ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

Direction de la Science, de la technologie et de l'industrie
Comité de la politique de l'information, de l'informatique et des communications

L'élaboration de politiques de protection des infrastructures d'information critiques (IIC)

Document de référence
DSTI/ICCP/REG(2007)20/FINAL

Réunion Ministérielle de l'OCDE le futur de l'économie Internet

Séoul, Corée , 17 ~ 18 juin 2008

Accueillie par 방송통신위원회
KOREA COMMUNICATIONS COMMISSION

AVANT-PROPOS

Ce rapport comprend une analyse comparative du développement des politiques pour la protection des infrastructures critiques d'information en Australie, Canada, Corée, Japon, Pays-Bas, Royaume-Uni et aux États-Unis. Il a été préparé par Nick Mansfield, consultant auprès de l'OCDE, sous la supervision d'Anne Carblanc, du Secrétariat de l'OCDE et sur la base des éléments fournis par les sept pays volontaires et de recherches complémentaires. Il complète et remplace deux études menées en 2006 et 2007 et publiées séparément. Les informations contenues dans le rapport reflètent la situation dans les pays volontaires telle qu'en décembre 2007.

Ce rapport a été discuté par le Groupe de Travail sur la Sécurité de l'Information et la Vie Privée et déclassifié par le Comité PIIC le 18 décembre 2007. Il est publié sous la responsabilité du Secrétaire Général de l'OCDE.

TABLE DES MATIÈRES

PRINCIPAUX POINTS

- Dans les sept pays examinés dans notre étude, les infrastructures d'information critiques (IIC) peuvent correspondre à une ou plusieurs des définitions suivantes :

    - Composantes informatiques sur lesquelles s'appuie l'infrastructure critique.
    - Infrastructures d'information sur lesquelles s'appuient des composantes *essentielles*[1] de l'activité gouvernementale.
    - Infrastructures d'information *essentielles* à l'économie nationale.

- Les sept pays ont des stratégies et des objectifs clairs en matière de protection des infrastructures critiques, et leurs démarches sont en accord avec les différentes cultures nationales. Tous font état d'un soutien et d'un engagement visibles des décideurs nationaux, comme en témoignent les structures et l'organisation des rôles et fonctions au sein des pouvoirs publics.

- Les sept pays sont dotés de systèmes de gestion de la sécurité assez similaires, avec certains éléments clés en commun, notamment une entité au niveau national chargée d'élaborer les normes et principes en matière de sécurité, lesquels sont souvent basés sur des standards internationaux. De plus, les sept pays possèdent une autorité publique chargée de veiller à la conformité lorsque ces normes et ces principes sont obligatoires pour les systèmes du gouvernement. Tous les pays volontaires suivent un processus, souvent basé sur une évaluation ou une analyse, visant à identifier leurs infrastructures d'information critiques. Ces processus se basent généralement sur une analyse des conséquences (ou de l'impact), des vulnérabilités (ou des faiblesses) et des menaces.

- Les points communs entre les différents pays volontaires en termes de pratique de gestion des risques sont notamment une stratégie nationale effective de gestion du risque, qui prend la forme d'un ensemble de politiques et d'objectifs s'appliquant depuis les niveaux les plus élevés de l'administration jusqu'aux différents propriétaires et opérateurs des infrastructures d'information critiques. Ce dispositif est complété par un cadre national de gestion du risque, définissant le détail de l'organisation ainsi que les outils et les mécanismes de surveillance nécessaires pour appliquer cette politique à tous les niveaux.

- Les sept pays suivent des stratégies comparables pour réduire leurs vulnérabilités et surveiller les menaces. Les évaluations de la vulnérabilité sont menées suivant une pluralité d'approches, de méthodologies, et l'analyse des menaces est axée sur les impacts les plus préoccupants. Notre étude n'a pas permis de dégager de méthode commune pour la conduite des évaluations.

1. Terme choisi pour sa neutralité.

- Étant donné la diversité des cultures nationales, il est complexe de mettre en correspondance les fonctions et responsabilités similaires dans les différents pays et de comprendre les seuils de déclenchement de la coopération transnationale. Par conséquent, la coopération sur les questions relevant de la politique transnationale pourrait être facilitée par une meilleure compréhension des délégations d'autorité et des seuils d'événements et de circonstances auxquels un pays n'a pas, à lui seul la capacité de faire face.

- Dans chaque pays, les propriétaires et opérateurs privés sont aussi engagés dans la protection des CII et collaborent avec les pouvoirs publics pour faire face aux défis et poursuivre les objectifs communs.

- Les principaux obstacles à la protection transnationale des infrastructures d'information critiques sont définis à peu près dans les mêmes termes dans les sept pays. Tous reconnaissent la nécessité de la coopération internationale, d'une capacité nationale opérationnelle de sécurité des infrastructures, de l'existence d'une volonté et d'une possibilité d'échanger des renseignements, d'une coopération étroite avec les instances pertinentes du secteur privé, d'un cadre juridique de lutte contre la criminalité informatique, et d'une culture affirmée de la sécurité face au développement rapide de la technologie et des changements qu'elle induit dans les sociétés. Pour avancer sur une partie de ces chantiers, un bon point de départ pourrait être la définition d'une approche commune d'un certain nombre de domaines, avec notamment une consultation plus étroite avec les propriétaires et opérateurs privés d'infrastructures d'information critiques.

- L'échange de renseignements pourrait être amélioré sur les plans tant national qu'international, au niveau opérationnel comme à celui des politiques. On pourrait faire davantage pour favoriser le développement de relations de confiance et de mécanismes d'échange d'informations des équipes CERT et CSIRT (équipes d'intervention en cas d'incident de sécurité informatique) et des autorités gouvernementales avec leurs homologues d'autres pays et les organisations représentatives du secteur privé.

INTRODUCTION

Objectifs

Les infrastructures d'information représentent une composante essentielle de l'ensemble infrastructurel qui permet le fonctionnement des sociétés modernes. Des menaces toujours plus fortes planent sur la sécurité de ces infrastructures et des services qu'elles sous-tendent. Le partenariat entre les secteurs public et privé et entre plusieurs pays est un mode courant de fourniture et d'exploitation de ressources informatiques toujours plus critiques. Les technologies de l'informatique et leurs marchés se sont ainsi véritablement mondialisés, en même temps que les risques qui menacent leur sécurité. La divulgation non autorisée, la corruption, le vol, les perturbations ou le déni d'accès à des ressources informatiques représentent des risques qui peuvent affecter les administrations, les entreprises et la société dans son ensemble.

En oeuvrant pour le développement d'une culture de la sécurité dans l'ensemble de la société, l'OCDE a notamment pour objet d'aider les gouvernements à échanger leurs bonnes pratiques et à élaborer des politiques cohérentes pour assurer la sécurité des systèmes et réseaux d'information. Parmi l'ensemble des systèmes d'information, il en est certains 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. Ces systèmes d'information constituent ce que l'on appelle les infrastructures d'information critiques ; assurer leur robustesse est une mission prioritaire des politiques nationales ; cela nécessite un travail de coordination avec le secteur public et avec les autres pays.

Ce rapport, rédigé à partir de deux études menées en 2006 et 2007[2], propose une analyse des politiques de sécurité des infrastructures d'information critiques[3] en Australie, au Canada, au Japon, en Corée, aux Pays-Bas, au Royaume-Uni et aux États-Unis, en cherchant plus particulièrement à mettre en évidence les facteurs qui favorisent leur développement et ceux qui l'entravent. L'objectif général de ce rapport est de favoriser une meilleure compréhension des stratégies de protection des infrastructures d'information critiques et d'intensifier la coopération internationale en favorisant un partage du savoir et de l'expérience entre les sept pays volontaires de l'OCDE qui ont participé à l'étude, les autres pays de l'OCDE et les non-membres.

Ce rapport examine la manière dont les risques pour les infrastructures d'information critiques sont généralement évalués et gérés et observe les modèles émergents et existants d'échange d'informations entre secteurs public et privé, ainsi que la manière dont les différents pays réagissent face à la nécessité accrue d'une collaboration transnationale. Il dégage les points communs et les différences entre les politiques nationales et met en évidence ce qui peut être considéré comme les bonnes pratiques de protection des infrastructures d'information critiques dans les sept pays. Il cherche à faire la lumière sur la manière dont les pouvoirs publics se coordonnent avec les propriétaires et opérateurs des systèmes et réseaux d'infrastructures d'information critiques qui ne relèvent pas de leur autorité, à l'intérieur et hors de

2. DSTI/ICCP/REG(2006)15/FINAL; DSTI/ICCP/REG(2007)16/FINAL.

3. La portée de la sécurité de l'information s'étend au delà de l'infrastructure d'information critique et comprend la gestion de l'authentification et de l'identité. Si d'autres aspects pertinents sont pris en considération, ce rapport se limite à une analyse des aspects sécurité de l'information de la protection de l'infrastructure d'information critique.

leurs frontières, et sur la manière dont les gouvernements font évoluer leurs politiques et leurs programmes de protection des infrastructures d'information critiques.

Enfin, ce rapport propose un instantané des politiques et des pratiques en vigueur actuellement dans les sept pays volontaires. Il importe de noter que ces politiques et ces pratiques peuvent très bien évoluer et changer au fil du temps pour s'adapter à un cyberespace par nature dynamique. D'ailleurs, il est important que les pays membres et non membres de l'OCDE s'efforcent sans relâche d'améliorer leurs politiques et leurs pratiques de protection des infrastructures d'information critiques.

Méthodologie

Réponses des pays volontaires

L'analyse proposée dans ce rapport se base sur les réponses fournies par les sept pays volontaires à cinq questions dont l'objet est de planter le décor, de comprendre les principales composantes critiques existantes de la protection des infrastructures d'information critiques, et de mettre en évidence les grands défis transnationaux au processus d'amélioration permanente. Voici les cinq questions qui étaient posées :

- Quelles sont les mesures et stratégies nationales de sécurité en vigueur dans votre pays et quelle est la structure actuelle de vos autorités et agences ?
- Qu'entend-on exactement dans votre pays par « infrastructure d'information critique » et quels sont vos objectifs sur le plan de l'action publique ? Comment les pouvoirs publics de votre pays identifient-ils ce qui constitue l'infrastructure d'information critique ?
- Quel rôle les pouvoirs publics jouent-ils dans la gestion des risques de l'infrastructure d'information critique ?
- Quels sont les mécanismes d'échange d'informations et les autres mécanismes utilisés au sein des administrations et avec les autres parties prenantes en matière de protection de l'infrastructure d'information critique ?
- Quelles sont, de l'avis des pouvoirs publics de votre pays, les principales difficultés de la gestion transfrontière de l'infrastructure d'information critique ? Que font-ils pour y faire face ?

Critères de comparaison

L'analyse a été conduite en passant en revue le développement des politiques de protection des infrastructures d'information critiques par rapport, d'une part aux *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information*[4] et d'autre part aux bonnes pratiques en matière de sécurité informatique. Les *Lignes directrices* proposent des orientations pour les principes à suivre. Les bonnes pratiques de sécurité informatique guident leur mise en œuvre.

Lignes directrices de l'OCDE régissant la sécurité

Toutes les normes, lignes directrices et bonnes pratiques en matière de sécurité informatique font ressortir l'importance des éléments de base des neuf *Principes des Lignes directrices de l'OCDE en matière de sécurité*. L'étude de la manière dont les pays volontaires mettent en œuvre ces principes dans la protection de leurs infrastructures d'information critiques a débouché sur un examen de leurs processus et systèmes de sécurité gouvernementaux. Si certains pays peuvent mettre l'accent sur les processus et les

4. www.oecd.org/sti/security-privacy.

systèmes de gestion alors que d'autres s'intéressent davantage à la sécurité technique, les deux approches s'appuient en pratique sur les mêmes composantes fondamentales de la gestion du risque.

Bonnes pratiques de sécurité informatique

Si l'on en juge par l'expérience[5], un certain nombre de bonnes pratiques sont considérées comme critiques à une bonne sécurité informatique au sein des organisations publiques et privées. Ce sont notamment :

- Des stratégies et des objectifs clairs.
- Une démarche compatible avec la culture de tous les participants.
- Un soutien et un engagement perceptibles de la part des décideurs.
- Une bonne compréhension des besoins grâce à l'évaluation et à la gestion des risqué.
- Un partage effectif de l'information entre tous les participants.
- Une bonne communication de la stratégie et des exigences en direction de tous les participants.
- Un effort suffisant de formation et d'éducation.
- Des systèmes de mesure exhaustifs et équilibrés pour évaluer les performances et apprécier les mesures en place, et un système de retour d'information participant à un processus d'amélioration permanente.

En se fondant sur cette expérience, on a examiné un certain nombre d'éléments sur lesquels doivent réfléchir les gouvernements dans la mise en œuvre des stratégies nationales de protection des infrastructures d'information critiques et des programmes de sécurité informatique. Ce sont notamment :

- Une stratégie nationale
- Des bases juridiques
- Une capacité de réaction aux incidents
- Les partenariats public-privé
- Une culture de la sécurité
- Un mécanisme d'échange de renseignements
- Une démarche de gestion des risques

Structure de ce rapport

A partir des contributions fournies par l'Australie, le Canada, le Japon, la Corée, les Pays-Bas, le Royaume-Uni et les États-Unis, ce rapport propose une analyse comparative des politiques des sept pays, qui vient compléter et remplacer les analyses comparatives de 2006 et 2007 sur le développement des politiques de protection des infrastructures d'information critiques[6]. Une synthèse des réponses de chacun des sept pays et une bibliographie seront ajoutées au rapport lors de sa publication sous forme d'annexes.

L'analyse comparative des politiques est une *interprétation* des informations spécifiques à chaque pays obtenues en comparant les facteurs propres à l'élaboration des politiques de protection des infrastructures d'information critiques dans les sept pays. Les spécificités de l'approche de chaque pays, jointes à un certain degré d'ambiguïté dans les informations fournies ont rendu quelque peu délicates les comparaisons entre les sept pays. Toutefois, un certain nombre de thèmes communs se dégagent des réponses. Ils pourront être utiles pour le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) dans l'élaboration de recommandations pour orienter le développement des politiques de protection des infrastructures d'information critiques.

5. Adapté de la norme ISO/IEC 17799:2000(E).

6. DSTI/ICCP/REG(2006)15/FINAL et DSTI/ICCP/REG(2006)16.

ANALYSE COMPARATIVE DES POLITIQUES

1. Description de l'infrastructure d'information critique

Le problème de la protection des infrastructures d'information critiques focalise l'attention dans nombre de pays de l'OCDE depuis quelques années. Les sept pays qui ont participé à l'étude définissent généralement leurs infrastructures d'information critiques par rapport au caractère critique que revêtent certains secteurs ou services spécifiques pour la sûreté et la sécurité de leur société, de leur administration et de leur économie. Si les pays utilisent le terme d'« infrastructure critique » dans une acception large, le terme d'« infrastructure d'information critique » se rencontre moins fréquemment dans les politiques, les stratégies et les structures nationales. Le terme d'« infrastructure d'information critique » apparaît toutefois comme un terme relativement neutre et général dans la communauté internationale, même s'il n'y a eu aucune tentative officielle pour parvenir à une définition ou à une acception communes.

Pour dresser un tableau fidèle des éléments fournis par les sept pays, ce rapport s'abstient de proposer une définition formelle des infrastructures d'information critiques. La diversité des réponses des pays n'autorise pas la formulation d'une définition commune unique. Les sept pays, d'une manière ou d'une autre, ont élaboré des politiques et de bonnes pratiques pour la sauvegarde des systèmes d'information et des réseaux qui peuvent être considérés comme des infrastructures d'information critiques. Pour faciliter les comparaisons et parvenir à une définition commune dans les sept pays, tous les éléments contenus dans les réponses des différents pays ont été analysées et sont désignées par l'intitulé commun de « protection des infrastructures d'information critiques ».

Au Japon, le terme d' « infrastructures d'information critiques » n'existe pas ; le caractère critique ou non d'un système, d'un réseau ou d'une infrastructure d'information est déterminé en fonction des critères nationaux qui définissent une infrastructure critique. Les infrastructures critiques sont formées par des entités commerciales[7] qui fournissent des services hautement irremplaçables et sont essentielles à la vie sociale et aux activités économiques. Si le fonctionnement d'une infrastructure est interrompu, perturbé ou non accessible, la vie sociale et l'activité économique en seront très affectées.

L'Australie, le Canada, les Pays-Bas, le Royaume-Uni et les États-Unis ont une vision comparable et définissent les infrastructures d'information critiques comme les systèmes informatiques (logiciels, matériels et données) et les services sur lesquels reposent une ou plusieurs infrastructures critiques et dont la perturbation ou la panne nuirait gravement au fonctionnement de l'infrastructure ou des infrastructures qui en dépendent. Tous ces pays n'utilisent pas directement le terme d' « infrastructures d'information critiques », mais tous retiennent une définition approchante.

La Corée est le seul des pays participant à l'étude à faire expressément référence aux infrastructures d'information critiques. La loi CIIP (Act No. 6383), votée et promulguée en janvier 2001[8] établit le Comité sur la protection des infrastructures d'information critiques (CPII) sous le contrôle direct du Ministre chargé de la coordination des politiques gouvernementales, pour coordonner et ajuster les tâches

7. Voir Annexe A page 54, qui contient une définition d'une « entité commerciale » au Japon.

8. Voir Annexe A la réponse de la Corée à la question 1. La loi CIIP a été revisé partiellement en novembre 2007.

concourant à l'élaboration et à l'exécution des politiques en matière d'infrastructures d'information critiques des ministères et instituts, pour une protection efficace de l'information dans l'ensemble des administrations publiques.

Vers une acception commune

Dans les sept pays volontaires, il existe une relation étroite entre les infrastructures critiques et les infrastructures d'information critiques, mais cette relation n'est pas la même dans tous les pays participants. Cela peut s'expliquer en partie parce qu'ils retiennent des critères différents pour définir ce qui constitue les infrastructures critiques ou les infrastructures d'information critiques, et qu'ils ont suivi des processus légèrement différents, quoique complémentaires, pour identifier les unes, les autres, ou les deux. Par conséquent, toute définition commune de ce qui constitue les infrastructures d'information critiques devrait être suffisamment large pour englober les besoins spécifiques des pays et les différentes approches évoquées précédemment.

L'une des options pour définir cette acception commune serait de se concentrer uniquement sur les systèmes et réseaux d'information sur lesquels reposent ces infrastructures critiques, comme c'est le cas au Japon et aux États-Unis. Toutefois, décrire les infrastructures d'information critiques uniquement comme une composante des infrastructures critiques pourrait être trop étroit pour les cinq autres pays. Par exemple en Australie, au Canada, en Corée, aux Pays-Bas et au Royaume-Uni, le concept d'infrastructures d'information critiques est inclus dans celui d'infrastructures critiques, mais il ne se limite pas aux composants sur lesquels repose l'infrastructure critique[9].

