilités perçues, avec un programme de mesures visant à améliorer la résilience si nécessaire. Les plans individuels sont classifiés, mais le Cabinet Office résume chaque version en un plan global de résilience sectorielle pour les infrastructures essentielles.	2017	https://www.gov.uk/government/collections/sector-resilience-plans
Royaume-Uni	Registre national des risques d'urgences civiles	Document politique (version publique)	Fournit une vue d'ensemble des principaux risques susceptibles de causer des perturbations importantes au Royaume-Uni. Explique les types de situations d'urgence qui pourraient survenir, ce que le gouvernement et ses partenaires font pour les atténuer et comment, en tant que particuliers, familles ou petites entreprises, l'on peut contribuer. Un certain nombre de sections traitent directement de la protection des infrastructures essentielles contre les actes malveillants et terroristes.	2017	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf
Ukraine	Livre vert sur la protection des infrastructures essentielles en Ukraine	Stratégie/Document de politique générale	Formuler des objectifs stratégiques de politique publique dans le domaine de la protection des infrastructures essentielles en Ukraine.	2015	http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf
Ukraine	Décision du Conseil national de sécurité et de	Instrument normatif	Fixe un calendrier pour la mise en place progressive d'une politique nationale globale de protection des	2016	http://en.niss.gov.ua/content/articles/files/niss_Engl

	défense relative à l'amélioration des mesures visant à assurer la protection des infrastructures essentielles (mise en œuvre par décret présidentiel du 16 janvier 2016 n° 8/2017)		infrastructures essentielles et d'un cadre juridique complet en la matière		Collection _druk-24cce.pdf
Etats-Unis d'Amérique	Évaluation stratégique nationale des risques	Stratégie/Document de politique générale	Menée par le Secrétaire à la Sécurité intérieure, elle vise à identifier les types d'incidents qui représentent la plus grande menace pour la sécurité intérieure de la nation. Les actifs, les systèmes et les réseaux essentiels font face à bon nombre des menaces catégorisées, y compris les terroristes et les autres acteurs qui cherchent à causer du tort et à perturber les services essentiels.	2011	https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
Etats-Unis d'Amérique	Plan national de protection des infrastructures (PNPI)	Stratégie/Document de politique générale	Décrit comment le gouvernement et les participants du secteur privé de la communauté des infrastructures essentielles travaillent ensemble pour gérer les risques et obtenir des résultats en matière de sécurité et de résilience.	2013	https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
Etats-Unis d'Amérique	Directive de politique présidentielle 21 (PPD-21) : Sécurité et résilience des infrastructures essentielles	Instrument normatif	Charge le pouvoir exécutif de : -Développer une capacité de connaissance de la situation qui aborde les aspects physiques et cybernétiques du fonctionnement de l'infrastructure en temps quasi réel. -Comprendre les conséquences en cascade des défaillances de l'infrastructure -Évaluer et faire mûrir le partenariat public-privé -Mettre à jour le Plan national de protection des infrastructures -Élaborer un plan complet de recherche et de développement	2013	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Etats-Unis d'Amérique	Décret-loi (OT) 13636 : Amélioration de la cybersécurité des infrastructures essentielles	Instrument normatif	Charge le pouvoir exécutif de : -Élaborer un cadre de cybersécurité volontaire neutre sur le plan technologique. -Promouvoir et encourager l'adoption de pratiques en matière de cybersécurité -Augmenter le volume, l'actualité et la qualité de l'échange d'information sur les cybermenaces. -Intégrer de solides mesures de protection de la vie privée et des libertés civiles dans toutes les initiatives visant à protéger nos infrastructures essentielles. -Explorer l'utilisation de la réglementation existante pour promouvoir la cybersécurité	2013	https://obamawhite house.archives. gov/the-press-office/2013/ 02/12 /executive-order-improving-critical-infrastructure-cyber security
Etats-Unis d'Amérique	Le défi de la sécurité et de la résilience du PPNI	Mécanisme de financement	Permet à la collectivité des infrastructures essentielles de contribuer à l'élaboration de technologies, d'outils, de processus et de méthodes qui répondent aux besoins immédiats et renforcent la sécurité et la résilience à long terme des infrastructures critique. Il aide à identifier et à financer des idées novatrices qui peuvent fournir à la communauté des IC des technologies et des outils prêts ou presque prêts à l'emploi.	2017	https://www.dhs. gov/sites/default /files/publications /nipp-challenge-overview-fact-sheet -2017-508.pdf