Autre caractéristique importante à prendre en compte dans la conceptualisation d'une définition commune de l'infrastructure d'information critique, la relation entre les infrastructures d'information critiques, les systèmes électroniques critiques des administrations et l'infrastructure informatique nationale.[10] Par exemple, les États-Unis décrivent les *Ressources clés* comme les ressources « sous contrôle public ou privé et essentielles pour les activités minimales de l'économie et du gouvernement ».”[11] Ils font une subtile distinction entre les infrastructures critiques et les ressources clés, tout en reconnaissant que les unes et les autres reposent sur les infrastructures d'information critiques. Tous les autres pays à l'exception du Japon, retiennent la même distinction que les États-Unis mais avec des formulations différentes. En outre, les États-Unis font une distinction supplémentaire entre la protection des infrastructures d'information critiques et la sécurité informatique (cybersecurity). Aux États-Unis, la sécurité informatique recouvre la protection des systèmes et réseaux d'information sur lesquels reposent les infrastructures critiques et les ressources clés.

Pour ces raisons, il est suggéré qu'une acception commune aux sept pays volontaires de ce qui constitue les infrastructures d'information critiques devrait comprendre un ou plusieurs des éléments suivants :

9. Aux États-Unis, le terme correct pour décrire ce que les cinq pays définissent comme l'infrastructure d'information critique serait « cybersecurity ». Toutefois, la cybersécurité aux États-Unis couvre la protection contre toutes les formes d'incidents informatiques pour l'ensemble des internautes ; elle est donc plus large que les définitions des cinq autres pays.

10. La cyber-infrastructure se compose de l'ensemble des systèmes d'information et d'informatique et des réseaux de communication qui les relient à l'intérieur du pays.

11. Voir le NIPP à la page www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

1. Les éléments informatiques sur lesquels repose l'infrastructure critique, et/ou

2. Les infrastructures informatiques sur lesquelles reposent les éléments *essentiels*[12] de l'activité du gouvernement, et/ou

3. Les infrastructures informatiques *essentielles* à l'économie du pays.

Une autre option pour parvenir à une base commune pour le concept d'infrastructures d'information critiques pourrait être de faire référence aux infrastructures désignées par un processus national.

2. Politiques et stratégies nationales, structure des autorités et des agences

De nombreux facteurs – la politique, la stratégie, et la structure institutionnelle existante des autorités et des agences – déterminent la manière dont les gouvernements identifient leurs infrastructures d'information critiques et dont ils répondent à la nécessité de les protéger. Ces facteurs sont le reflet des priorités, du style et de la culture propre de chaque pays et de son gouvernement. Ils forment la toile de fond sur laquelle est élaborée et conduite la politique de protection des infrastructures critiques. Ces mêmes facteurs constituent aussi le contexte qui prévaut à l'interprétation des mesures existantes de protection des infrastructures d'information critiques et à la compréhension de la manière dont les différents États font face aux différents défis qui se posent en la matière.

Stratégie et objectifs de l'action publique

Les sept pays volontaires donnent de leurs politiques et de leurs objectifs en matière d'infrastructures d'information de haut niveau des descriptions assez proches. Tous font référence d'une manière ou d'une autre à des événements qui pourraient coûter des vies humaines ou avoir des conséquences graves ou dramatiques sur la santé, la sécurité, la sûreté des citoyens ou l'économie du pays. Il existe des différences dans les termes employés ou dans les structures institutionnelles propres à chaque pays, mais guère sur le fond. Les sept pays volontaires définissent leurs stratégies et leurs objectifs en matière d'infrastructures d'information critiques après avoir identifié leurs infrastructures critiques. Malgré des différences dans leurs visions du risque, l'élaboration des stratégies et des objectifs de l'action publique obéit aux mêmes processus.

La répartition des responsabilités au sein des pouvoirs publics a une influence importante sur la stratégie et la politique en matière de protection des infrastructures d'information critiques. Au Canada, la politique fédérale porte essentiellement sur les événements et les circonstances qui ne peuvent être gérés à l'échelle de la province. Par exemple, le Canada s'est doté d'une organisation de gestion des urgences composée des centres opérationnels sectoriels et territoriaux, avec un centre opérationnel gouvernemental central qui orchestre l'ensemble des activités. De même, l'Australie et les États-Unis ont des organisations investies de responsabilités opérationnelles et décisionnelles spécifiques pour la protection des infrastructures d'information critiques.

Le Royaume-Uni représente une autre forme de répartition du contrôle gouvernemental : un ensemble concis d'objectifs des politiques publiques a été établi aux niveaux les plus élevés du gouvernement central, et il est interprété à tous les échelons de haut en bas jusqu'au plus local. Cette approche prévoit la répartition des responsabilités des stratégies et politiques locales de manière décentralisée et autonome par rapport au gouvernement central.

12. Expression choisie pour son caractère neutre.

Les stratégies et politiques nationales de protection des infrastructures d'information critiques sur lesquelles s'appuient les infrastructures critiques sont généralement développés dans les sept pays suivant une approche verticale à l'intérieur de chaque secteur de l'infrastructure critique. Toutefois, certains des sept pays ont une approche plus transversale de la protection des infrastructures d'information critiques. Par exemple, outre le secteur des technologies de l'information lui-même, les États-Unis ont défini une approche trans-sectorielle qui prend en compte la dépendance de tous les secteurs à l'égard des ressources informatiques. Aux États-Unis, la protection des infrastructures d'information critiques est un sous-ensemble de la sécurité informatique.

Il existe un élément commun à tous les pays volontaires concernant l'élaboration de la stratégie et des politiques : tous procèdent au niveau national à une forme d'évaluation du risque, ou d'analyse du risque, sur laquelle nous reviendrons plus en détail dans notre analyse, pour identifier leurs infrastructures d'information critiques. De là sont définis la direction de la stratégie et les objectifs de la protection de leurs infrastructures d'information critiques.

En termes pratiques, les risques ne peuvent jamais être totalement éliminés, quelles que soit la stratégie et la politique suivies. Ceci étant posé, la société doit accepter un certain niveau de risque, et il faut toujours trouver un équilibre entre les coûts d'une part, et la sécurité et la sûreté de l'autre. Le gouvernement des Pays-Bas formule ce principe dans sa Lettre au Parlement[13] en notant : « les risques résiduels doivent être acceptables. La tentation est de refuser de tolérer tout risque résiduel, justement parce que l'on est arrivé à un tel niveau de sécurité. En d'autres termes, plus il existe de mesures préventives, moins on a de tolérance aux risques (résiduels) et aux catastrophes imprévues. Cela s'appelle le paradoxe de la sûreté et de la sécurité. Quand on approche de 100 %, les coûts d'amélioration marginale de la sécurité deviennent prohibitifs et le rendement en termes de sûreté et de sécurité n'augmente plus aussi vite. Ce qu'il faut garder à l'esprit c'est que nous, en tant que société, devons faire preuve de raison vis à vis des risques auxquels nous sommes confrontés. »

Autorités et agences gouvernementales

Les sept pays ont délégué une partie de l'autorité et des responsabilités relevant des pouvoirs publics à des secteurs définis comme étant « critiques » ou « essentiels ». Chacun est doté d'une agence responsable des normes et des principes directeurs pour ses agences nationales ou fédérales. De même, chacun dispose d'une autorité chargée de veiller à la conformité des mesures grâce à des mécanismes de suivi et de reporting. Malgré ces similitudes, il serait complexe de dresser un organigramme des rôles et des responsabilités dans les sept pays car la structure et l'organisation varient selon la culture des différents pays, comme le montrent les exemples qui suivent.

- Au Japon, le Centre national pour la sécurité de l'information (NISC)[14] et le Conseil de politique de la sécurité de l'information (ISPC) jouent un rôle de coordination de tous les aspects de sécurité de l'information relevant des différents ministères. Le Ministère des affaires intérieures et des communications (MIC), le Ministère de l'économie, du commerce et de l'industrie (METI), le Ministère de la défense (MOD) et l'Agence nationale de police (NPA) sont désignés comme agences de soutien au NISC et assurent des fonctions essentielles dans le domaine de la sécurité de l'information. En outre, chaque secteur des infrastructures critiques formule les mesures nécessaires sous la supervision de son ministère de tutelle.

13 . Voir en Annexe A la contribution des Pays-Bas, lettre au Parlement sur la protection des infrastructures critiques datée de septembre 2005.

14. Voir www.nisc.go.jp/eng/index.html

- Aux Pays-Bas, le Ministère de l'intérieur est chargé de la préparation du Plan national d'urgence, qui comprend une structure générique et un central d'information, auquel se conforment les équipes de réponse aux crises. Outre ce Plan, chaque ministère a mis en place des mesures spécifiques de réponse aux urgences s'appliquant à son secteur de compétence. Par exemple le Ministère des affaires économiques, en tant que responsable de la politique des télécommunications et des technologies de l'information, a conçu et mis en place les mesures spécifiques pour répondre aux situations de crise qui se produiraient dans le secteur des télécommunications.

- Aux États-Unis, le Secrétariat du Département de la sécurité intérieure (Department for Homeland Security, DHS) a la responsabilité globale de la coordination de l'effort national visant l'amélioration de la protection des infrastructures critiques et des ressources clés aux États-Unis. Ce Secrétariat est aussi chargé de planifier les mesures de protection des infrastructures nationales et coordonne les activités de protection de 17 secteurs des infrastructures critiques et ressources clés (CI/KR)[15]. En outre, le Secrétariat évalue l'opportunité de la création de nouvelles catégories d'infrastructures critiques et de ressources clés et coordonne la couverture des risques dont elles font l'objet, le cas échéant. Par ailleurs, les agences sectorielles spécifiques sont les départements et agences fédéraux responsables des activités de protection des infrastructures dans un secteur désigné des infrastructures clés ou dans une catégorie donnée de ressources clés. Si le DHS est l'agence sectorielle spécifique responsable du secteur des technologies de l'information (TI) et est aussi chargé de la planification de la protection des infrastructures critiques de nature transsectorielle, de nombreux départements et agences de niveau fédéral collaborent avec lui sur différents aspects de la protection des infrastructures critiques et des infrastructures d'information critiques.

Pour identifier les organismes homologues parmi l'écheveau complexe des communications gouvernementales internes, il est utile d'avoir une compréhension claire des structures nationales, des rôles et des responsabilités des agences et des autorités gouvernementales. Cela permet une meilleure communication tant entre entités du secteur public aux échelons les plus élevés et celles de niveau local, qu'entre instances publiques et entreprises du secteur privé. C'est aussi un atout pour aborder les relations d'interdépendance aux niveaux national et international. Par exemple, la publication de la liste des agences sectorielles spécifiques avec leurs rôles et leurs responsabilités dans la protection des infrastructures d'information critiques peut contribuer à accélérer les actions transnationales.

Si l'on se fonde sur l'analyse ci-dessus, les éléments suivants peuvent être considérés comme des exemples de bonnes pratiques pour les politiques et stratégies nationales, et la structure des autorités et des agences :

- Existence de politiques et d'objectifs clairs fixés au niveau décisionnel le plus élevé de gouvernement, et interprétés tout au long de la chaîne de décision jusqu'à l'échelon le plus local.
- Soutien et engagement des décideurs nationaux reflétés dans les structures et l'organisation des rôles et responsabilités au sein des pouvoirs publics.
- Existence d'une entité qui élabore les normes et les lignes directrices en matière de sécurité au niveau national.
- Existence d'une entité qui veille au respect des normes et des lignes directrices lorsqu'elles sont requises pour les systèmes de l'administration.
- Bonne communication quant aux rôles et responsabilités des autorités et agences gouvernementales.

15. Infrastructures critiques / ressources clés.

- Existence d'un processus national d'évaluation du risque ou d'analyse du risque pour identifier toutes les composantes de l'infrastructure d'information critique.
- Adoption d'une approche transversale compte tenu du fait que les infrastructures d'information critiques sont indispensables au fonctionnement de différentes infrastructures critiques, d'où un certain nombre de relations d'interdépendance.
- Adoption d'une approche d'équilibre des coûts au regard des impératifs de sécurité et de sûreté, et définition d'un niveau raisonnable de risque qui doit être accepté par la société.
- La politique et la stratégie nationales supposent une collaboration avec le secteur privé.

3. Rôle des pouvoirs publics dans la gestion des risques pesant sur les infrastructures d'information critiques

La détermination du risque dépend de la perspective propre de chaque pays concernant sa propre dépendance à l'égard de ses ressources infrastructurelles d'information. Le risque est toutefois habituellement déterminé par une analyse des conséquences (ou de l'impact), qui aboutit à identifier les causes potentielles des menaces et des points de vulnérabilité (ou faiblesses). A cet égard, les sept pays ont mis au point des stratégies de gestion du risque pour réduire leurs vulnérabilités et surveiller les menaces.

Le rôle des pouvoirs publics dans la gestion du risque des différentes composantes des infrastructures d'information critiques varie, comme en atteste la variété et la complexité des structures et l'organisation des rôles et des responsabilités au sein des pouvoirs publics, que nous venons d'évoquer. Le rôle détaillé de l'Etat dans chaque pays dépend du niveau d'autorité ou d'influence qu'il exerce.

Les stratégies des différents pays en matière de gestion du risque national donnent une idée des approches qu'ils peuvent avoir de la gestion des risques pesant sur leurs infrastructures d'information critiques. Les stratégies, à leur tour, façonnent les cadres institutionnels de la gestion du risque national. Dans les sept pays, les priorités en matière de gestion des risques pesant sur les infrastructures d'information critiques découlent des stratégies en matière de gestion des risques et des cadres régissant les infrastructures critiques.

Stratégie de gestion des risques

Pour comprendre les rôles et responsabilités des pouvoirs publics dans la protection des infrastructures d'information critiques, il est nécessaire d'analyser le niveau d'autorité ou d'influence exercé par l'Etat. A cet égard, les sept pays partagent une même vision, où l'Etat est responsable de la continuité des infrastructures d'information critiques. Par exemple, aux Pays-Bas, c'est le gouvernement qui est responsable de la partie des infrastructures d'information critiques qui est possédée ou contrôlée par des administrations publiques, et par conséquent, le gouvernement est pleinement compétent pour réaliser les analyses de risque et appliquer des mesures. Pour la partie des infrastructures d'information critiques qui est possédée ou contrôlée par des entreprises ou des organismes privés, le gouvernement des Pays-Bas est responsable de veiller à ce que les différentes parties procèdent à des analyses du risque et prennent les mesures de protection appropriées.

Dans la majorité des sept pays étudiés, la protection des infrastructures d'information critiques est coordonnée par un organisme gouvernemental qui a la responsabilité d'un secteur spécifique. La capacité des ces organismes à exercer cette responsabilité dépend d'un certain nombre de facteurs, parmi lesquels le degré de régulation en vigueur dans leur secteur spécifique, l'existence de partenariats public-privé, les mécanismes d'échange de renseignements, et d'autres facteurs. Ils sont souvent investis de certains pouvoirs de régulation et peuvent contraindre les propriétaires ou les opérateurs privés d'infrastructures d'information critiques à prendre des mesures de protection contre ce qui est défini par le Royaume-Uni (par exemple) comme « une perte ou une atteinte… qui pourrait conduire à la perte de nombreuses vies

humaines, à un préjudice économique de long terme, à des conséquences graves pour la société, ou qui serait pour toute autre raison un sujet de préoccupation immédiat pour les pouvoirs publics.[16] » Les critères définissant le « sujet de préoccupation immédiat » évoqué par le Royaume-Uni et dans les sept pays participants sont très voisins, mais peuvent être formulés différemment. Si la législation n'autorise pas de mesures contraignantes, les organismes du secteur public établissent des partenariats avec le secteur privé ou jouent un rôle consultatif.

Autre point commun entre les sept pays, l'établissement de partenariats public-privé pour encourager les propriétaires et les opérateurs d'infrastructures critiques à prendre des décisions pour la sauvegarde et la protection de leurs propres actifs d'infrastructure critique. Par exemple les Pays-Bas, le Royaume-Uni et les États-Unis ont établi des Centres d'information, et les États-Unis ont également établi des Conseils de coordination sectorielle (Sector Coordinating Councils, SCC), des Conseils de coordination gouvernementale (Government Coordinating Council, GCC), et des Centres de partage et d'analyse de l'information (Information Sharing and Analysis Centers, ISAC) pour de nombreux secteurs.

Cadre de gestion du risque

Dans chaque pays, c'est la stratégie globale en matière de gestion du risque qui détermine le cadre national de gestion du risque.

La portée des cadres de gestion du risque est à peu près la même dans les sept pays. On peut prendre l'exemple de l'Australie, avec l'adoption[17] d'une stratégie en cinq points pour la protection des infrastructures d'information critiques :

- Élaboration des politiques couvrant le Commonwealth, le secteur privé, ainsi que les Etats et territoires
- Collecte et analyse de l'information
- Mesures défensives comprenant à la fois des mesures de protection de la sécurité et de sensibilisation
- Mécanismes de réaction incluant des réponses techniques à des incidents techniques et des dispositifs de gestion des crises
- Planification des contingences couvrant non seulement les incidents mais aussi leur impact global.

Dans les sept pays, le cadre national de gestion du risque combine des organisations, des processus et des normes gouvernementales aboutissant à des mesures de gestion des risques et d'amélioration de la protection des infrastructures d'information critiques.

Éléments d'organisation

Chaque pays est doté d'un ensemble d'organisations investies de pouvoirs différents mais couvrant, d'une manière ou d'une autre, les cinq points énumérés dans la stratégie de l'Australie. L'élaboration de la politique de gestion des risques est généralement cohérente avec les autres domaines du gouvernement, avec le même niveau de centralisation et de développement, en fonction du niveau d'autorité ou d'influence exercé par les pouvoirs publics. Par exemple, la Corée a adopté une méthode pour analyser et évaluer les vulnérabilités. Le cadre coréen est organisé par la Korean Managing Authority qui réalise une

16. Voir réponse du Royaume-Uni, page 57..

17. www.dsd.gov.au/infosec/infrastructure_protection.html

analyse et une évaluation précises des vulnérabilités, puis, tous les deux ans, en fonction des résultats, établit les mesures de protection qui s'imposent.

De même, de plus en plus, on voit s'établir des partenariats public-privé chez les pays volontaires. La forme que prennent ces partenariats varie d'un pays à l'autre, en fonction des différentes cultures nationales et des différents styles d'administration.

Au Japon, tout comme au Royaume-Uni et aux États-Unis, les partenariats public-privé sont des composantes reconnues du cadre national de gestion du risque. Au Japon, le Plan d'action définit les mesures qui doivent être formulées par chaque entreprise concernée par les infrastructures critiques pour assurer la continuité opérationnelle. Cela suppose aussi de définir précisément les actions pour identifier les mesures qui doivent être prises par les pouvoirs publics et par chaque secteur de l'infrastructure critique. Ce processus permet d'assurer que les mesures de sécurité de l'information liées aux infrastructures critiques sont appliquées en partenariat étroit avec les secteurs public et privé[18].

Toute institution de gestion du risque requiert pour être efficace une solide dimension d'autorité et d'organisation. C'est le cas dans les sept pays étudiés. Par exemple aux États-Unis c'est le DHS (Departement of Homeland security), en Corée le Comité de protection des infrastructures d'information (CPII) et au Japon le Conseil de la politique de sécurité de l'information, tous dotés de mécanismes de notification au plus haut niveau national sur les problèmes de politiques de protection des infrastructures d'information critiques. L'engagement démontré par les autorités de haut niveau est un message clair adressé aux opérateurs des infrastructures d'information critiques sur l'importance de la protection de cette infrastructure.

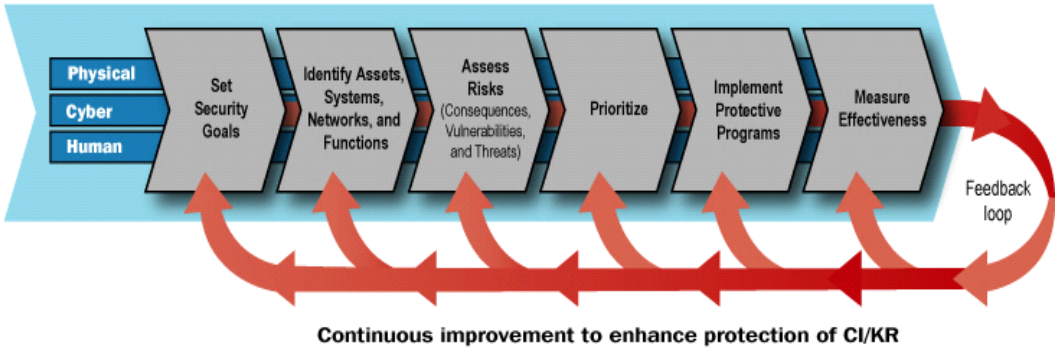
S'agissant de leurs propres systèmes gouvernementaux, les sept pays ont un ensemble de règles de fonctionnement définissant un certain niveau d'impératifs de sécurité de base que leurs différentes administrations doivent remplir pour assurer la sécurité de leurs systèmes d'information. Il s'agit notamment : d'un contrôle de la gestion, de l'évaluation du risque, du traitement des incidents de sécurité et des points de vulnérabilité des systèmes, d'audits de sécurité et de planification de la continuité opérationnelle.

Processus de gestion du risque

S'il existe un cadre de gestion des risques dans les sept pays, tous ne suivent pas un même modèle de processus. Le rôle de l'État dans la gestion du risque des infrastructures d'information critiques varie, comme nous l'avons vu précédemment, et le niveau d'intervention des pouvoirs publics dépend de l'expérience de chaque pays, de sa culture et du style d'administration. L'exemple des États-Unis offre l'image d'un ensemble complet de processus. La pierre angulaire du Plan de protection des infrastructures nationales des États-Unis (National Infrastructure Protection Plan, NIPP) est le Cadre de gestion du risque représenté par la matrice ci-dessous, qui établit le processus utilisé pour faire la synthèse des informations sur les menaces, les vulnérabilités et les conséquences pour évaluer et gérer le risque. Cette démarche est spécifique aux États-Unis, mais toutes les activités contenues dans ce modèle se retrouve chez les sept pays.

18 . Les principes pour la formulation de « Standards, lignes directrices, etc. de sécurité « concernant l'assurance de la sécurité de l'information des infrastructures critiques peuvent être consultés à la page www.nisc.go.jp/eng/pdf/principles_ci_eng.pdf.

Figure 1. États-Unis : Le cadre de gestion du risque NIPP



Si le processus général est commun aux sept cadres de gestion du risque, la formulation et les actions, à l'intérieur de chaque activité, paraissent très différentes dans chaque pays. Par exemple, le processus cyclique évoqué précédemment de la Korean Managing Authority qui intervient tous les deux ans est axé sur l'évaluation des vulnérabilités et sur l'amélioration continuelle du système en l'absence d'une menace spécifique. C'est l'exemple d'un cas où les pouvoirs publics exercent ce qu'on appelle la « due diligence » connue dans le secteur privé. Le processus appliqué en Corée comporte cinq étapes :

- Étape 1: Planification des analyses et des évaluations des vulnérabilités
- Étape 2: Choix des cibles pour l'analyse et l'évaluation des vulnérabilités
- Étape 3: Analyse des facteurs de menace et des vulnérabilités
- Étape 4: Évaluation des vulnérabilités (Évaluation du niveau de risque)
- Étape 5: Mise au point des mesures de protection

En Australie, le Comité ESPAC (E-Security Policy and Coordination Committee)[19], présidé par le Département du procureur général (AGD), est investi de la responsabilité d'identifier l'infrastructure d'information de l'Australie et de formuler des recommandations pour sa protection. Le programme CIPMA (Critical Infrastructure Protection Modelling and Analysis)[20] contribue à la tâche du Comité ESPAC en établissant les conséquences potentielles d'une défaillance de l'IIC.

Tous les pays volontaires mettent en œuvre leurs processus de gestion du risque avec des niveaux de rigueur différents pour les différentes composantes de l'infrastructure d'information critique et de ses priorités. Mais pour fixer un standard minimum en matière de gestion du risque pour l'ensemble des composantes de l'IIC possédées ou contrôlées par les pouvoirs publics, les gouvernements des sept pays ont presque tous établi de manière formelle des normes techniques de sécurité qui doivent être respectées.

Un processus-cadre comme celui des États-Unis avec le NIPP[21] pourrait être une bonne base pour les discussions transnationales en matière de processus de gestion du risque pour protéger les infrastructures d'information critiques. Un autre fondement pourrait être l'approche japonaise établie dans le Plan d'action. Ces deux cadres comportent des éléments communs qui pourraient être considérés comme de bonnes pratiques dans l'élaboration de tout cadre national.

19. www.dcita.gov.au/__data/assets/pdf_file/71201/ESNA_Public_Policy_Statement.pdf.

20. www.tisn.gov.au/agd/WWW/TISNHome.nsf/Page/CIP_Projects.

21. Voir Figure 1.

Normes en matière de gestion du risque

Les normes techniques de sécurité, qu'elles émanent des gouvernements ou d'autres instances, jouent un rôle essentiel dans les cadres de gestion du risque des sept pays. Le Japon applique un cadre reposant sur les normes[22] pour les systèmes possédés ou contrôlés par l'État. De plus, le Plan d'action du Japon appelle à prendre des mesures préventives contre les dysfonctionnements informatiques avant même l'apparition de menaces spécifiques. Le Plan d'action exige également une revue annuelle de ces mesures et un processus d'amélioration continuelle selon le modèle PDCA (Plan, Do, Check, Act, ou en français, Planifier, Faire, Vérifier, Agir)[23]. Voilà un autre exemple de mise en œuvre du cadre de gestion du risque générique décrit précédemment, en conformité avec la culture et le style d'un gouvernement particulier.

Les normes de sécurité de l'information gouvernementale ne sont pas les mêmes dans tous les pays volontaires. Certains sont dotées d'agences spécifiques, comme aux États-Unis le National Institute of Standards and Technology (NIST), chargé de formuler les normes pour les systèmes possédés ou contrôlés par les pouvoirs publics alors que d'autres pays, comme l'Australie ou le Japon, adaptent les normes internationales existantes.

Les normes et les principes directeurs en matière de sécurité de l'information gouvernementale doivent être adossés à des systèmes d'audit et de contrôle efficaces. Si toutes les réponses reçues ne rentrent pas dans le détail, il apparaît que tous les pays volontaires ont établi un mécanisme d'audit et de reporting pour organiser un retour d'information vers le processus décisionnel gouvernemental, afin de mettre en œuvre des mesures d'atténuation du risque et dans une démarche d'assurance de l'information. En règle générale, la responsabilité globale de l'audit et du contrôle incombe à l'autorité de contrôle financier et d'audit du gouvernement central. Les processus décrits par le Canada constituent un exemple type de ceux qui sont appliqués dans la plupart des pays volontaires.

Priorités en matière de gestion du risque

Chacun des sept pays a établi des priorités en matière de gestion du risque, priorités qui sont le reflet des circonstances nationales de chaque pays, ainsi que de sa culture et de son style de gouvernement. Cela étant, dans les sept pays, les priorités en matière de risques sur l'infrastructure d'information critique sont définies dans le cadre de processus mettant en œuvre la stratégie et le cadre de gestion des risques. Ainsi, si les sept pays présentent peu de points communs dans le détail de leurs priorités, il y a davantage de similitudes dans les processus qui conduisent à l'établissement de ces priorités. Au Canada, des processus d'autoévaluation et d'audit ont été mis en œuvre pour fixer les priorités en matière de protection des systèmes d'information des pouvoirs publics. Chaque ministère ou département de l'administration est responsable d'identifier sa propre infrastructure d'information critique et de maintenir les plans appropriés pour la continuité opérationnelle. Cela semble être un processus commun dans l'établissement des priorités nationales de gestion du risque. Toutefois, le succès du déploiement vertical des priorités au

22. Le terme de « standard » est utilisé au sens très large. Il inclut les normes au sens où nous l'entendons habituellement, mais il peut aussi comprendre les réglementations, les règles, les impératifs ou les mesures édictés dans le cadre du processus de gestion du risque défini par la NISC. Cette utilisation du terme de « standard » correspond au sens usuel du terme au Japon.

23. Les normes « Standards for Information Security Measures for the Central Government Computer Systems » constituent une application de la norme JISQ 27001 (Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences) (=ISO/IEC 2700) et JISQ27002 (Technologies de l'information – Techniques de sécurité – Code de pratique pour la gestion de la sécurité de l'information) (=ISO/IEC17799). Il s'agit de normes visant à assurer l'efficacité de l'établissement, de la gestion, de la surveillance, de la maintenance et de l'amélioration des systèmes de gestion de la sécurité des organisations. Le cycle PDCA est la pierre angulaire de ces normes.

niveau national et de leur déploiement horizontal sur l'ensemble des infrastructures d'information critiques semble variable.

L'approche de la Corée diffère de celle du Canada, en ce qu'elle part d'un ensemble de priorités sur lesquelles elle base son cadre de gestion du risque. Elle met l'action sur l'amélioration de la technologie et la coopération afin d'identifier et d'analyser la menace. C'est tout à fait conforme à la démarche de ce pays en matière de gestion du risque, qui part d'une analyse des faiblesses. L'approche du Japon, tout comme celle de la Corée, part d'un ensemble de priorités recensées dans le Plan d'action sur les mesures de sécurité de l'information pour les infrastructures critiques, lequel ensemble déclenche une série de processus (PDCA) visant à impulser une amélioration continuelle.

Les priorités du Royaume-Uni sont les infrastructures nationales critiques et sont fixées sur le plan opérationnel secteur par secteur afin d'identifier les opérateurs de services critiques au niveau national qui s'appuient sur des systèmes d'information, et d'évaluer leur caractère critique. Plus ce caractère critique est prononcé, plus la priorité est forte. Ce travail aboutit à un processus d'établissement des priorités pour mettre en œuvre les contre-mesures destinées à prévenir les risques d'attaque électronique associés aux scénarios catastrophes identifiés dans l'évaluation du risque national.

Comme le Royaume-Uni, les États-Unis ont défini leurs priorités à la suite d'un processus en trois étapes visant : *i*) à identifier les ressources informatiques, les systèmes et les réseaux ; *ii)* à évaluer le risque informatique ; *iii)* à mettre en œuvre des programmes de protection destinés à réduire le risque ; cette démarche se distingue de celle du Japon, dont le Plan d'action contient des priorités détaillées.

L'Australie a adopté une approche plus systématique avec le Programme de modélisation et d'analyse des infrastructures critiques, ou CIPMA. Le résultat – notamment pour les infrastructures d'information – est probablement le même que ceux des processus des États-Unis et du Royaume-Uni, avec l'identification de relations de dépendance et d'interdépendance primaires entre éléments des infrastructures critiques et de la chaîne des conséquences qui découlent d'une défaillance.

Le résultat du modèle australien représente typiquement ce à quoi les sept pays s'efforcent de parvenir : le processus décisionnel en matière de gestion du risque chez les pouvoirs publics comme dans le secteur privé est appuyé sur des constatations et des analyses concernant les aspects suivants :

- Les relations de dépendance et d'interdépendance entre systèmes d'infrastructures critiques.
- Les conséquences en chaînes d'une défaillance survenant sur une infrastructure critique.
- Les points d'étranglement, les points uniques de faille et les autres grandes vulnérabilités.
- Les options d'investissement et les autres stratégies d'atténuation du risqué.
- Les scénarios, notamment les catastrophes naturelles et les actes terroristes interrompant la fourniture de services d'infrastructures critiques et mettant à mal la continuité de l'activité et les autres plans de réponse.

Une grande partie des technologies de systèmes d'information qu'utilisent les pays volontaires sont les mêmes ou sont comparables : il est donc probable que leurs vulnérabilités (ou leurs faiblesses) soient les mêmes. A l'inverse, la perception qu'on a des menaces paraît plus spécifique à chaque pays. Cela pourrait signifier qu'il est difficile de parvenir à une idée commune de toutes les menaces pesant sur les infrastructures d'information critiques. En revanche, il pourrait être plus facile de formuler une définition commune de certaines vulnérabilités. Cela pourrait aussi être une des voies vers plus de coopération transnationale sur la stratégie et la politique de protection de l'infrastructure d'information critique.

Le fait que les conséquences et les vulnérabilités soient plus faciles à identifier que les menaces pourrait conduire à ce que l'on mette trop l'accent sur les premières en l'absence des secondes, aboutissant

à une réaction excessive des intéressés. Une coopération plus étroite sur certaines des menaces les plus répandues, comme les maliciels, pourrait permettre une meilleure compréhension des menaces transnationales aux infrastructures d'information critiques et servir à améliorer les stratégies et leur mise en œuvre.

On pourrait parvenir à une conception commune des vulnérabilités des infrastructures d'information critiques par une coopération plus étroite et une meilleure communication entre les équipes d'intervention en cas d'incident de sécurité informatique (les CSIRT), qui relèvent des pouvoirs publics, le secteur privé et les autres parties prenantes. Cela pourrait être facilité par l'utilisation d'un ensemble de concepts et d'un vocabulaire communs sur lesquels tous les participants accepteraient de fonder leur action. La simplification de la terminologie pourrait faciliter une meilleure communication entre tous les participants.

D'après l'analyse qui précède, les éléments suivants pourraient être considérés comme des exemples de bonnes pratiques pour la gestion du risque sur les infrastructures d'information critiques par les pouvoirs publics :

- Existence d'un cadre formel de gestion du risque s'appuyant sur une organisation, des outils et une surveillance de l'application de la politique de sécurité à tous les échelons décisionnels des secteurs public et privé, jusqu'aux propriétaires et aux opérateurs des infrastructures d'information.
- Existence de processus pour la gestion du risque, à savoir notamment : l'élaboration des politiques, la collecte et l'évaluation des renseignements, les mesures préventives, les mesures d'intervention en cas d'incidents et d'urgences, les plans de secours pour la continuité de l'activité (reprise après sinistre et reprise des opérations).
- Existence de normes, principes directeurs et mécanismes de partage de l'information relevant des pouvoirs publics appuyés par des systèmes efficaces d'audit et de contrôle sur la sécurité des systèmes d'information de l'Administration.
- Existence d'un jeu d'outils communs d'évaluation du risque pour soutenir le processus de gestion du risque, permettant des évaluations et un établissement des priorités comparables entre les différentes technologies et composantes de l'infrastructure critique de l'information.
- Existence de priorités en matière de gestion du risque comprenant une analyse des conséquences (ou de l'impact) pour établir des comparaisons, tant verticalement (au sein de chaque secteur) qu'horizontalement (entre secteurs).
- Elaboration d'un vocabulaire et d'une terminologie simplifiés, ainsi que d'un cadre commun pour la gestion du risque pesant sur l'infrastructure d'information critique, qui puisse être compris par l'ensemble des participants.

4. Initiatives d'échange de renseignements et autres initiatives visant à protéger l'infrastructure d'information critique

Le partage de l'information est un important facteur de succès que soulignent les sept pays volontaires dans la majorité de leurs réponses aux quatre questions. L'échange de renseignements au sein d'une structure particulière de gestion relevant de l'Administration ou d'une communauté de participants, semble fonctionner aux niveaux national et international. Des faiblesses et des difficultés semblent apparaître au-delà de ces groupes fermés.

Les sept pays utilisent des sites Internet comme moyen principal de diffusion de l'information relative à l'infrastructure d'information critique. Tous les sept ont communiqué des listes d'adresses de sites Internet d'administrations et de forums. Ces sites Internet renferment de nombreux exemples de bonnes pratiques. Pour cette analyse, nous avons évalué des échantillons de sites Internet des administrations au regard de quelques critères simples, en vue de tirer quelques conclusions générales. Le premier critère concerne le modèle de base de circulation de l'information utilisé pour partager l'information. Dans un

modèle de type « pull », l'information est accessible si l'utilisateur peut la trouver. Si l'utilisateur peut la trouver, alors le téléchargement est le moyen le plus commun pour y accéder. Dans un modèle de type « push », des avertissements, des alertes etc. sont envoyées (poussées) automatiquement aux utilisateurs de l'information. Dans le modèle « push », qui fonctionne suivant un système d'abonnements, l'expéditeur de l'information n'a pas à se préoccuper d'identifier les destinataires. Ceux qui souhaitent recevoir certains alertes ou autres messages ajoutent leurs coordonnées à la liste de distribution. Cela permet une gestion automatique efficace des listes de distribution, mais certains participants qui devraient figurer dans la liste ne sont pas abonnés. Les autres critères portent sur la facilité d'utilisation des forums et des sites Internet recensés.

L'examen de certains des sites Internet cités montre que les informations intéressantes sur les infrastructures d'information critiques ne sont pas toujours aisées à trouver. Il faut souvent aller les chercher derrière plusieurs couches d'arborescence. L'éligibilité et les conditions à remplir pour s'abonner à certains sites de l'administration sont parfois peu claires. Plus généralement, la recherche de l'information tend à prendre du temps. La navigation est un facteur critique, non seulement à l'intérieur d'un même site mais aussi d'un site à l'autre. En règle générale, les sources d'information conjointes sont rares. La viste des sites Internet a également permis de récolter de longues listes d'acronymes de forums et de sites Internet supplémentaires qui rendent parfois l'information plus difficile à comprendre.