ANNEXE II – LA RÉSOLUTION 2341 (2017) DU CONSEIL DE SÉCURITÉ

Le Conseil de sécurité,

Rappelant ses résolutions 1373 (2001), 1963 (2010), 2129 (2013) et 2322 (2016),

Réaffirmant qu'il tient de la Charte des Nations Unies la responsabilité principale du maintien de la paix et de la sécurité internationales,

Réaffirmant que, conformément à la Charte des Nations Unies, il respecte la souveraineté, l'intégrité territoriale et l'indépendance politique de tous les États,

Réaffirmant que le terrorisme, sous toutes ses formes et dans toutes ses manifestations, constitue une des menaces les plus graves pour la paix et la sécurité internationales et que tous les actes de terrorisme sont criminels et injustifiables, quels qu'en soient les motivations, le moment, le lieu et les auteurs, et *demeurant résolu* à contribuer encore à améliorer l'efficacité de l'action d'ensemble menée contre ce fléau à l'échelle mondiale,

Réaffirmant également que le terrorisme fait peser une menace sur la paix et la sécurité internationales et que pour lutter contre cette menace il faut mener une action collective aux niveaux national, régional et international dans le respect du droit international, y compris le droit international des droits de l'homme et le droit humanitaire international, et de la Charte des Nations Unies,

Réaffirmant en outre que le terrorisme ne doit être associé à aucune religion, nationalité ou civilisation ni à aucun groupe ethnique,

Soulignant que la participation et la collaboration actives de l'ensemble des États et organisations internationales, régionales et sous-régionales sont nécessaires pour contrer, affaiblir, isoler et neutraliser la menace terroriste, et *insistant* sur l'importance de l'application de la Stratégie antiterroriste mondiale des Nations Unies, qui figure dans la résolution 60/288 de l'Assemblée générale datée du 8 septembre 2006, et des examens ultérieurs de la Stratégie,

Réaffirmant qu'il faut prendre des mesures pour prévenir et combattre le terrorisme, notamment en privant les terroristes des moyens de mener à bien leurs attaques, comme souligné dans le deuxième volet de la Stratégie, qu'il faut aussi redoubler d'efforts pour améliorer la sécurité et la protection des cibles particulièrement vulnérables comme les infrastructures et les lieux publics, ainsi que la résilience face aux attaques terroristes, en particulier dans le domaine de la protection des civils, tout en étant conscient du fait que les États peuvent avoir besoin d'aide à cet égard,

Considérant que chaque État détermine quelles sont ses infrastructures critiques et les moyens de les protéger efficacement contre toute attaque terroriste,

Conscient qu'il importe plus que jamais de veiller à ce que les infrastructures critiques soient fiables et résilientes et d'assurer leur protection contre les attaques terroristes, pour préserver la sécurité nationale, l'ordre public et l'économie des États concernés ainsi que le bien-être et la qualité de vie de leur population,

Considérant que pour pouvoir faire face aux attaques terroristes, il faut mener des activités de prévention, de protection, d'atténuation des effets, d'intervention et de relèvement, en mettant l'accent sur la promotion de la sécurité et de la résilience des infrastructures critiques,

notamment par l'intermédiaire de partenariats entre secteur public et secteur privé, selon qu'il convient,

Conscient que la protection exige le déploiement d'efforts dans de nombreux domaines, qu'il s'agisse de la planification; de l'information du public et des systèmes d'alerte; de la coordination des opérations; du renseignement et de la mise en commun des informations; des efforts d'interdiction et de blocage; du dépistage, de la recherche et de la détection; du contrôle des accès et de la vérification d'identité; de la cybersécurité; des mesures de protection physique; de la gestion des risques pour les programmes et les activités de protection; ou de la sécurité et de l'intégrité de la chaîne d'approvisionnement,