Le partage de l'information au niveau national

Le partage de l'information au sein de l'administration au niveau national semble être bien développé, même si tous les pays signalent des difficultés aux échelons les plus élevés. Outre l'existence de nombreux sites Internet, la plupart des pays volontaires organisent des réunions et des téléconférences régulières entre les principaux acteurs en la matière, généralement les responsables de la sécurité de l'information (ou CISO, chief information security officers). Le partage de l'information s'observe aussi au niveau opérationnel. Tous les pays volontaires sont dotés de CSIRT publics. La plupart des CSIRT de compétence nationale font partie d'une manière ou d'une autre d'un réseau comprenant d'autres CSIRT.

Nous l'avons vu, il est essentiel d'avoir une organisation efficace des rôles et responsabilités dans la protection de l'infrastructure d'information critique au sein des pouvoirs publics. Quand le partage de l'information fonctionne bien au niveau national, on a plus de chances qu'il y ait une relation de partage d'information plus productive avec le secteur privé et la communauté internationale.

Le partage de l'information avec le secteur privé

Les sept pays sont dotés ou sont en train d'établir des forums de partage de l'information avec le secteur privé. Les mécanismes de partage de l'information entre entreprises (TISN en Australie, CEPTOAR au Japon, ISAC et SCC aux États-Unis, et les Information Exchanges au Royaume-Uni et aux Pays-Bas) paraissent être les plus fréquents, sous une forme ou sous une autre, dans tous les pays volontaires. Certains organisent le fonctionnement de leurs forums de différentes manières suivant les cultures.

Toutes les réponses font ressortir l'importance de partenariats étroits avec le secteur privé, tout en soulignant aussi les difficultés du partage de l'information avec des organisations privées. De même, les entreprises peuvent être réticentes à partager des informations avec l'Administration. Dans un cas comme dans l'autre, les partenariats public-privé ne sont pas toujours aussi étroits que les participants pourraient le souhaiter. Ainsi, l'étude montre que le partage de l'information avec le secteur privé sur la protection de l'infrastructure d'information critique est une difficulté permanente pour les gouvernements. Pour la surmonter, il peut être nécessaire – au-delà d'une législation qui, par exemple, protègerait le partage de l'infrastructure d'information critique – de travailler sur la confiance et le sentiment de sécurité. Un certain

nombre de problèmes de confiance ont été pointés des deux côtés lors des recherches menées sur certains des sites Internet. Tous ne sont pas cités dans les réponses des pays volontaires et il pourrait être utile de mener des recherches complémentaires pour examiner plus en détail les difficultés du partage d'information entre secteurs public et privé, ainsi que les mécanismes de renforcement de la confiance qui permettraient d'améliorer la communication entre participants.

Le partage de l'information au niveau international

Comme le notent les États-Unis, la coopération internationale et une action collaborative sont indispensables pour bâtir les relations nécessaires à une prise de conscience de la situation et à une meilleure coordination de la réponse aux incidents informatiques dans l'environnement informatique mondial.

Les sept pays font état de difficultés dans le partage de l'information, particulièrement des renseignements sensibles, au niveau international. Ce problème se retrouve, d'une manière ou d'une autre, dans les réponses des sept pays concernant les difficultés dans les affaires transnationales, que nous détaillons ultérieurement dans ce rapport. Cela peut s'expliquer en partie par le lien qui existe entre l'infrastructure d'information critique, l'infrastructure critique et la sécurité nationale, qui pourrait conduire à limiter l'accès à la plus grande partie de l'infrastructure d'information tout entière, à cause de la nécessité de protéger une fraction minoritaire de l'infrastructure d'information sensible. A cet égard, la coopération internationale entre gouvernements sur la protection de l'infrastructure d'information critique pourrait être améliorée par l'adoption d'un modèle de sécurité qui soit « ouvert, à l'exception de certains éléments fermés » par opposition au modèle traditionnel de sécurité « fermé, à l'exception de certains éléments ouverts ». Cela pourrait faciliter le partage des informations sur l'infrastructure sans compromettre les informations sensibles.

Les contributions des pays volontaires fournissent des exemples d'accords bilatéraux sur le partage d'informations. On peut citer le Cadre pour la coopération dans la protection des infrastructures essentielles (PIE), ou « cadre PIE conjoint » : Le Cadre PIE conjoint a été établi en conformité avec le PSP (Partenariat nord-américain pour la sécurité et la prospérité lancé en mars 2005) et résulte d'un engagement pris dans le cadre de la Déclaration sur la frontière intelligente[24]. Il établit la structure d'une collaboration continue en identifiant des objectifs stratégiques pour les autorités des deux pays. Parmi ces objectifs, le développement et la mise en œuvre de stratégies de protection et d'intervention compatibles et de programmes pour les infrastructures critiques partagées dans des domaines prioritaires établis d'un commun accord, notamment les systèmes informatiques. Ces dispositions bilatérales pourraient servir de modèle pour établir d'autres accords multilatéraux.

Le partage multilatéral de l'information se fait au sein de nombreuses organisations internationales existantes. Les sept pays citent les organisations internationales auxquelles ils appartiennent, parmi lesquelles l'OCDE. L'analyse des réponses ne fait pas ressortir d'organisations particulières s'agissant de la protection de l'infrastructure critique d'informations ; toutefois plusieurs pays citent le réseau IWWN (International Watch and Warning Network) et la Meridian Conference, qui sont des forums de partage d'informations.

L'étude suggère que le partage de l'information à l'échelon international et à l'échelon national entre les CERT/CSIRT et les pouvoirs publics est essentiel pour la protection de l'infrastructure d'information critique. A mesure que le partage de l'information au niveau opérationnel des CERT/CSIRT continue de

24 . La Déclaration sur la frontière intelligente comprend un ensemble d'initiatives, regroupées sous le terme de Plan d'action en 30 points, ayant pour objet d'assurer la circulation sans danger des personnes, des marchandises et des infrastructures communes, et coordonner le partage de l'information.

s'intensifier, il faut aussi poursuivre les efforts d'amélioration de la communication, particulièrement entre les différents CERT de compétence nationale. Les mécanismes transnationaux de partage de l'information sont essentiels pour gérer une crise et atténuer les dégâts potentiels en cas d'incidents qui pourraient s'étendre au-delà du domaine de compétence ou de la capacité d'action des CERT opérationnels locaux et évoluer au stade d'urgence, affectant la fourniture de services d'une ou plusieurs des infrastructures nationales.

L'un des moyens de gérer des situations de ce type pourrait être d'encourager les autorités gouvernementales à échanger des renseignements avec leurs homologues d'autres pays. A cet égard, le développement de relations de confiance et l'établissement de mécanismes de partage de l'information pourraient apporter d'appréciables pierres à l'édifice. Toutefois, l'existence d'un grand nombre de canaux de partage de l'information au sein des gouvernements signifie peut-être qu'il faut définir plus clairement lesquels il convient le mieux d'utiliser.

Formation et sensibilisation

Les réponses collectives des sept pays aux questions sur le partage d'information au regard de l'éducation et de la sensibilisation ne sont pas suffisamment approfondies pour faire l'objet d'une analyse détaillée. L'Australie, le Canada et le Royaume-Uni décrivent un certain nombre d'initiatives pour informer l'ensemble des citoyens et de campagnes pour défendre les intérêts des consommateurs. Dans l'ensemble, les sept pays reconnaissent l'importance de la formation et de la sensibilisation, qui passe notamment par une communication active en direction des citoyens, dans le cadre de leur plan global de protection de l'infrastructure critique. Tous ont mis en place des mécanismes de sensibilisation et de partage d'information dans le contexte de leur plan de sécurité informatique, mais pas toujours dans le contexte spécifique des infrastructures d'informations critiques.

Recherche

Les sept pays constatent la rapidité du progrès technologique, et soulignent l'importance de la recherche dans le cadre de leur plan global de protection de l'infrastructure critique. Toutefois, les contributions des pays volontaires sur le partage d'information dans le domaine de recherche sont limitées, et ne comprennent pas suffisamment d'exemples de programmes spécifiques en vigueur pour permettre une analyse. Des informations spécifiques sur des travaux de recherche figurent dans les contributions du Canada, des Pays-Bas (voir infra.) et du Royaume-Uni. Les États-Unis décrivent en détail le rôle des différentes composantes du Département de la sécurité intérieure (DHS) dans la recherche sur la sécurité informatique.

Les Pays-Bas ont mis en place un programme intitulé Sentinels pour parvenir à un meilleur ciblage de la recherche scientifique concernant la sécurité des réseaux et systèmes d'information. Ce programme est financé par des partenaires publics et privés. Le programme Sentinels a démarré en 2004 pour une période de six ans et a pour objet d'améliorer l'expertise en matière de sécurité aux Pays-Bas. L'un des objectifs est de bâtir une communauté nationale de chercheurs sur la sécurité des TIC, et de diffuser les résultats de ses travaux en direction des entreprises et des pouvoirs publics. Les liens avec les partenaires européens et internationaux seront aussi développés. Le programme Sentinels comporte deux volets : le premier concerne la recherche scientifique, avec des résultats obtenus en collaboration avec les industriels du secteur ; le second est de veiller à ce que les connaissances dérivées de ces projets soient partagées avec le secteur privé et l'administration aux Pays-Bas et éventuellement à l'étranger. Un ambassadeur de Sentinels

a été désigné pour veiller à la visibilité des fruits des recherches de Sentinel et à leur accessibilité pour les entreprises[25].

Si indéniablement, ces initiatives améliorent les connaissances concernant la protection de l'infrastructure critique d'information, il n'a pas été possible de procéder à une analyse détaillée du partage de l'information sur les activités de recherche en matière de protection des infrastructures d'information critiques. Il semble ressortir que le partage d'information sur les recherches concernant la protection de l'infrastructure d'information critique laisse à désirer.

D'après l'analyse ci-dessus, les éléments qui suivent peuvent être considérés comme des exemples de bonnes pratiques pour le partage de l'information et les autres mécanismes pour la protection des infrastructures d'information critiques :

- Compréhension des délégations d'autorité et de responsabilités au sein des pouvoirs publics et dans le secteur privé.
- Sites des administrations clairs et permettant une navigation facile.
- Adoption d'une politique de partage d'information sur la sécurité plus ouverte que fermée, n'interdisant l'accès qu'aux informations sensible.
- Partenariats stratégiques et partage transnational d'informations diligent entre gouvernements et avec le secteur privé.
- Organisation de réunions régulières et bonne communication entre les principaux acteurs, notamment les responsables sécurité (CISO).
- Existence d'un CERT/CSIRT national de l'administration dans le cadre d'un réseau international de CERT/CSIRT.
- Clarté des canaux de partage d'informations sur la protection des infrastructures critiques d'information au sein des pouvoirs publics.
- Existence de mécanismes réciproques de partage d'information concernant la protection des infrastructures d'information critiques entre le secteur privé et les pouvoirs publics.
- Actions de sensibilisation et de formation aux mesures de protection de l'infrastructure d'information critique.
- Mesures pour cibler et accroître les ressources consacrées à la recherche scientifique en matière de sécurité des réseaux et systèmes d'information, en particulier les échanges de connaissances entre pouvoirs publics et secteur privé.

5. Les difficultés de la gestion transnationale des infrastructures d'information critiques, et les efforts des gouvernements pour les surmonter

Difficultés des échanges transnationaux

Tous les pays volontaires expriment des vues proches sur les différents aspects des difficultés transnationales auxquelles ils sont confrontés. L'Australie indique que l'absence de frontières sur l'Internet fait que les menaces dont font l'objet les systèmes et réseaux d'information critiques en Australie peuvent venir de partout. Le gouvernement du Royaume-Uni souligne qu'une partie des difficultés est liée à « l'intensification de la mondialisation, aux externalisations internationales et au fait que les infrastructures peuvent appartenir à des structures étrangères ». Le Canada énumère les principaux impératifs exprimés par l'ensemble des pays volontaires : « Mesure clé pour améliorer le PIE au Canada, le gouvernement a entrepris de renforcer sa capacité à prédire et à prévenir les cyberattaques provenant de l'intérieur ou de

25. Pour plus de détails sur ce programme et ses onze projets, voir: www.sentinels.nl (le texte est traduit en anglais).

l'extérieur du pays, dans la mesure où une grande partie de l'infrastructure critique du Canada est connectée aux réseaux internationaux ». Les États-Unis soulignent les éléments fondamentaux de la solution : « Du fait du caractère mondial et sans frontières du cyberespace, la coopération internationale et les mesures de collaboration sont indispensables pour édifier les relations nécessaires au renforcement de sensibilisation à la situation et l'amélioration des mécanismes de réponse coordonnée, de détection et de protection contre les incidents informatiques et de reprise des opérations, dans l'environnement informatique mondial. »

Les sept pays recensent quelques uns des principaux obstacles à la coopération et à la collaboration internationales :

- Capacités : L'échange d'informations en matière de veille, d'alerte et de réponse aux incidents constitue un aspect opérationnel important de la coopération internationale pour la protection de l'infrastructure d'information critique. Les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) chargées de représenter le gouvernement et les intérêts nationaux de chaque pays jouent un rôle important dans la détection, la réaction et l'atténuation des incidents informatiques. En l'absence d'une telle entité, la coopération et l'échange transnational d'informations sont difficiles. Les CSIRT nécessitant des capacités et des ressources spécialisées, la mise sur pied d'un CSIRT à compétence nationale peut être difficile.
- Échange de renseignements : La possibilité d'échanger des renseignements entre pays peut être compromise par la classification de certains renseignements, par des contraintes juridiques, et en raison des incertitudes quant à la divulgation ultérieure des renseignements échangés.
- Secteur privé : La participation du secteur privé dans la possession des infrastructures critiques peut être différente d'un pays à l'autre, de même que les mécanismes en matière d'engagement, avec une incidence sur la structure de leur administration et sur leur politique de protection de l'infrastructure d'information critique.
- Problèmes juridiques[26]: La protection des données peut restreindre le flux d'information qui peut traverser les frontières nationales ou économiques.
- Police : Les cadres juridiques applicables à la délinquance informatique revêtent une importance particulière pour la coopération. Or, dans de nombreux pays, les cadres juridiques nécessaires sont inexistants, inadaptés ou inappliqués, et il est difficile de traiter ces affaires sans cadres juridiques établis.
- Culture : Sachant l'importance qu'il y a à bâtir et à entretenir une culture de la sécurité face aux progrès rapides de la technologie, il peut être complexe et difficile pour de nombreux pays de décider de l'allocation du temps et des ressources en arbitrant entre priorités concurrentes.
- Mondialisation[27]: La multiplication des délocalisations et le contrôle étranger d'une partie des infrastructures compliquent la tâche des pouvoirs publics pour engager toutes les parties prenantes.
- Gestion des identités[28]: actuellement, les approches en vigueur en matière de gestion numérique des identités sont loin de permettre que l'on exploite pleinement le potentiel de l'Internet.
- Langues et fuseaux horaires : Les problèmes qui se posent depuis toujours du fait des langues et des fuseaux horaires différents sont aggravés par l'intensification de la mondialisation, par la

26. Extrait du texte du Royaume-Uni.

27. Adaptation du texte du Royaume-Uni.

28. Adapté du texte du Canada.

participation de masse de toutes les couches de la société (pas uniquement d'une minorité de personnes extrêmement qualifiées et/ou maîtrisant plusieurs langues) et par la rapidité des évolutions.

Le Canada et les États-Unis collaborent pour renforcer la protection des infrastructures d'information critiques au sein du Partenariat nord-américain pour la sécurité et la prospérité. Les Pays-Bas et le Royaume-Uni travaillent au niveau international avec des organisations telles que le CERT européen et les organisations chargées de la protection des infrastructures d'information critiques pour échanger des renseignements et confronter leurs pratiques. L'Australie, le Canada, le Japon, les Pays-Bas, le Royaume-Uni et les États-Unis participent tous au réseau international de veille et d'alerte, qui réunit des représentants des politiques, des CSIRT et des autorités de police de 15 pays. Les activités les plus ciblées se tiennent aux États-Unis où le NCSD prévoit, dans le cadre d'un Programme international, la collaboration avec des entités internationales, dans l'objectif d'établir un système national d'intervention pour la sécurité informatique et de réduire les vulnérabilités informatiques.

Réponses des pouvoirs publics

Il est difficile d'analyser les réponses fournies par les pays volontaires aux difficultés transnationales que nous venons d'évoquer. Bien qu'elles indiquent très clairement que les sept pays prennent des mesures, la réponse de chaque pays paraît dépendre du contexte de son fonctionnement plus général.

D'après l'analyse qui précède, les éléments suivants peuvent être considérés comme des exemples de bonnes pratiques pour répondre aux difficultés de la gestion transnationale des infrastructures d'information critiques :

- Existence à l'échelon national d'une capacité de veille, d'alerte et d'intervention en cas d'incident.
- Existence de mécanismes politiques et techniques d'échange de renseignements d'un pays à l'autre.
- Existence de cadres juridiques pour répondre aux aspects transfrontaliers de la délinquance informatique.
- Existence d'une culture de la sécurité.
- Participation à un réseau transnational de veille, d'alerte et d'intervention en cas d'incident.

Il serait envisageable d'élaborer un cadre stratégique, politique et opérationnel pour la coopération transnationale dans l'objectif de rendre plus efficaces et plus réactives les actions transnationales et la gestion du risque des infrastructures d'information critiques, ce qui serait souhaitable étant donné les relations d'interdépendance qui existent entre les pays. Une règle pour définir les événements et les circonstances auxquels un pays n'a pas la capacité de faire face seul pourrait être un bon départ pour la coopération transnationale. Un tel cadre pourrait s'appuyer sur certaines des principales conclusions de l'analyse, et notamment sur les recommandations suivantes :

- Adoption d'une définition commune internationale du concept d'infrastructure d'information critique.
- Adoption d'un seuil approprié pour solliciter la coopération des autres pays (par exemple définissant les événements et les circonstances auquel un pays seul n'a pas la capacité de faire face).

- Publication de la liste des agences de compétence sectorielle avec leurs rôles et leurs responsabilités dans la protection de l'infrastructure d'information critique afin d'améliorer la réactivité des actions transnationales.

- Élaboration et adoption d'un cadre commun pour les processus de gestion des risques, tel que le NIPP aux États-Unis (voir DSTI/ICCP/REG(2006)15/FINAL pour plus d'informations).

- Meilleure compréhension des menaces transnationales sur les infrastructures d'information critiques, qui peut permettre d'améliorer les stratégies et les politiques répondant à ces menaces (coopération plus étroite sur certaines des menaces plus répandues comme les maliciels).

- Établissement des vulnérabilités communes grâce à une coopération plus étroite, à la coopération et à la communication entre équipes d'intervention en cas d'incident de sécurité informatique (CSIRT), secteur privé et autres parties prenantes.

- Établissement d'un ensemble commun d'expressions et de définitions qui faciliterait la communication entre tous les participants et sur la base duquel ils pourraient décider des interventions (simplification du vocabulaire et de la terminologie).

- Organisation et renforcement du partage d'information au niveau opérationnel entre les CSIRT de compétence nationale afin de mieux gérer les crises et d'atténuer les dégâts potentiels en cas d'incident auquel un CERT opérationnel local n'aurait pas la compétence et les capacités suffisantes pour faire face.

ANNEXE A : GLOSSAIRE DES ACRONYMES

Généralités

BCP	Planification de la continuité des opérations
CIIP	Critical Information Infrastructure Protection (États-Unis Cyber Security)
CIO	Chief Information Officer - Directeur informatique
CSIRT	Computer Security Incident Response Team – Équipe d'intervention en cas d'incident de sécurité informatique
FAI	Fournisseur d'accès Internet
FIRST	Forum of Incident Response and Security Team
G8	Groupe des huit
GT/TI	Gestion de l'information/technologie de l'information
IC	Infrastructure critique
IIC	Infrastructure d'information critique
ISAC	Information Sharing and Analysis Center
ISTI	Sécurité des technologies de l'information
IWWN	International Watch and Warning Network – Réseau international de veille et d'alerte
MOD	Ministry of Defense
MSc	Maîtrise de sciences
OEA	Organisation des États américains
OTAN	Organisation du traité de l'Atlantique nord
PDCA	Plan-Do-Check-Act –Planifier-Faire-Vérifier-Agir
PIN	Personal Identification Number – Numéro d'identification personnel
PME	Petites et moyennes entreprises
R&D	Recherche et développement
S&T	Sciences et technologies
SCADA	Supervisory Control And Data Acquisition
TI	Technologies de l'information
VOIP	Voice Over Internet Protocol – (Protocole de) Téléphonie IP
WPISP	Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée

Australie

ASIO	Australian Security Intelligence Organisation
AusCERT	national Computer Emergency Response Team for Australia
CIAC	Critical Infrastructure Advisory Council
CIPMA	Critical Infrastructure Protection Modelling and Analysis
DCITA	Department of Communications, Information Technology (IT) and the Arts
DSD	Defence Signals Directorate
DSTO	Defence Science and Technology Organisation
EAGs	Expert Advisory Groups
ESNA	E-Security National Agenda
ESPAC	E-Security Policy and Coordination Committee
GovCERT.au	Australian Government Computer Emergency Readiness Team
IAAGs	Infrastructure Assurance Advisory Groups
ITSEAG	Information Technology Security Expert Advisory Group
PM&C	Department of the Prime Minister and Cabinet
TISN	Trusted Information Sharing Network

Canada

CAEIAE	Canadian Academic Excellence in Information Assurance Education
Can CERT	Équipe canadienne d'intervention d'urgence en informatique
CCRIC	Centre canadien de réponse aux incidents cybernétiques
CIEM	Centre intégré d'évaluation des menaces
COG	Centre des opérations du gouvernement
CST	Centre de la sécurité des télécommunications
GRC	Gendarmerie royale du Canada
MDN	Ministère de la Défense nationale
MSCP	Programme de coopération sur la sécurité de Microsoft
NCSD	National Cyber Security Division
NCSIP	National Sub-Committee on Information Protection
RDDC	Recherche et développement pour la défense Canada
SCRS	Service canadien du renseignement de sécurité
SPPCC	Sécurité publique et Protection civile Canada

Japon

APCERT	Asia Pacific Computer Emergency Response Team
CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response
FSA	Financial Services Agency
ISPC	Information Security Policy Council
JPCERT/CC	CSIRT (Computer Security Incident Response Team) CSIRT of the CSIRTs in Japanese
METI	Ministry of Economy, Trade and Industry
MIC	Ministry of Internal Affairs and Communications
MHLW	Ministry of Health, Labour and Welfare
MLIT	Ministry of Land, Infrastructure and Transport
NISC	National Information Security Centre
NPA	National Police Agency

Corée

CSPMC	Cyber Security Policy Mediation Committee
EC CPII	Executive Committee
KISA	Korean Information Security Agency
KRCERT	Korean CERT[29]
MIC	Ministry of Information & Communication
MOGAHA	Ministry of Government Administration & Home Affairs
NCSSC	National Cyber Security Management
NCA	National Computerization Agency
NCSMR	National Cyber Security Management Regulations
NCSPM	National Cyber Security Preparation Meeting
NCSSM	National Cyber Security Strategy Meeting
NSC	National Security Council

29. www.krcert.or.kr/index.jsp.

Pays-Bas

DigiD	National governmental authentication service
NAVI	Nationaal Adviescentrum Vitale Infrastructuren - Centre national consultatif sur les infrastructures critiques
NCTb	National Coordinator for Counterterrorism
NICC	National Infrastructure Cyber Crime – successeur du Centre national sur la criminalité dans le domaine des hautes technologies, NHTCC
SURFnet-CERT	Computer Emergency Response Team of SURFnet formerly CERT-NL

Royaume-Uni

BBC	British Broadcasting Corporation
BS7799	ISO/IEC 17799:2005 - Code of practice for information security management[30]
CBI	Confederation of British Industry
CESG	Communications Electronic Security Group
CNI	Critical National Infrastructure
CONTEST	UK Government Security Strategy
CSIA	Central Sponsor for Information Assurance
DSTL	Defense Science and Technology Laboratory[31]
DTI	Department of Trade and Industry
EEMA	European Electronic Messaging Association[32]
GCHQ	General Communications Headquarters
GIPSI	Cabinet Office/CSIA
GSi	Government Secure Intranet
IA	Information Assurance
IAAC	Information Assurance Advisory Council
IOD	Institute of Directors[34]
ITSOF	IT Security Officers' Forum
ISF	Information Security Forum[35]
ISPA	Internet Service Providers Association[36]
LRAG	Local Resilience Assessment Guidance
LRF	Local Resilience Forum
MI5	UK Security Services
MOD	Ministry of Defense
NCI	National Critical Infrastructure
NISCC	National Infrastructure Security Co-ordination Centre
NHTCU	National High Technology Crime Unit
NPA	National Police Agency
RRF	Regional Resilience Forum

30. www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.

31. www.dstl.gov.uk.

32. www.eema.org.

33. www.iaac.org.uk.

34. www.iod.com.

35. www.securityforum.org.

36. www.ispa.org.uk.

WAG	Welsh Assembly Group
WARP	Warning and Advice Reporting Point

États-Unis

CBK	Common Body of Knowledge
CIPB	Critical Infrastructure Protection Board
CI/KR	Critical Infrastructure/Key Resources
DHS	Department of Homeland Security
FIPS	Federal Information Publishing Standard
FISMA	Federal Information Security Management Act
GCC	Government Coordinating Council
G FIRST	Government Forum of Incident Response and Security Team
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
ITPC	Infosec Training Paths and Competencies
MITS	Management of Information Technology Security
MS-ISAC	Multi-State Information Sharing and Analysis Center
NADB	National Asset DataBase
NCAS	National Computer Alert System
NCRCG	National Cyber Response Coordination Group
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCC	(Critical Infrastructure Protection) Policy Coordinating Committee
PDD	Presidential Decision Directive
PUB	Publication
RMD	Risk Management Division
SCC	Sector Coordinating Council
SFS	Scholarship for Service
SSA	Sector-Specific Agencies
SSP	Sector-Specific Plans
TBS	Treasury Board Secretariat
TF-CSIRT	Task Force-Computer Security Incident and Response Team

ANNEX B: SUMMARY OF RESPONSES
(disponible en anglais uniquement)

For the purpose of comparing the development of policies for the protection of the CII in the seven OECD countries, the critical components of protection have been summarised into a preliminary question aimed at setting the stage and four additional key questions, the first three reflecting the existing and the fourth one relating to the major cross-border challenges facing the process of continuous improvement.

Preliminary question to set the stage: What are your national security policy and strategy and existing structure of authorities and agencies?

There are many influences that shape the way that governments respond to the need to protect their national critical infrastructure. Some of the major ones are the national security policy and strategy and the existing structure of authorities and agencies. These reflect the priorities, style and culture of the country and government setting the stage on which the protection of the national critical infrastructure policy will be developed and operated. These factors also have a strong influence on the interpretation of any analysis or comparisons between countries of how governments respond to their CIP challenges. They provide the contextual backdrop to the national critical information infrastructure protection measures in place.

National policy for critical information infrastructure protection is influenced by government's higher level national security policy and strategy on the one hand, and by the existing structure of their authorities and agencies, on the other. Providing background information on those elements sets the context for the volunteer countries' responses. It facilitates sharing of knowledge and experience, fosters a better understanding of CII protection, and facilitates international co-operation. Two major elements in this respect are:

- National policy and strategy.
- Government authorities and agencies.

CII protection is a component of national security policy and strategy. The policy and strategy are realised within the structure of government authorities and agencies which is influenced by national cultures. In this respect answers to the above-mentioned questions reflect, to some degree, the culture of the volunteer countries and the style of support and commitment from the government leadership. This impacts national CIIP policies and helps identify some of the commonalities and differences. A description of both the national policy and strategy, and government authorities and agencies in each volunteer country helps identify which critical success factors are in place in terms of:

- Clear CIIP policy and objectives.
- Approach that is consistent with the culture of all the participants.
- Visible support and commitment from the government leadership.

Australia

National security policy and strategy

In Australia, the Critical Infrastructure Protection National Strategy provides the overarching statement of principles for critical infrastructure protection outlines the major tasks within this area and assigns responsibilities necessary for their application. The Strategy defines national critical infrastructure as "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security." The Strategy advocates an "all hazards" approach to critical infrastructure protection.

The majority of Australia's critical infrastructure is owned and operated on a commercial basis. The Strategy is for use not only by all levels of government, but also by the owners and operators of infrastructure, their representative bodies, professional associations, regulators and standards-setting institutions.

Government authorities and agencies

Australia's Strategy for the protection of critical infrastructure relies on strong co-operative, co-ordinated and consultative relationships between the Australian Government, State and Territory governments, their departments and agencies. The roles and responsibilities of Australia's key national security agencies are listed below.

The Attorney-General, supported by the National Security Committee of Cabinet and other Ministers, has responsibility for operational co-ordination on national security issues. The Attorney-General's Department co-ordinates national security and crisis management arrangements and provides legislative advice on these issues.

The Department of the Prime Minister and Cabinet (PM&C) co-ordinates Australian Government policy responses to terrorism, participates in risk management decisions on dignitary protection, provides the secretariat for a number of high-level national security and counter-terrorism committees that give advice to the Government on national security policies and advises the Prime Minister on matters relating to national security.

The Australian Security Intelligence Organisation (ASIO) is the national authority for assessing threats to national security. ASIO collects analyses and distributes relevant intelligence to both government and industry.

The Australian Government Information Management Office and the Defence Signals Directorate contribute to the protection of the Australian Government's information infrastructure through the development of policies, standards and guidance that are applicable to all Australian Government agencies.

A number of other Australian Government agencies have sector-specific national security responsibilities arising from their roles in providing secretariat support for the advisory groups established under the Trusted Information Sharing Network for Critical Infrastructure Protection discussed below. These include but are not limited to the Department of Communications, IT and the Arts, the Department of Industry, Tourism and Resources and the Department of Health and Ageing.

Canada[37]

National policy and strategy

Canada recognises that strengthening the resiliency and protection of critical infrastructure (CI), including that of critical information infrastructure (CII), requires the engagement and close collaboration of all stakeholders. Canada is focusing on modernising its legislative and policy framework to facilitate partnerships and timely information sharing among CI and CII partners at all levels of government and the private sector.

As information sharing is an essential element of protection and assurance of CI and cyber CI, Canada's new (proposed) *Emergency Management Act* aims to facilitate the sharing of CI and emergency management information and expertise. This includes threats and warnings, vulnerability assessments, business continuity plans, best practices and lessons learned. A critical requirement for effective information sharing is the ability to protect sensitive CI, CII and emergency management information from inappropriate disclosure. The new (proposed) *Act* introduces specific protection from unauthorised disclosure for critical infrastructure information, including information concerning critical systems and networks. This is an important measure that is intended to support stronger co-ordination mechanisms nation-wide, and will form the basis of a consistent approach to information sharing between the Government of Canada and the private sector. Under the aegis of its National Critical Infrastructure Protection Strategy (under development), Canada will address the need for standardised protocols for information sharing and information protection for purposes of CIP, CIIP, and emergency management.

Canadian Security Policy is contained in[38] *Securing an Open Society: Canada's National Security Policy* and was released by the Government on 27 April 2004. The first-ever policy of its kind in Canada, it sets out a strategic framework and action plan designed to ensure that the Government can prepare for and respond to a range of security threats, including terrorist attacks, outbreaks of infectious diseases, natural disasters, cyber attacks on critical infrastructure and domestic extremism. One year later, in April 2005, Canada published a progress report: *Securing an Open Society - One Year Later: Progress Report on the Implementation of Canada's National Security Policy* which details progress in all areas of security including CIP.[39]

The Policy focuses on three core national security interests:

- Protecting Canada and the safety and security of Canadians at home and abroad.
- Ensuring Canada is not a base for threats to their allies.
- Contributing to international security.

The National Security Policy focuses attention and actions on building a more integrated security system and sets out specific actions in six key areas: intelligence, emergency planning and management, public health emergencies, transportation security, border security, and international security.

The Policy adopts an integrated approach to security issues across government, including those related to the security of information systems and networks. The focus of the Policy is on events and

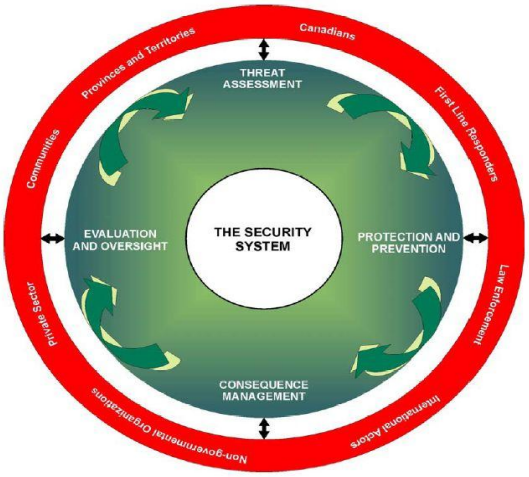
37. Taken from the Canadian response.

38. www.psepc.gc.ca/pol/ns/secpol05-en.asp

39. www.pco-bcp.gc.ca/docs/ministers/deputypm/secure_e.pdf

circumstances that are generally beyond the capacity of individuals, communities or provinces to address alone.

INTEGRATED SECURITY SYSTEM



Source: Canada.

Canada's federal Department of Public Safety and Emergency Preparedness (PSEPC), along with other federal departments and agencies with public safety and security responsibilities are responsible for developing and implementing the Policy.

The Policy sets out various processes for engaging the provinces, territories, and private sector partners in further defining and implementing the strategy and action plan. In particular, the Policy calls for the creation of a National Security Advisory Council (composed of security experts external to government), an advisory Cross-Cultural Roundtable on Security (composed of members of Canada's ethno-cultural and religious communities) and a National Cyber Security Task Force (with public and private sector representation). The latter will be charged with developing a National Cyber Security Strategy aimed at reducing Canada's vulnerability to cyber attacks and cyber incidents.

Since the release of the Policy, the Department has been working with its provincial and territorial partners to put in place various elements and components of the strategy. The Council, Roundtable and Task Force will work with the Department on an ongoing basis to advise on implementation aspects of the strategy going forward.

Government authorities and agencies

The following public bodies have been assigned specific roles and responsibilities under the Policy:

- Public Safety and Emergency Preparedness Canada (PSEPC)[40]
    - Development of operational standards and technical documentation relating to the protection and assurance of the critical networks,[41] information systems and other critical assets of the Government of Canada.

40. www.psepc-sppcc.gc.ca/index-en.asp

41. www.psepc-sppcc.gc.ca/prg/em/nciap/index-en.asp

- The Government of Canada has recently established a new Government Operations Centre (GOC) within PSEPC. Located in Ottawa, the GOC is now able to provide stable, around-the-clock co-ordination and support across government and to key national players in response to emerging or occurring events affecting the national interest. It also receives and issues information dealing with potential threats to the safety and security of Canadians and Canada's critical infrastructure.

    - The GOC is the hub of a network of operations centres run by a variety of federal departments and agencies including the RCMP, Health Canada, Foreign Affairs, CSIS and National Defence. The GOC also maintains contact with the provinces and territories as well as international partners such as the United States and NATO. It operates 24 hours a day, 7 days a week, gathering information from other operations centres and a wide variety of sources, both open and classified, from around the world.
    - The GOC deals with anything – real or perceived, imminent or actual, natural disaster or terrorist activity – that threatens the safety and security of Canadians or the integrity of Canada's critical infrastructure.

- Canadian Security Intelligence Service (CSIS)[42]

    - Investigation and analysis of physical and cyber threats to national security.
    - Threat and risk assessment.
    - Central index of security assessments.
    - The CSIS is linked into Canada's strategic-level operations centre, the Government Operations Centre (GOC).[43]

- Communications Security Establishment (CSE)

    - Development of operational standards and technical documentation as it relates to Signal Intelligence, Communication Security and ITS.[44]
    - Provides security engineering services.
    - Test, inspection and evaluation of IT products and systems to identify risks and vulnerabilities.
    - Certification of private sector test and evaluation facilities.

42. www.csis-scrs.gc.ca/en/index.asp

43. www.psepc.gc.ca/prg/em/goc/index-en.asp#1

44. www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg-e.html

- Royal Canadian Mounted Police (RCMP)
    - Lead department for federal law enforcement with a crime prevention mission.
    - Development of ITS operational standards and technical documentation as it relates to the application of access controls and biometrics, data forensics, media disposal, system monitoring, malicious software, major events, reviews, inspection and audits.

The Canadian federal government (PSEPC) has established a Canadian Cyber Incident Response Centre (CCIRC[45]) which will serve as the strategic level focal point for dealing with cyber threats and incidents impacting Canada's critical infrastructure 24 hours a day, 7 days a week. In this capacity, the Canadian Cyber Incident Response Centre (CCIRC) provides the following services to critical infrastructure owners and operators:

- Co-ordination and support for incident response efforts.
- Monitoring and analysis of the cyber threat environment ("watch and warning").
- IT security-related technical advice.
- National capacity building (standards, good practices, awareness, education).