Sachant que les communautés informées qui sont sur le qui-vive jouent un rôle essentiel en aidant à faire connaître et comprendre la menace terroriste existante, et en particulier en repérant les activités suspectes et en les signalant aux autorités de maintien de l'ordre, et qu'il importe de sensibiliser davantage le public au problème, de faire œuvre de mobilisation et de renforcer au besoin le partenariat entre secteur public et secteur privé, en particulier en ce qui concerne les menaces terroristes et les faiblesses potentielles, au moyen d'activités régulières de concertation, de formation et de communication à l'échelon national et local,

Notant l'existence de liens transfrontières de plus en plus forts entre les infrastructures critiques des pays, notamment en ce qui concerne la production, l'acheminement et la distribution de l'énergie, les transports aériens, terrestres et maritimes, les services bancaires et financiers, l'approvisionnement en eau, la distribution alimentaire et la santé publique,

Conscient que, en raison de l'interdépendance croissante des secteurs des infrastructures critiques, certaines peuvent être exposées à des menaces et des vulnérabilités toujours plus nombreuses et diverses qui posent de nouveaux problèmes sur le plan de la sécurité,

Constatant avec préoccupation que des attaques terroristes visant des infrastructures critiques pourraient considérablement perturber le fonctionnement du secteur public comme du secteur privé et avoir des répercussions au-delà du secteur des infrastructures,

Soulignant que la protection efficace des infrastructures critiques exige l'adoption d'approches sectorielles et intersectorielles de la gestion des risques et implique notamment d'identifier les menaces terroristes et de se préparer afin de limiter la vulnérabilité des infrastructures critiques, de prévenir et de déjouer si possible les complots terroristes qui les prennent pour cibles, de réduire au minimum les répercussions des attaques terroristes et les délais de reprise des activités en cas de dégâts causés par une telle attaque, d'identifier la cause des dégâts ou l'origine de l'attaque, de préserver les éléments de preuve de l'attaque et d'amener les responsables à répondre de leurs actes,

Considérant à cet égard que la protection des infrastructures critiques est beaucoup plus efficace lorsqu'elle repose sur une approche qui tient compte de l'ensemble des menaces et des dangers, notamment les attaques terroristes, et qu'elle est associée à des consultations et une coopération régulières et approfondies avec les opérateurs d'infrastructures critiques, avec les agents des forces de l'ordre et des forces de sécurité chargés de la protection des infrastructures critiques, et, le cas échéant, avec d'autres parties prenantes, y compris les propriétaires privés,

Considérant également que la protection des infrastructures critiques exige que soit instaurée une coopération à l'échelon national et transfrontalier avec les autorités publiques, les

partenaires étrangers, les propriétaires privés et les opérateurs de ces infrastructures, et que soient mis en commun leurs connaissances et leur expérience dans l'élaboration des politiques, leurs bonnes pratiques et les enseignements tirés de l'expérience,

Rappelant que dans sa résolution 1373 (2001), il a demandé aux États Membres de trouver les moyens d'intensifier et d'accélérer l'échange d'informations opérationnelles, concernant en particulier les actions ou les mouvements de terroristes ou de réseaux de terroristes, les documents de voyage contrefaits ou falsifiés, le trafic d'armes, d'explosifs ou de matières sensibles, l'utilisation des technologies de communication par des groupes terroristes, et la menace que constituent les armes de destruction massive en possession de groupes terroristes, et de coopérer, en particulier dans le cadre d'accords et d'arrangements bilatéraux et multilatéraux, afin de prévenir et de réprimer les actes de terrorisme,

Notant l'action menée dans le cadre des organisations, organismes, forums et réunions concernés aux niveaux international, régional et sous-régional en ce qui concerne le renforcement de la protection, de la sécurité et de la résilience des infrastructures critiques,

Se félicitant de la poursuite de la coopération dans la lutte contre le terrorisme entre le Comité contre le terrorisme et l'Organisation internationale de police criminelle (INTERPOL), l'Office des Nations Unies contre la drogue et le crime, notamment en matière d'assistance technique et de renforcement des capacités, et tous les autres organismes des Nations Unies, et *encourageant vivement* une collaboration plus étroite entre ceux-ci et l'Équipe spéciale de lutte contre le terrorisme en vue d'assurer la coordination et la cohérence d'ensemble de l'action antiterroriste menée par le système des Nations Unies,