A private sector company (EWA Inc) has been operating a Canadian Computer Response Team ("CanCert"[46]) since 1998. The initiative functions as a trusted centre at the operational level for the collection and dissemination of information related to networked computer threats, vulnerabilities, incidents and incident response for Canadian government, business and academic organisations.

Both CCIRC and CanCert are part of a worldwide network of "Certs" that collaborate and share security-related information on a 24/7 basis.

Japan

National security policy and strategy

The Information Security Policy Council (ISPC) and the National Information Security Center (NISC)[47] play important roles in issues of Critical Information Infrastructure Protection for the Japanese Government.

The ISPC is the central decision-making body for formalising information security-related policy measures. It has been established under the IT Strategic Headquarters since 30 May 2005. NISC is the operational arm of ISPC and is responsible for the central co-ordination of information security issues in the Japanese Government. NISC has been established in the Cabinet Secretariat of Japanese Government since 25 April 2005.

ISPC formulated "The First National Strategy on Information Security[48]," on 2 February 2006 as the mid- and long-term national strategy with an overview and basic principles of information security issues.

45. www.psepc.gc.ca/prg/em/ccirc/index-en.asp

46. www.cancert.ca/Home/Default.php

47. www.nisc.go.jp/eng/index.html

48. www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf

The term for this strategy is three years from FY2006 to FY2008. ISPC also formulated "Secure Japan 2006" on 15 June 2006 as a promotion plan for each fiscal year based on the mid- and long-term strategy. During these three fiscal years, the government will strengthen various relevant measures based on the National Strategy in order to establish a "new public-private partnership model" with all entities appropriately playing their roles.

In protection of the critical information infrastructure, ISPC formulated the "Action Plan on Information Security Measures for Critical Infrastructures[49]" on 13 December 2005. This addresses the rapid spread of IT usage and increasing IT dependence in the critical infrastructure sectors as well as growing interdependence among the critical infrastructure sectors.

This Action Plan is a sector plan of the National Strategy, and identifies 10 targeted critical infrastructure sectors[50] (*i.e.* information and communications, finance, civil aviation, railways, electricity, gas, governmental/administrative services, medical services, water works, and logistics) to ensure the level of information security. The Action Plan also identifies the causes of IT-malfunctions that can interrupt services and reduce the function of critical infrastructures which include not only intentional "cyber attacks" but also "unintentional (accidental) factors" and "(natural) disasters".

Government authorities and agencies

In addition to the ISPC and NISC, the Ministry of Internal Affairs and Communications (MIC), the Ministry of Economy, Trade and Industry (METI), the Ministry of Defence (MOD) and the National Police Agency (NPA) are designated as supporting agencies to the NISC and play major roles in information security.

Each critical infrastructure sector formulates protection measures under the supervision of the responsible department. Designated critical infrastructure sectors are:

- Information and Communications.
- Governmental/Administrative services (including local governments) (supervised by MIC).
- Gas, Electricity (supervised by METI).
- Finance (supervised by the Financial Services Agency (FSA)).
- Civil aviation, Railways, Logistics (supervised by the Ministry of Land, Infrastructure and Transport (MLIT)).
- Water works and Medical services (supervised by the Ministry of Health, Labour and Welfare (MHLW)).

49. www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf

50. In the future, considering the degree of change in the business environment and IT dependency, targeted critical infrastructure sectors would be reviewed.

Korea

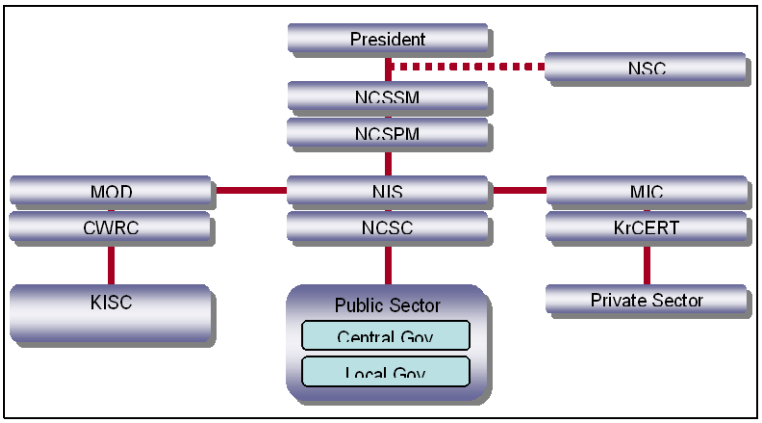
National security policy and strategy

Korean CIIP Policy is embodied in the Korean CIIP Act enacted and promulgated (Act No. 6383) in January 2001.[51] The CIIP Act was partially revised in November 2007. Under this Act the Committee on the Protection of II (CPII) was established under the Minister of the office for Government Policy Co-ordination to co-ordinate and adjust the tasks of establishing and executing the CII policies of the relevant ministries and institutes for the purpose of efficient information protection on a government-wide basis. Under this Committee there are two Executive Committees (EC) for the public and private sector.

After the hacking incidents that targeted some of the major government organisations in 2004, the government undertook to develop a strong and integrated management system on a government-wide basis for quick response and incident handling against cyber terror. The "National Cyber Security Management Regulations" [Title 141, 2005.1.31] were enacted to reform the basic structure of national cyber security.

Government authorities and agencies

Based on the regulation, the "National Cyber Security Strategic Council" was established for planning and improving the national cyber security structure and mediating roles and responsibilities among related government organisations. The, "National Cyber Security Meeting" was established in order to support the operation of NCSSC efficiently and effectively.



Source: Korea.

National cyber security management structure

National Security Council (NSC)

The office of the National Security Council (NSC) had managed cyber security for public sectors (finance, administration, diplomacy, energy, transportation) etc. centred around the Cyber Security Policy Mediation Committee (CSPMC) in general until the National Cyber Security Management Regulations were enacted. Since the enactment of NCSMR critical issues related to national cyber security have been handled by the National Cyber Security Strategy Committee.

51. Korean input.

National Cyber Security Strategy Meeting (NCSSM)

The main purpose of establishing NCSSM is to deliberate critical issues related to national cyber security. The meeting consists of the chairman, the director of National Intelligence Service, and the member(s) appointed by one of the vice ministers of the Ministry of Foreign Affairs & Trade, the Ministry of Justice, the Ministry of Defence, the Ministry of Government Administration & Home Affairs, the Ministry of Information & Communication, the director of the Office of the National Security Council, the chairman of the National Cyber Security Strategy Meeting and one of the vice ministers from the government bodies.

The role of the Meeting is:

- To plan and improve the structure of national cyber security.
- To deal with the policy issues of national cyber security and to mediate and clarify the roles and responsibilities among the organisations.
- To take proper actions on the President's orders regarding national cyber security.
- To inquire into certain issues raised by the chairman.

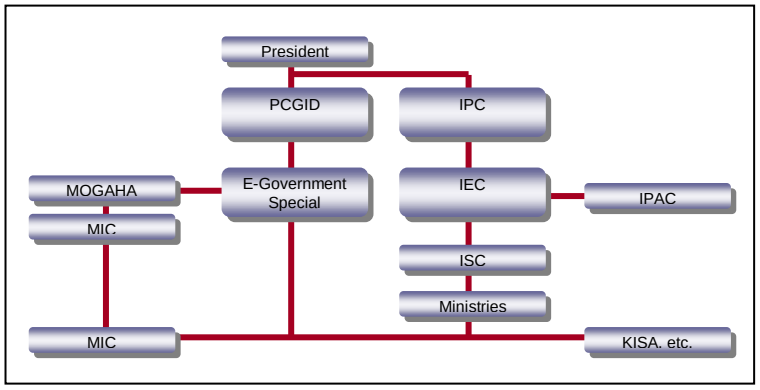
National Cyber Security Preparation Meeting (NCSPM)

NCSPM has been established to support the operation of NCSSM under NCSSM. The chairman is the director who is in charge of cyber security in NIS, and members of the Meeting are general directors from government organisations.

The roles of NCSPM are to enquire into:

- National cyber security management plans and measures.
- Action plans for decisions made at NCSSM.
- Mandated issues from NCSSM and orders from the chairman of NCSPM.
- Other issues raised by the chairman.

The structure of e-government security



Source: Korea.

E-government is defined as the service-oriented government that allows citizens to access diverse public services anywhere, anytime by putting these services on line. The aim of the e-government is to improve business efficiency and transparency. Furthermore, providing the world's better public services, maximising productivity, transparency and civil participation, and creating a better environment for businesses, are also the aims of e-government.

The e-Government roadmap was announced by "Government Innovation & Decentralization" in August 2003. The roadmap consists of 4 areas, 10 agendas, and 31 tasks. Among these 31 tasks the "National Security Management System" was included to consolidate the security of e-government. The "National Security Management System" will concentrates on two issues:

- Building a combined operational capability to manage national security and an integrated system for disaster and emergency response.
- Enhancing the national safety management service system.

E-Government Special Committee

The e-Government Special Committee under Government Innovation and Decentralization is a core government body for e-Government. It was founded in April 2003. The Committee consists of the chairman and 24 members from the public and private sectors.

As one of the presidential committees, the committee draws the roadmap, plans e-Government on a government-wide basis and checks and assesses the status of the 31 tasks on a quarterly basis. MOGAHA (Ministry of Government Administration and Home Affairs) and MIC (Ministry of Information and Communication) mainly support the e-Government Special Committee at the operational level. The function of executing the roadmap and government innovation is integrated into MOGAHA. NCA (National Computerization Agency) takes charge of technical support for e-Government.

In addition, MOGAHA has invested enormous efforts into information security. In 2005, MOGAHA reorganised itself to consolidate information sharing and establish information security infrastructure, such as information security policy and authentication.

The CIIP Act instructs the response system in the direction of close co-operation and co-ordination between the ministries and the institutes for stable management and operation of the CII. As a result, the CIIP committee was originally established under the direct control of the Prime Minister. In November 2007, the Act was revised and the Committee is now chaired by the Minister of the Office for Government Policy Co-ordination. The Committee co-ordinates and adjusts the tasks of establishing and executing the CII policies of the relevant ministries and institutes of the concerned authorities for the purpose of efficient information protection on a government-wide basis.

The mission of the CIIP committee is:

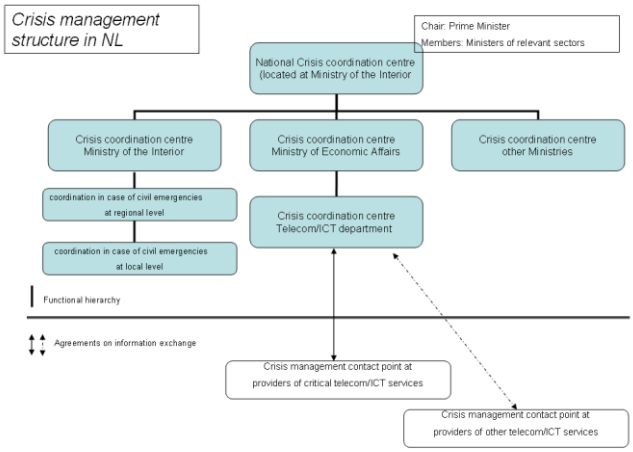
- To integrate and co-ordinate the plans of CIIP from the relevant ministries.
- To co-ordinate the protection policies for the CII.
- To deliberate a designation and designation-cancellation of the CII.

The Netherlands

National Security Policy and Strategy

This description is valid for any crisis or emergency situation that is likely to occur or is taking place in The Netherlands. A specific approach regarding crises or emergencies in information infrastructures is under development.

The Netherlands national emergency response plan includes a generic structure and information exchange that crisis response teams should follow. This umbrella plan is valid for public authorities tasked to participate during an emergency, regardless of the administrational level (national, regional and local). The development, implementation and maintenance of the umbrella plan are the responsibility of the Ministry of the Interior.



Source: The Netherlands

This national emergency plan, including procedures, tasks, responsibilities, etc is set out in the National Handbook on Crisis Management. Currently, the national emergency response plan is under major review to change the plan to the current (2007) perception of crisis management. A fully renovated national plan is scheduled for completion in 2008. During the review process the Handbook is "silent" and has been removed from ministries' websites.

In addition to the umbrella plan, each ministry has specific crisis response measures dedicated to the sector the ministry is responsible for. This tailors the measures to individual sectors. There is no formal oversight process to ensure that this is completed and kept up to date, each ministry is responsible for its own specific measures. However, the Ministry of the Interior requests at irregular intervals (couple of years) the ministries to report the current status, followed by giving advice on necessary adjustments.

The Ministry of Economic Affairs, as responsible authority for the telecommunications/ICT policy in The Netherlands, has developed and specific measures to respond to a crisis situation occurring in the telecommunications sector (regardless of the cause). One of the measures regarding critical telecommunications services and infrastructures is the National Continuity Forum Telecommunications. A

description of these measures is included in the paragraph further on in this paper on "Risk Management Framework".

In the case of an emergency or crisis so severe that national interests are threatened, the Prime-Minister may decide to declare (via a specific legal procedure) a State of Emergency. In this case the Minister of Economic Affairs has the authority to oblige any telecommunications operator to follow any order given by the Minister.[52]

A situation of "Exceptional Circumstances" can be declared by Royal Decree upon recommendation of the Prime-Minister. This action will be used only if the normal legal powers that exist are no longer sufficient to solve a crisis and the Minister of Economic Affairs has to issue instructions directly to telecom operators.

If a Decree is issued the government assumes full control of telecoms services and infrastructures. However this is only as far as public service providers and private networks are not affected by the Decree. This means that when a crisis occurs but not serious enough to justify a Decree the government has no legal powers to oblige the private providers to take specific measures. In practice it is not expected that a situation of "Exceptional Circumstances" will ever occur, it has not for the last 50 years. The government estimation is that only the realistic threat of traditional war will lead to the issuing a Decree.

The Minister of the Interior bears co-ordination responsibility for critical infrastructure protection in his capacity as co-ordinating minister for crisis management. The nature of this co-ordination is as follows:

- Furnishing a step-by-step plan that results in mapping out vulnerability and resistance.
- Offering help where topics are not exclusive to one particular sector and call for a joint approach.
- Investigating whether intersectoral harmonisation had taken place, and whether suggested protection measures have also been adopted by other sectors that are dependent on the critical product or service the measures intend to protect.

In summary the national policy on protection of critical information infrastructure is based on the policy on CIP.[53] A specific approach to the protection of critical information infrastructure will be developed in 2007.

Government authorities and agencies

In The Netherlands a national emergency response plan has been implemented which includes a generic structure and information exchange according to which a crisis response team should act. This umbrella plan is valid for public authorities tasked to participate in some way during an emergency, regardless of the administrational level (national, regional or local.) The development, implementation and maintenance of the umbrella plan rests with the Ministry of the Interior.

In addition to this umbrella plan, each ministry has implemented specific crisis response measures dedicated to the sector the ministry is responsible for. This allows the measures to be tailored to each sector.

52. See also www.ez.nl/content.jsp?objectid=150711&rid=150708 (English).

53. The national policy is described in a letter to the NL Parliament dated September 2005. For a detailed description of the relevant organisations see the "International CIIP Handbook 2006" describing the situation in the Netherlands.

The Ministry of Economic Affairs in its capacity as responsible authority for telecommunications/ICT policy in The Netherlands has developed and implemented specific measures to respond to a crisis situation occurring in the telecommunications sector (regardless of the cause).

In the case where an emergency or crisis is so severe that national interests are threatened, the Prime Minister may decide to declare (via specific legal procedure) a State of Emergency. In this case the Minister of Economic Affairs has the authority to oblige any telecommunications operator to follow any order given by the Minister.

The Minister of the Interior bears co-ordination responsibility for critical infrastructure protection in his capacity as co-ordinating minister for crisis management. The nature of this co-ordination is as follows:

- Furnishing a step-by-step plan that results in mapping out vulnerability and resistance.
- Offering help where topics are not exclusive to one particular sector and calling for a joint approach.
- Investigating whether inter sector harmonisation had taken place, and
- Whether suggested protection measures have also been adopted by other sectors that are dependent on the critical product or service the measures intend to protect.

The national policy on protection of critical information infrastructure is based on The Netherland's policy on CIP. The national policy is described in the annex of the letter to the NL Parliament (September 2005). A specific approach on protection of the critical information infrastructure has not yet been decided, but will be developed in 2007.

For a description of the relevant organisations please see the chapter from the "International CIIP Handbook 2006" describing the situation in the Netherlands.

United Kingdom

National security policy and strategy

The high level UK risk management strategy is contained in "Countering International Terrorism – The United Kingdom's Strategy".[54] This document, which addresses physical, personnel and electronic issues, includes unclassified details of the threat and response. The strategy and the programme to implement it (known within Government as CONTEST) are divided into four principal areas:

- PREVENT
- PURSUE
- PROTECT
- PREPARE

54. www.mi5.gov.uk/files/pdf/ct_strategy.pdf

The PROTECT strand includes the role of the National Infrastructure Security Co-ordination Centre (NISCC), which was established by the Home Secretary to promote the protection of the UK's Critical National Infrastructure (CNI) from electronic attack, and to report on the level of protection in place.

Government authorities and agencies

National Infrastructure Security Co-ordination Centre (NISCC)

In order to fulfil its remit, NISCC works through four broad workstreams: Threat Assessment; Response; Outreach and Research and Development (R&D).

- Threat Assessment – Using a wide range of resources to investigate, assess and disrupt threats.
- Response – Promoting protection and assurance by encouraging information sharing, offering advice and fostering best practice. This assurance process is high level using a standard set of assurance indicators, and does not amount to accreditation. The primary deliverable of the process is the NISCC Assurance Report.
- Outreach – Promoting protection and assurance by encouraging information sharing, offering advice and fostering best practice.
- R&D – Devising the most advanced techniques and methods to support efforts across all work streams.

NISCC is an inter-departmental centre which co-ordinates activity in support of this aim across a range of organisations. Each of these contributes resources and expertise to NISCC's programme of work according to its own remit, its own priorities, in relation to the challenge at hand, and depending on what value it can add.

Contributing departments are:

- The Security Service (MI5)[55]
- Communications Electronic Security Group (CESG)
- Home Office
- Cabinet Office Security Policy Division
- Civil Contingencies Secretariat
- Central Sponsor for Information Assurance
- Ministry of Defence (MoD)
- Serious Organised Crime Agency (SOCA)
- Department of Trade and Industry (DTI)
- Defence Science and Technology Laboratory (DSTL[56])

55 . www.dstl.gov.uk/

56. www.mi5.gov.uk/output/Page2.html

Security Service MI5

The Security Service is the UK's National Security Authority and is responsible for protecting the United Kingdom against threats to national security. The MI5 website provides information on the current major threats to UK security and practical advice to help businesses and organisations to protect against them.

Cabinet Office[57]

The Cabinet Office plays a central role in planning for emergencies and works with other government departments to ensure that the United Kingdom is prepared to deal with unexpected events.

The Cabinet Office co-ordinates a number of CIIP activities. One example is the Central Sponsor for Information Assurance (CSIA) which is a unit of the UK Government's Cabinet Office and works with partners in the public and private sectors, as well as its international counterparts, to help safeguard the nation's IT and telecommunications services.

The CSIA provides a central focus for information assurance in promoting the understanding that it is essential for government and business alike to maintain reliable, secure and resilient national information systems.

The CSIA encourages a 'culture of security' regarding information systems across central and local government, the private sector as well as to the general public.

Home Office - ITsafe[58]

ITsafe is a government service, launched on 23 February 2005, to provide both home users and small businesses with advice in plain English on protecting computers, mobile phones and other devices from malicious attack.

Department of Trade and Industry (DTI)

The supply of electronic communications networks and services is provided by private sector enterprises and is regulated within the framework set by European Directives, which includes specifically matters relating to resilience, emergency response and consumer protection. Beyond the specific mandatory requirements of the European regulatory framework, the approach of the UK authorities is to work with industry as far as possible on a voluntary basis in ensuring the safety, reliability and security of the networks and services. Sometimes this approach needs to be backed with specific legal provisions such as the Civil Contingencies Act 2004, which places obligations on utilities, including telecoms, in relation to civil protection, and gives ministers wide emergency powers to deal with regional and national emergencies.

The UK Industry Ministry works closely with the independent regulator, Ofcom, and the telecoms industry within a voluntary Emergency Planning Forum to exchange ideas, discuss incidents and impacts on industry and to plan for dealing with emergencies both within the requirements of the regulatory framework, but also on an extra-statutory basis *i.e.* voluntary to achieve a flexible and integrated approach without the need for prescriptive law wherever possible.

57. www.cabinetoffice.gov.uk/security_and_intelligence/

58. www.itsafe.gov.uk/about/index.html

Communications Electronic Security Group (CESG)

CESG[59] is the Information Assurance (IA) arm of GCHQ. It is the UK Government's National Technical Authority for IA, responsible for enabling secure and trusted knowledge sharing. The customers are central government departments and agencies and the Armed Forces. CESG also provides services to bodies in the wider public sector and to various private sector companies. These include local government, the health sector, law enforcement, and all essential services forming the Critical National Infrastructure, such as power and water. CESG gives authoritative advice on assessing current and foreseeable risks including:

- Technical advice.
- Documentation.
- Other services.

United States[60]

National policy and strategy

The term "critical information infrastructure" (CII) is not specifically referenced in the United States although the concept of CII is captured within the context of Critical Infrastructure Protection (CIP). Homeland Security Presidential Directive 7 (HSPD-7) identifies 17 critical infrastructure/key resources (CI/KR) sectors that the public and private sectors must work jointly to protect. Protection of the IT Sector and the cross-sector cyber infrastructure within all the sectors aligns with the concept of "critical information infrastructure" protection or in the United States, cyber security.

Government authorities and agencies

Department of Homeland Security (DHS)[61]

The Secretary for DHS has an overarching responsibility for co-ordinating national efforts to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary co-ordinates protection activities for 17 CI/KR sectors. In addition, the Secretary evaluates the need for and co-ordinates the coverage of additional critical infrastructure and key resources categories over time, as appropriate.

Consistent with the President's National Strategy to Secure Cyberspace ("the Strategy")[62], DHS maintains an organisation to serve as a focal point for the security of cyberspace in order to facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international entities and organisations.[63] Within DHS the National Cyber Security Division (NCSD) was created to focus on the task of co-ordinating the implementation of the Strategy to help protect the nation's cyber infrastructure and cyber-dependent assets.

59. www.cesg.gov.uk/site/about/index.cfm?menuSelected=0&displayPage=0

60. Adapted from the US Contribution.

61. See www.dhs.gov/dhspublic/

62. See www.whitehouse.gov/pcipb/

63. For more information visit www.whitehouse.gov/news/releases/2003/12/20031217-5.html

The organisation's mission includes two overarching priorities of *i*) Cyber risk management, and *ii*) A national cyber security response system.

Sector-Specific Federal Agencies

Sector-Specific Agencies (SSAs) are those Federal departments or agencies responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. They include the:

- Department of Agriculture.
- Health and Human Services.
- Environmental Protection Agency.
- Department of Energy.
- Department of Homeland Security
- Department of the Treasury
- Department of the Interior
- Department of Defence.

The SSAs collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including key persons and entities in their infrastructure sector. They conduct or facilitate vulnerability assessments of the sector and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

DHS released the National Infrastructure Protection Plan, known as the NIPP, on 30 June 2006 after consultation with industry. The NIPP formalises the collaboration between government and industry through the Sector Partnership Model with Sector Co-ordinating Councils (SCC) and Government Co-ordinating Councils (GCC) working together to address risk by analysing consequences, vulnerabilities, and threats. The NIPP provides a unifying structure for protection of the Nation's 17 Critical Infrastructure and Key Resources (CI/KR) sectors designated in HSPD-7, including the Information Technology Sector and the Internet. The NIPP calls upon each sector to develop a Sector Specific Plan based on the risk management framework. DHS is the Sector Specific Agency (SSA) responsible for both the Information Technology Sector and the Communications Sector and assists other sectors with the cyber elements of their infrastructure. The IT Sector, also referred to as the "IT Industrial Base," comprises the producers and providers of hardware, software, and IT systems and services, and the Internet.

All Federal department and agency heads are responsible for the identification, prioritisation, assessment, remediation, and protection of their respective internal critical infrastructure and key resources, consistent with the Federal Information Security Management Act of 2002 (FISMA).

Co-ordination with the private sector

DHS and the other sector-specific agencies collaborate with appropriate private sector entities; encourage the development of information sharing and analysis mechanisms, and support sector-co-ordinating mechanisms to:

- Identify, prioritise, and co-ordinate the protection of critical infrastructure and key resources.

- Facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and good practices.

Question 1: What does "critical information infrastructure" actually refer to in your country and what are your policy objectives? How does your government identify what constitutes CII?

The volunteer countries' responses have been collected under two main sub sections:

- Critical Infrastructure.

- Strategy and Policy.

The source material on Critical Infrastructure includes the volunteer countries' perspective on how they identify what constitutes their critical infrastructure leading on to what constitutes their critical information infrastructure. The responses on strategy and policy provide direction on how the volunteer countries tackle identifying the CII in terms of their different roles in risk management. The responses show that the volunteer countries have a similar concept of CII though there is no simple single definition of CII.

Australia

Critical information infrastructure

Australia's 'national information infrastructure' (NII) is a subset of the national critical infrastructure. It is made up of the electronic systems and infrastructure that underpin critical services such as telecommunications, transport and distribution, energy and utilities, banking and finance.

Australia's infrastructures[64] are deemed 'critical' if their failure would affect the entire economic and social system, or affect Australia's ability to ensure national security. Each of these infrastructures is increasingly dependent on information infrastructure for monitoring and controlling their operations, however, the information infrastructure is itself also reliant on access to electrical power and other services. The result is a complex set of interdependencies and vulnerabilities.

In September 2001, the Australian Government announced the E-Security National Agenda (ESNA) as a measure to create a secure and trusted electronic operating environment for both the public and private sectors. Protection of the NII was identified as a strategic goal of the ESNA. The major elements of ESNA focused on enhancing intelligence and response capabilities of key Australian government agencies, raising awareness of e-security issues across the economy, developing the e-security skills base and encouraging R&D in e-security. Funding was provided to a number of Australian Government agencies with security, law enforcement and national critical infrastructure protection roles to progress the Agenda.

Strategy and policy objectives

The Australian Government recognises that since 2001 the online environment has changed significantly. Its highly interconnected nature means that e-security threats to different segments of the Australian economy can no longer be addressed through separate discrete efforts. The protection of all Internet users, including home users and small and medium businesses, from electronic attacks is seen as

64. www.dcita.gov.au/__data/assets/pdf_file/20457/New_SFIE_July_2004_final.pdf

an important line of defence in the protection of Australia's national information infrastructure and the Government's own information and communications systems and technologies.

The increased risk in the electronic environment led to the Government initiating a review of the ESNA in 2006 to assess the adequacy of the Government's e-security policy framework and operational arrangements. The areas focused on during the review were the Australian Government's co-ordination and collaboration arrangements; protection of government-owned information and communications technologies and systems; co-operative arrangements with industry; law enforcement; raising awareness about e-security issues, particularly with home users and small and medium enterprises, international collaboration, and research and development.

A primary goal of the ESNA review will be to further enhance the protection of Australia's critical infrastructure, including the NII, from electronic attack.

Identifying the Australian NII

Identification of Australia's NII has been dependent on identification of the national critical infrastructure that it underpins. Risk assessments of critical infrastructure have been undertaken in a strategic context relevant to the community or sector concerned. That is, each sector and government was required to identify infrastructure critical to their mission. State and Territory governments identified critical infrastructure within their respective jurisdictions, and the Australian Government identified those elements of the critical infrastructure which are regulated at a national level, support national security and defence, the continuity of government, the delivery of its services, and any infrastructure of additional national importance.

Similarly, each critical sector was responsible for identifying infrastructure that is vital to the on-going continuity of supply to the community, particularly those that exhibit high vulnerability or where there is mutual dependence across the sector. The identification of critical infrastructure is an ongoing process and is reviewed regularly to keep abreast of changes to the infrastructure, both physical and logical, the ever-increasing dependency of the community, and the emerging/changing interdependencies between infrastructures.

The Australian Government is building a Critical Infrastructure Protection Modelling and Analysis capability to examine the primary dependencies and interdependencies between national critical infrastructures and the flow-on consequences of critical infrastructure failure. This will assist both government and industry in further evaluating their assessments of critical infrastructure.

Canada[65]

Critical Information Infrastructure

Canada defines its national critical infrastructure (NCI) as "those physical and information technology facilities, networks, services and assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada".[66] This includes physical and cyber components.

65. Canadian responses with additional research of Canadian Government websites.

66. First Canadian response document

In November 2004, PSEPC released a position paper on a national strategy for critical infrastructure protection.[67] The paper is intended to elicit feedback from stakeholder groups and to form the basis of a national strategy for critical infrastructure protection. The key outcomes that have been identified for the strategy include that:

- CI sectors and owners are aware of, accept and take action on the accountabilities, risks and vulnerabilities to their CI.
- The Government of Canada has an ongoing programme to assure its physical and cyber infrastructures and thereby demonstrates leadership to other sectors.
- New knowledge and tools for CIP are to be developed and shared.

The necessary processes for achieving these desired outcomes will be articulated in the strategy which is currently under development.

Canada's national critical infrastructure is made up of ten sectors:[68]

- Energy and utilities (*e.g.* electrical power, natural gas, oil production and transmission systems).
- Communications and information technology (*e.g.* telecommunications, broadcasting systems, software, hardware and networks including the Internet).
- Finance (*e.g.* banking, securities and investment).
- Health care (*e.g.* hospitals, health care and blood supply facilities, laboratories and pharmaceuticals).
- Food (*e.g.* safety, distribution, agriculture and food industry).
- Water (*e.g.* drinking water and wastewater management).
- Transportation (*e.g.* air, rail, marine and surface).
- Safety (*e.g.* chemical, biological, radiological and nuclear safety, hazardous materials, search and rescue, emergency services and dams).
- Government (*e.g.* services, facilities, information networks, assets and key national sites and monuments).
- Manufacturing (*e.g.* defence industrial base, chemical industry).

Strategy and policy objectives

Canadian strategy and policy objectives have as a priority the following elements:

- Setting a national direction for improving the resilience and assurance of CI and CII in Canada.

67. www.psepc-sppcc.gc.ca/prg/em/nciap/best_practices-en.asp#

68. www.psepc.gc.ca/prg/em/nciap/about-en.asp

- Strengthening the trust relationships and information sharing among CI and CII partners at all levels of government and the private sector.

- Addressing the interconnectedness and interdependencies across CI and CII sectors and across jurisdictions.

- Encompassing risk management principles and practices.

- Addressing all hazards.

Canada's critical infrastructure could potentially be affected by both physical and cyber threats. For example, electricity supply can be severely disrupted by a tornado (physical threat), a major accident (physical or cyber threat) or a computer hacking attack that disables an essential control system (cyber threat). The NCIAP takes into consideration all hazards.

Critical infrastructure protection can be defined as actions and programmes that:

- Identify the critical infrastructure and its specific components (human, physical and cyber).
- Assess vulnerabilities.
- Mitigate or take protective measures to reduce vulnerabilities.
- Better risk management.

Given the interdependencies and connections among critical infrastructures, an interruption of any one service could have a cascading effect and disrupt other essential services or systems. For example, during the 1998 Ice Storm, large segments of rural and urban communities were in the dark and without heat. Traffic and street lights were out. Banking and government services were interrupted. The disruption in one sector – electricity – affected a score of others, interrupting the delivery of important services upon which Canadians depend.

Japan

Critical information infrastructure

Although there would still be room to make consideration of what "critical infrastructure" is, it is also necessary to consider what "critical information infrastructure" means exactly. In the "Action Plan on Information Security Measures for Critical Infrastructures"[69], "Critical Infrastructures" is introduced as follows: "Critical infrastructures are formed by business entities providing highly irreplaceable services and are essential for people's social lives and economic activities. If an infrastructure's function is suspended, reduced or unavailable, people's social lives and economic activities will be greatly disrupted."

Strategy and policy objectives

In the Action Plan, the current target includes the following 10 sectors. "Information and Communications", "Finance", "Civil aviation", "Railways", "Electricity", "Gas", "Governmental /Administrative services (including local governments)", "Medical services", "Water works" and "Logistics". At each sector, targeted business entities[70] engaged in critical infrastructures and examples of

69. www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf

70. In the future, considering the degree of change in the business environment and IT dependency, target business entities would be reviewed.

target critical information systems are introduced in the Action Plan; for instance, in the information and communications sector, target business entities are main telecommunications and broadcasting companies, and examples of target systems are network systems, operation support systems, news/programme systems, and programming/operating systems.

These 10 target sectors, target business entities of critical infrastructure, and critical information infrastructure of each critical infrastructure are decided in consideration of the influence on people's social lives and economic activities, and will be continuously reviewed to correspond with the promotion and expansion of the use of IT and environmental changes of each service.

The policy objective of the Action Plan is to protect critical infrastructures from IT-malfunction out of failures occurring in each business sector of critical infrastructures, which may have a significant impact on people's social lives and economic activities.

The Action Plan shall also define independent measures that should be formulated by each business entity engaged in operating critical infrastructures to enhance business continuity. To ensure continuing service maintenance and rapid resumption in the case of IT-malfunction occurrence, business entities engaged in operating critical infrastructures should flesh out the details of the measures, along with formulating measures that should be taken by the government (especially the Cabinet Secretariat) [71] and each critical infrastructure sector consistent with current acts and guidelines of disaster-prevention plans. This would ensure information security measures of critical infrastructures are under close partnership with the public and private sectors.

71. Policy for information security measures for the central government computer systems, see: www.nisc.go.jp/eng/pdf/guidelines_sism_g_eng.pdf

Target critical information systems for each critical infrastructure sector

Sector		Threats, risks such as information system failure and illegal operation	Target business entities engaged in critical infrastructures, etc (Note 1)	Examples of target critical information system (Note 2)
Telecommunications		Stoppage of telecommunication service Problems with safe and stable supply of telecommunication service Stoppage of broadcasting service	Main telecommunication companies Main broadcasting companies	* Network System * Operation Support System * News/Program system * Programming/Operating System
Finance	Bank Life Insurance Damage Insurance Securities company Stock exchange	Stoppage of deposit withdrawal, fund transfer such as crediting and loan process * Stoppage of the paying of insurance amount * Stoppage of the buying and selling of valuable securities, etc.	Banks, cooperative banks, credit cooperative, agricultural cooperative, etc. * Life insurances, damage insurances, securities companies, etc. * Stock exchange, etc	*Accounting system * Fund bill system * International system * External connection system * Insurance system *Stock exchange system * Exchange system, etc (including services using open networks)
Civil aviation		*Delay and Cancellation of Operation *Problems with safe operation of aircrafts	*Main scheduled air carriers *Ministry of Land, Infrastructure and Transport (Air control, weather)	* Operation System * Booking and boarding system * Maintenance system * Cargo system * Air control system * Weather information system
Railways		* Delay and cancellation of train operation *Problems with safe and stable operation of trains	* Main railway companies such as each JR company and major private railway companies	* Train traffic control system * Electricity management system * Seat reservation system
Electricity		Stopping of electrical power * Problems with safety operation of electrical power plants, etc.	* General electrical power suppliers, Japan Atomic Power Co. and Electric Power Development Co., Ltd.	* Plant Control system * Plant Operation and monitoring system
Gas		* Stoppage of gas supply * Problems with safety operation of gas plants, etc	* Major gas suppliers	* Plant control system * Remote monitor/control system
Governmental/ Administrative services		* Problems with governmental/administrative services Leakage, sniffing and falsifying of personal information	*Each ministry and agency * Local governments	*Information system of each ministry and agency and local governments (corresponding to e-Government/ e-municipality)
Medical services		* Problems with operation at practice support division	* Medical institutions	* Electronic medical charts management system * Remote medicine system
Water works		* Stoppage of water supply by water line *Water supply with inappropriate water quality	* Water supply enterprises and city water supply enterprises (except for small scale ones)	* Monitoring system for water utilities and tap water. * Control system for water utilities, etc.
Logistics		*Delay and cancellation of transportation * Difficulty in tracing location of cargo	*Major distribution companies	* Management system for delivery and collection * Cargo tracing system * Warehouse management system

Note1 Targeted business entities shown in this table are business entities engaged in critical infrastructures which should be intensively implemented with relevant measures. In the future, considering the degree of changing in the business environment and IT dependency, target business entities shall be reviewed.
Note 2 Details of target critical information systems shall be determined by business entities engaged in critical infrastructures in consideration of examples of threats and dangers.

Source: Attachment 1 to Action Plan

Korea

Critical Information Infrastructure

Critical Information Infrastructure refers to an information management system or an information and communication network in public and private institutions that seriously affect national security, citizen's daily life, and national economic stability when cyber terror has occurred. Examples are as follows:

- Roads, subway, airports.
- Energy and water resources.
- Broadcasting, national map network.
- Nuclear energy, national defence related technology, government research institutions, etc.