1. *Engage* tous les États à faire des efforts concertés et coordonnés, notamment par l'intermédiaire de la coopération internationale, pour mener des activités de sensibilisation et faire mieux connaître et comprendre les défis posés par les attaques terroristes, de façon à être mieux préparés en cas d'attaque contre des infrastructures critiques;

2. *Demande* aux États Membres d'envisager d'élaborer des stratégies de réduction des risques posés par les attaques terroristes au regard des infrastructures critiques, ou d'améliorer celles qu'ils ont déjà adoptées, en prévoyant notamment d'évaluer et de faire mieux connaître les risques, de prendre des mesures de préparation, y compris pour intervenir de manière efficace en cas d'attaque, de favoriser une meilleure interopérabilité dans la gestion de la sécurité et des conséquences, et de faciliter des échanges fructueux entre toutes les parties prenantes concernées;

3. *Rappelle* que, dans sa résolution 1373 (2001), il a décidé que tous les États devaient ériger les actes de terrorisme en infractions graves dans la législation et la réglementation nationales et *demande* à tous les États Membres de veiller à affirmer la responsabilité pénale de ceux qui perpétuent des attaques terroristes visant à détruire les infrastructures critiques ou à les rendre inutilisables, ou qui se livrent à des activités de planification, de formation, de financement ou de soutien logistique en lien avec ces attaques;

4. *Demande* aux États Membres d'étudier les moyens d'échanger des informations utiles et de prendre une part active à la prévention des attaques terroristes, à la protection contre ces attaques, à l'atténuation de leurs effets, à la préparation à de telles attaques, aux enquêtes et

interventions menées en cas d'attaque et aux mesures de rétablissement d'un fonctionnement normal après une attaque terroriste visant ou pouvant viser des infrastructures critiques;

5. *Demande également* aux États de créer ou de renforcer les partenariats nationaux, régionaux et internationaux avec les parties prenantes, tant publiques que privées, selon qu'il conviendra, de mettre en commun leurs informations et leurs données d'expérience aux fins des activités de prévention, de protection, d'atténuation des effets, d'enquête, d'intervention et de rétablissement d'un fonctionnement normal en cas de dégâts causés par des attaques terroristes visant des infrastructures critiques, notamment au moyen de formations communes et de l'utilisation ou de la mise en place des réseaux de communication ou d'alerte d'urgence pertinents;

6. *Demande instamment* à tous les États de veiller à ce que tous leurs ministères, institutions et autres entités concernés collaborent étroitement et efficacement sur les questions de protection des infrastructures critiques contre les attaques terroristes;

7. *Engage* l'Organisation des Nations Unies ainsi que les États Membres et les organisations régionales et internationales concernées qui ont élaboré leurs propres stratégies de protection des infrastructures critiques à collaborer avec tous les États et les organisations internationales, régionales, sous-régionales et autres organismes compétents pour dégager et mettre en commun de bonnes pratiques et mesures en matière de gestion du risque d'attaques terroristes contre des infrastructures critiques;

8. *Affirme* que la coopération économique et les initiatives de développement aux niveaux régional et bilatéral contribuent de manière essentielle à assurer la stabilité et la prospérité régionales et, à cet égard, *demande* à tous les États d'envisager de renforcer leur coopération afin de protéger les infrastructures critiques, notamment les projets de connectivité régionale et les infrastructures transfrontières connexes, contre les attaques terroristes, selon qu'il conviendra, par des moyens bilatéraux et multilatéraux, de mise en commun des informations, d'évaluation des risques et de maintien de l'ordre;

9. *Demande instamment* aux États qui sont en mesure de le faire de contribuer de façon efficace et ciblée au renforcement des capacités, à la formation et à la fourniture d'autres ressources, à des services d'assistance technique, à des transferts de technologie et aux programmes nécessaires afin que tous les États puissent atteindre l'objectif de protection des infrastructures critiques contre les attaques terroristes;

10. *Demande* au Comité contre le terrorisme, avec le soutien de sa Direction exécutive, de continuer selon que de besoin, conformément à leurs mandats respectifs, d'examiner les efforts déployés par les États Membres pour protéger les infrastructures critiques contre les attaques terroristes dans le cadre de l'application de la résolution 1373 (2001), en vue de recenser les bonnes pratiques, les lacunes et les facteurs de vulnérabilité dans ce domaine;

11. *Encourage* à cet égard le Comité contre le terrorisme, avec le soutien de sa Direction exécutive, et l'Équipe spéciale de lutte contre le terrorisme à continuer de coopérer afin de faciliter l'apport d'une assistance technique en matière de protection des infrastructures critiques contre les attaques terroristes et le renforcement des capacités dans ce domaine, en faisant œuvre de sensibilisation au problème, en particulier en se concertant davantage avec les États et les organisations internationales, régionales et sous-régionales compétentes, et en

collaborant étroitement, notamment par des échanges d'informations, avec les prestataires d'une assistance technique bilatérale et multilatérale qui sont concernés;

12. *Encourage* le Groupe de travail sur la protection des infrastructures critiques y compris les cibles vulnérables, Internet et la sécurité du tourisme de l'Équipe spéciale de lutte contre le terrorisme à poursuivre son rôle en matière de facilitation et, en coopération avec d'autres institutions spécialisées des Nations Unies, à continuer d'apporter aux États Membres qui en feront la demande une assistance en matière de renforcement des capacités pour améliorer l'application des mesures;

13. *Prie* le Comité contre le terrorisme de lui rendre compte dans douze mois de l'application de la présente résolution;

14. *Décide* de rester saisi de la question.

ANNEXE III – PACTE MONDIAL DE COORDINATION CONTRE LE TERRORISME DES NATIONS UNIES

Le Secrétariat, les entités, les fonds et les programmes des Nations Unies, ainsi que les organisations affiliées, contribuent à l'application de la Stratégie antiterroriste mondiale de l'organisation des Nations Unies, tant dans le cadre de leurs mandats respectifs à travers de leur adhésion au Pacte mondial de coordination contre le terrorisme.

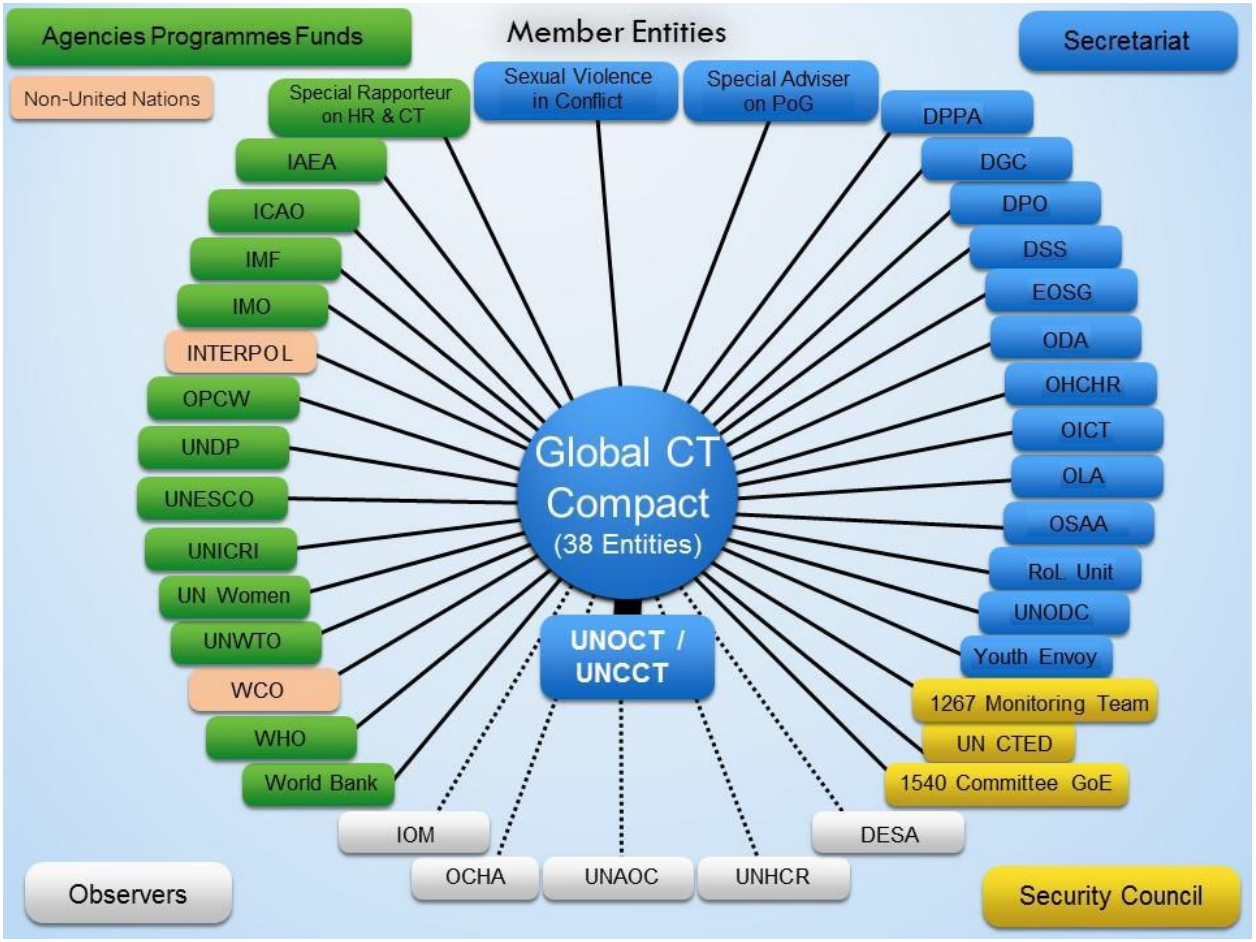
Le Pacte Mondial est composée de 38 entités internationales et d'INTERPOL, entités qui, en raison de leur travail, interviennent dans les efforts multilatéraux de lutte contre le terrorisme. Chaque entité cotise conformément à son propre mandat. Les membres du Pacte Mondial sont les suivants :

1. L'Équipe d'appui analytique et de surveillance des sanctions Nations Unies
2. Direction exécutive du Comité contre le terrorisme (DECT)
3. Département des opérations de paix (DPO)
4. Département des affaires politiques et consolidation de la paix (DPPA)
5. Département de la communication globale (DGC)
6. Département de la sûreté et de la sécurité des Nations Unies (DSS)
7. Groupe d'experts du Comité 1540
8. Agence internationale de l'énergie atomique (IAEA)
9. Organisation de l'Aviation civile internationale (OACI)
10. Organisation maritime internationale (OMI)
11. Fonds monétaire international (FMI)
12. Organisation internationale de police criminelle (INTERPOL)
13. Bureau des affaires de désarmement des Nations Unies (UNODA)
14. Bureau du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH)
15. Bureau des affaires juridiques (OLA)
16. Cabinet du Secrétaire général
17. Bureau du Conseiller spécial pour la prévention du génocide
18. Bureau de la Représentante spéciale du Secrétaire général des Nations Unies pour les enfants et les conflits armés
19. Bureau de la Représentante spéciale du Secrétaire général des Nations Unies sur les violences sexuelles en conflit
20. Bureau de l'Envoyée du Secrétaire général des Nations Unies pour la jeunesse
21. Organisation pour l'Interdiction des Armes Chimiques (OIAC)
22. Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
23. Programme des Nations Unies pour le développement (PNUD)
24. Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO)
25. Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI)
26. Office des Nations Unies contre la drogue et le crime (ONUDC)
27. Bureau du Conseiller spécial pour l'Afrique
28. Groupe de coordination et de conseil sur l'état de droit
29. ONU Femmes
30. Organisation mondiale du tourisme (OMT)
31. Organisation mondiale des douanes (OMD)

32. Banque mondiale
33. Organisation mondiale de la Santé (OMS)

OBSERVATEURS:

34. Organisation internationale pour les migrations (OIM)
35. Bureau de la coordination des affaires humanitaires (OCHA)
36. Département des affaires économiques et sociales (DAES)
37. Haut-Commissariat des Nations Unies pour les réfugiés (HCR)
38. Alliance des civilisations des Nations Unies



Au sein du Compact Mondial, un groupe de travail a été créé sur la protection des infrastructures essentielles, y compris les cibles vulnérables, l'Internet et la sécurité du tourisme.

Mandat :

Le mandat du Groupe de travail est basé sur la Stratégie antiterroriste mondiale de l'Organisation des Nations Unies. (A/RES60/288) :

- *« S'employer avec l'Organisation des Nations Unies, sans nuire à la confidentialité, dans le respect des droits de l'homme et conformément aux autres obligations prévues par le droit international, à explorer les moyens : a) De coordonner les efforts aux échelles internationale et régionale afin de contrer le terrorisme sous toutes ses formes et dans toutes ses manifestations sur l'Internet » (Section II, paragraphe 12)*

- *« Renforcer les efforts visant à améliorer la sécurité et la protection des cibles particulièrement vulnérables comme les infrastructures et les lieux publics, ainsi que les interventions en cas d'attaques terroristes et autres catastrophes, en particulier dans le domaine de la protection des civils, tout en reconnaissant que les États pourront avoir besoin d'une assistance à cet égard »* (*Section II, paragraphe 18)*

- *« Encourager l'Organisation des Nations Unies à collaborer avec les États Membres et les organisations internationales, régionales et infrarégionales compétentes pour dégager et mettre en commun les pratiques optimales permettant d'empêcher les attentats terroristes contre des cibles particulièrement vulnérables. Nous invitons l'Organisation internationale de police criminelle à collaborer avec le Secrétaire général pour qu'il puisse soumettre des propositions en ce sens. Nous reconnaissons par ailleurs qu'il importe de mettre en place dans ce domaine des partenariats public-privé. » (Section III, paragraphe 13)*

Considérant que la Stratégie antiterroriste mondiale réaffirme *« que la promotion et la protection des droits de l'homme pour tous et la primauté du droit »* sont *« essentielles à toutes les composantes de la Stratégie »*, le Groupe de travail intègre dans ses travaux la dimension des droits de l'homme.

Objectifs **:**

Les objectifs du Groupe de travail du Compact Mondial sur la protection des infrastructures essentielles, y compris les cibles vulnérables, l'Internet et la sécurité du tourisme, sont :

- de mettre en place des mécanismes appropriés pour faciliter le développement et le partage des meilleures pratiques en matière de protection des sites vulnérables, des espaces publics ou des infrastructures essentielles qui revêtent une importance pour leurs États et régions respectifs, ou qui sont d'importance internationale ;
- de renforcer les capacités des secteurs public et privé et d'accroître le développement de partenariats publics et privés pour la protection des infrastructures essentielles, y compris l'Internet et la sécurité de l'informatique et du tourisme, afin de prévenir et de réagir efficacement aux risques et menaces potentiels pour les installations connexes, notamment en faisant mieux connaître et comprendre l'équilibre nécessaire entre les questions économiques et de sécurité.
- d'améliorer la réactivité et la résilience en promouvant des méthodes de planification, de prévention, de gestion des crises et de récupération ;
- de promouvoir l'échange d'informations et de bonnes pratiques et mettre en place un réseau d'experts ;

- aider les États à mettre en œuvre les dispositions de la Stratégie antiterroriste mondiale de l'ONU qui sont pertinentes pour les domaines d'intervention du Groupe de travail (énumérés sous la rubrique « Mandat » ci-dessus).

Entités participantes :

- Organisation internationale de police criminelle (INTERPOL) (Président)
- Bureau de lutte contre le terrorisme (Co Président)
- Direction exécutive du Comité contre le terrorisme (DECT)
- L'Équipe d'appui analytique et de surveillance des sanctions Nations Unies
- Département de la communication globale (DGC)
- Bureau du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH)
- Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
- Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO)
- Office des Nations Unies contre la drogue et le crime / Service de la prévention du terrorisme (ONUDC/TPB)
- Département de la sûreté et de la sécurité des Nations Unies (DSS)
- Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI)
- Département des affaires politiques et consolidation de la paix (DPPA)
- Département des opérations de paix (DPO)
- Organisation de l'Aviation civile internationale (OACI)
- Organisation maritime internationale (OMI)
- Programme des Nations Unies pour le développement (PNUD)
- Organisation mondiale des douanes (OMD)
- Organisation mondiale du tourisme (OMT)
- Bureau de la coordination des affaires humanitaires (OCHA)