The chief of the managing authority for each part of the CII establishes the protection measures for the part of the CII under their control based on the results of a weakness analysis and assessment. The respective managing authority then reports these measures to the appropriate central administrative authority (Ministry). The chief of the central administrative authority (Minister) collects and co-ordinates the protection measures reported by their managing authorities and reports their plans to the EC. The EC deliberates and determines the final protection plans. Finally the EC reports to the CPII and advises on any adjustment of government policy necessary.

Strategy and policy objectives

The strategic objective is for all Korean authorities related to national cyber security to mutually co-operate with each other to implement national cyber security policies effectively. The NIS will play a pivotal role to facilitate collaboration among the authorities. These policies will enable Korea to:

- Build systems that detect and share information against cyber terror.
- Analyse and disseminate cyber security related information.
- Prepare countermeasures for cyber security threats.
- Study cyber terror techniques and disrupt attacks.

The Netherlands

Critical information infrastructure

The critical information infrastructure of The Netherlands consists of the information-systems (software, hardware and data) that support one or more critical infrastructure(s) and the disruption or outage of which causes severe damage to the functioning of that dependent critical infrastructure(s).

Critical infrastructure[72] refers to products, services and the accompanying processes that, in the event of disruption or failure, could cause major social disturbance. This could be in the form of tremendous casualties and severe economic damage, or in terms of an extremely lengthy recovery period and a lack of any readily available viable alternatives, while we depend on these products and services.

Because the consequences of this critical infrastructure – or parts thereof – could be so dire for large segments of the Dutch population, extra attention must be given to its protection. Accordingly, this protection is designed to prevent disruption and concerns the protection against technical/organisational failings, overloading, and extreme natural phenomena or intentional or unintentional human action. In April 2002, the Critical Infrastructure Protection (CIP) project was set up to this end. The aim is to arrive at a coherent package of measures to protect infrastructure in both the public and private sectors, and to anchor this package in normal business operations.

Strategy and policy objectives

The Government is responsible for the continuity of critical information infrastructure. For the part of the critical information infrastructure that is owned or controlled by public organisations the government has full authority to execute risk analyses and to implement measures.

72. Letter to Parliament about CIP in The Netherlands – general part – September 2005.

For the part of the critical information infrastructure that is owned or controlled by private organisations or companies the government is responsible for the respective parties carrying out risk analysis and taking appropriate protection measures. To what extent the government is able to fulfil this responsibility depends on the regulation in force for the specific branch of organisations or companies. If regulation does not oblige companies to perform critical information infrastructure activities such as risk management or implementing continuity measures then the government performs an advisory role.

One of the factors in this field is a trial voluntary agreement between the government and several large providers of public ICT services and/or infrastructures to report disruptions or outages (above a certain level of severity). The processes and procedures developed under the four year trial voluntary agreement may form the basis for a generic guide for all operators of critical telecommunications services in the future.

At the end of 2001 the government started a national project to identify Critical Services and Infrastructures and carry out risk analysis. The criteria used to identify critical infrastructure components are the impacts on each of five categories when a service is disrupted: human casualties, zoological casualties, material damage, psychological/emotional damage and environmental damage.

The analysis also included the services within a critical sector and the interdependencies with other critical sectors. To manage the complexity of this process the focus was placed on identifying critical infrastructures and services and not specifically on critical information infrastructure.

Based on the outcome of this project the Ministry of Economic Affairs started a project to identify critical infrastructure and possible protective measures regarding the sub-sectors of the ICT sector that were labelled critical. Activities carried out were:

- Questionnaire to identify vital services.
- Questionnaire to identify vital nodes.
- Selection process to determine critical services/nodes (physical as well as logical) from the identified vital services/nodes.
- Study on the interconnection aspects of services and infrastructures.
- Questionnaire on the impact of disruption of each critical service/node.
- Selection of disasters or crises scenarios that could possibly happen as input for risk analysis.
- Vulnerability analysis of selected critical services/nodes.
- Listing realistic and proportionate recommendations to improve protection against disruption.

During 2006 the project to identify critical infrastructure evolved into a regular policy subject, with two lines of co-operation:

- A national working party made up of representatives of ministries covering critical sectors.
- A platform to consult with the private sector on activities to protect the critical infrastructure.

Both these are chaired by the Ministry of the Interior and Kingdom Relations.

Since the subject of the protection of the critical information infrastructure is most related to ICT the Ministry of Economic Affairs (in its responsibility for national ICT policy) is the lead organisation to take the initiative in co-ordinating specific critical information infrastructure matters. At the time of providing input to this report the ministry is in the planning stage, a number of specific activities are progressing but an overall policy is still under development.

United Kingdom

Critical information infrastructure

The UK Government views the CNI as those assets, services and systems that support the economic, political and social life of the United Kingdom whose importance is such that any entire or partial loss or compromise could cause large scale loss of life; have a serious impact on the national economy; have other grave social consequences for the community, or any substantial part of the community; or be of immediate concern to the national government.[73] The CNI includes ten "sectors" of economic, political and social activity in which there are critical elements. They are:

- Communications.
- Emergency services.
- Energy.
- Finance.
- Food.
- Government and public service.
- Public safety.
- Health.
- Transport.

Not every activity within these sectors is critical, but the application of the criteria outlined above assists Government and managers within each sector to identify where better to concentrate protective security efforts.[74]

There are variations in the definition of CII from country to country. However, the United Kingdom considers that, although flexibility should be preserved for countries to respond in a way they consider appropriate, a common understanding at international level of what CII refers to would help identify the risks to CII.

Strategy and policy objectives

The UK policy is to keep the composition and responsibilities of the CII flexible. This allows the United Kingdom to address a wider range of risks as they emerge. The UK definition of CII is based upon impact and likelihood. CII identification is considered to be part of the national risk assessment process which constitutes a holistic review of all the risks to life in the United Kingdom.

73. www.mi5.gov.uk/output/Page76.html

74. See also www.niscc.gov.uk/niscc/aboutCNI-en.html

In an emergency situation the UK Civil Contingencies Act enables the government, under emergency powers, to assume responsibility for the operation of CII organisations. Under this legislation there is a duty placed on industry to co-operate where reasonable.

United States

Critical information infrastructure

The term "critical information infrastructure (CII)" is not specifically referenced in the United States. However, the concept of CII is captured within the context of Critical Infrastructure Protection (CIP). Homeland Security Presidential Directive 7 (HSPD-7) identifies 17 critical infrastructure/key resources (CI/KR) sectors that the public and private sector must work jointly to protect. Protection of the IT Sector and the cross-sector cyber infrastructure within all the sectors aligns with the concept of "critical information infrastructure" protection or in the United States, cyber security.

Strategy and policy objectives

Policy objectives

In 1996, the position of national co-ordinator for security, infrastructure protection, and counter-terrorism (sometimes called the position of "cyber-czar") was created as part of the White House's National Security Council to oversee national policy development and implementation of CIP.

In 1998, President Clinton issued Presidential Decision Directive 63 (PDD 63) in response to the Oklahoma City Bombing. PDD 64 established CIP as a national goal, and called for a national capability to defend critical infrastructures against deliberate attacks by the year 2003. It identified major critical infrastructure sectors, and designates lead agencies to act as the liaison with the private sector operators for each infrastructure sector. It also designated lead agencies for special functions to co-ordinate government efforts, a Critical Infrastructure Co-ordination Group (CICG) to facilitate inter-agency co-ordination, and a National Infrastructure Assurance Council, composed of CEOs from all infrastructure sectors, to enhance public-private partnerships and advise the President on a policy formulation of a National Plan.

Under PDD-63, the National Infrastructure Protection Center (NIPC) expanded within the FBI to serve as a threat assessment center and include members of the FBI, DoD, Secret Service and CIA. The NIPC served as a national focal point for gathering information on threats to the infrastructures. Information Sharing Analysis Centers (ISAC) were also set up by the private sector in response to PDD-63 (for each infrastructure sector), and although maintained by DHS, ISACS are largely owned and operated by the private sector. The purpose of an ISAC is to promote two-way exchanges of information and analysis related to security.

The Critical Infrastructure Assurance Office, an interagency office housed in the Commerce Department, was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies. The office also helped co-ordinate a national education and awareness programme, and legislative and public affairs. The CIAO was later moved to DHS as part of the Preparedness Directorate.

In February 2003, President George W. Bush issued the *National Strategy to Secure Cyberspace* ("the Strategy") and shortly thereafter created the National Cyber Security Division (NCSD) under what is now the DHS Preparedness Directorate.

The Strategy[75] was developed under a White House advisory group called the Critical Infrastructure Protection Board (CIPB) and in consultation with government agencies, the private sector, and civil society. Once DHS was formed, the functions of the CIPB were absorbed into DHS. NCSD was created to focus on the task of co-ordinating the implementation of the Strategy to help protect the nation's cyber infrastructure and cyber-dependent assets.[76] After much consultation with industry and public and private stakeholders, the Strategy outlined five national priorities to address current and future threats and vulnerabilities in cyberspace:

- Priority I: A national cyberspace security response system

Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to be effective at a national level, the United States needs a partnership between government and industry to perform analyses, issue warnings, and co-ordinate response efforts. Privacy and civil liberties must be protected in the process. Because no cyber security plan can be impervious to concerted and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly.

- Priority II: A national cyberspace security threat and vulnerability reduction programme

By exploiting vulnerabilities in our cyber systems, an organised attack may endanger the security of our Nation's critical infrastructures. The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet. Lesser-secured sites on the interconnected network of networks also present potentially significant exposures to cyber attacks. Vulnerabilities result from weaknesses in technology and because of improper implementation and oversight of technological products.

- Priority III: A national cyberspace security awareness and training programme

Many cyber vulnerabilities exist because of a lack of cyber security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers (CIOs), chief executive officers, and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructures regardless of whether they exist within the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certification programmes for cyber security professionals complicate the task of addressing cyber vulnerabilities.

- Priority IV: Securing government's cyberspace

Although governments administer only a minority of the Nation's critical infrastructure computer systems, governments at all levels perform essential services in the agriculture, food, water, public health, emergency services, defense, social welfare, information and telecommunications, energy, transportation, banking and finance, chemicals, and postal and shipping sectors that depend upon cyberspace for their delivery. Governments can lead by example in cyberspace security, including fostering a marketplace for more secure technologies through their procurement.

75. Noting the increasing dependency of our nation on cyber infrastructure, the Strategy states, "The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States."

76. For more information visit www.whitehouse.gov/pcipb/

- Priority V: National security and international cyberspace security co-operation

America's cyberspace links the United States to the rest of the world. A network of networks spans the planet, allowing malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross-borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding and defending its critical systems and networks. Enabling our ability to do so requires a system of international co-operation to facilitate information sharing, reduce vulnerabilities, deter and prosecute malicious actors.

In December 2003, President Bush further solidified NCSD's mandate as a national focal point for cyber security by issuing HSPD-7 which calls for DHS to "…maintain an organisation to serve as a focal point for the security of cyberspace…." HSPD-7 also established a national policy for federal departments and agencies to identify and prioritise United States CI/KR and to protect them from terrorist attacks, and it laid out how DHS should address critical infrastructure protection, including "…a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and co-ordinate the protection of critical infrastructure and key resources".

US strategy

Among other activities for implementing HSPD-7, the Secretary for DHS produced a national plan, the National Infrastructure Protection Plan (NIPP), for protecting the country's critical infrastructure and key resources.

The National Infrastructure Protection Plan (NIPP) and the Sector-Specific Plans (SSP)[77]

The NIPP establishes the overarching concepts relevant to all CI/KR sectors identified in HSPD-7, and addresses the physical, cyber, human, and international dimensions required for effective implementation of comprehensive risk management programmes. The NIPP also specifies the key initiatives, milestones, and metrics required to achieve the United States CI/KR protection mission, including a comprehensive risk management framework.

The NIPP's complementary Sector-Specific Plans (SSPs) detail the approach to CI/KR protection goals, initiatives, processes, and requirements for each sector. SSPs are developed by the designated Federal Sector-Specific Agencies (SSAs) in co-ordination with their public and private sector security partners. They provide the mechanisms for:

- Identifying assets – including cyber assets, systems, and networks.
- Assessing risk including understanding threats, assessing vulnerabilities and consequences.
- Implementing information-sharing and protection measures within and across CI/KR sectors.

DHS, with support from all security partners, maintains and continuously improves a comprehensive inventory containing descriptive information on CI/KR assets, systems, and networks. Currently, this inventory is maintained in the National Asset Database (NADB). The NADB facilitates the analysis that identifies which of these assets, systems, and networks is nationally critical and therefore designated as CI/KR.

77. See the NIPP at www.dhs.gov/xprevprot/programmes/editorial_0827.shtm

The National Infrastructure Protection Plan (NIPP) describes in detail the role of cyber protection in CIP and outlines a plan to address it. The NIPP addresses reducing cyber risk and enhancing cyber security in two ways:

i) A cross-sector cyber element that involves DHS, as the SSA for the IT Sector, and private sector owners and operators; and

ii) A major component of the Information Technology sector's responsibility in partnership with the Telecommunications sector.

The NIPP further defines cyber security and cyber infrastructure as follows:

Cyber infrastructure includes electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as SCADA systems, and networks such as the Internet, are all part of cyber infrastructure.

Information and communications systems are composed of hardware and software that process, store, and communicate. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communication includes sharing and distribution of information.

The nation's cyber infrastructure, including the protection of critical infrastructure from disruption by cyber means, is a critical area that the United States has prioritised for protection and security. Cyber Security, as defined by the NIPP, is the prevention of damage to, unauthorised use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability. Cyber security has united once distinct critical information infrastructures, including emergency preparedness communications, and our critical digital and process control systems infrastructures.[78] Protection of these systems is essential to the survivability and reliability of the critical infrastructures of the nation and requires collaborative action by government, private sector, academia, and international entities.

Question 2: What role does the government play in the risk management of CII?

The responses to the question on the roles governments play in risk management of CII have been collected under three major components:

- Risk management strategy.
- Risk management framework.
- Risk management priorities.

The risk management strategy provides an insight into the individual national approaches. This leads into the individual national risk management frameworks. Each framework is a combination of organisations, processes and government standards leading to actions to improve CIIP and manage risk.

78. Control systems are computer-based systems used within many of our nation's critical infrastructures to monitor and control sensitive processes and physical functions. Control systems are implemented with remote access, open connectivity, and connections to open networks such as corporate intranets and the Internet, making them vulnerable to cyber and Internet-based attacks if proper cyber security measures are not implemented.

Australia

Risk management strategy

The Australian Government plays a lead role in the protection of critical infrastructure and, within that, the NII. Its responsibilities are to:

- Provide strategic leadership and co-ordination in the development and implementation of a nationally consistent approach to the protection of critical infrastructure.
- Provide co-ordination and national leadership in areas of joint responsibility.
- Liaise with and support State and Territory governments in critical infrastructure protection arrangements.
- Ensure protection of essential Australian Government services.
- Communicate relevant intelligence and information to stakeholders.
- Ensure that protective arrangements are in place for Australian Government-regulated sectors.
- Ensure that protective arrangements are in place to protect offshore assets and multi-jurisdictional critical infrastructure.
- Develop and maintain a database of nationally significant critical infrastructure.
- Co-ordinate liaison with overseas governments on critical infrastructure protection issues.
- Communicate required information to international organisations in accordance with treaty obligations.
- Promote aspects of critical infrastructure protection as national research priorities.
- Assist owners and operators of critical infrastructure in Australian Government-regulated sectors with the development, validation and audit of relevant plans.
- Promote the need for investment in resilient, reliable infrastructure with market regulators.
- Strengthen national capacity to safeguard information security, including the research and development and skills base; and
- Manage and co-ordinate public information and the media at a national level.

Owners and operators of critical infrastructure have responsibility for ensuring adequate security of their assets and actively applying risk management techniques to their planning processes. The Australian Government actively supports this activity through the Trusted Information Sharing Network for Critical Infrastructure Protection discussed later in this report.

Risk management framework

The Critical Infrastructure Protection Modelling and Analysis (CIPMA) Program[79] will deliver strategic support to decision makers involved in critical infrastructure protection, counter-terrorism and emergency management, especially with regard to prevention, preparedness and planning, and recovery.

The primary goal of the CIPMA Programme is to strengthen national security and better protect Australia's critical infrastructure by developing the capability to model, simulate, analyse and examine the primary dependencies and interdependencies between elements of Australia's critical infrastructure and the flow-on consequences of critical infrastructure failure.

The inter-departmental e-Security Policy and Co-ordination Committee, chaired by AGD, is the peak policy committee on protecting Australia's NII, and acts as a clearing house for policy initiatives.

Risk management priorities

The Australian Government[80] has adopted a five-point strategy for the protection of their NII:

- Policy development to include Commonwealth, industry and the States and Territories.
- Information collection and analysis.
- Defensive measures, including both protective security measures and awareness raising.
- Response arrangements ranging from technical responses to single incidents to crisis management arrangements; and
- Contingency planning covering both incidents and the wider impact of incidents.

Specifically, CIPMA is supporting decision making in government and business by helping to:

- Identify connections between critical infrastructure nodes and facilities within sectors and across sectors.
- Provide insights into the behaviour of complex networks.
- Analyse relationships and dependencies.
- Examine the flow-on effects of infrastructure failure.
- Identify choke points, single points of failure, and other vulnerabilities.
- Assess various options for investment in security measures, and
- Test mitigation strategies and business continuity plans.

The protection strategy in combination with the CIPMA programme leads to identifying the risk management priorities at national, regional and local levels.

79. www.tisn.gov.au/agd/WWW/TISNHome.nsf/Page/CIP_Projects

80. www.dsd.gov.au/infosec/infrastructure_protection.html

Canada

Risk management strategy

As Canada moves forward in developing its National Critical Infrastructure Protection Strategy, a key area of focus is the promotion of an integrated risk management approach that addresses all hazards to critical infrastructure, including both physical and cyber components, and that will be applicable across the national critical infrastructure in the public and private sectors.

Risk management methodology calls for the use of a consistent set of criteria to identify and determine the relative level of risk. The relative criticality and priority of CI and cyber CI resources and assets are identified by assessing the impact of their loss on the operation of a particular sector and other sectors, and the consequence of their loss. As more than 85% of Canada's critical infrastructure, including CII, is owned or operated by the private sector, governments rely on CI and CII owners and operators to make decisions about safeguarding their own critical assets and ensuring the continued viability of their services. Governments in Canada use established risk management approaches within their respective jurisdictions to fulfil their responsibilities for assurance of critical government assets and services to Canadians.

Critical infrastructure (CI) partners are encouraged to use a consistent set of criteria to identify and rank their CI and to determine the relative level of risk. The relative criticality and priority of CI assets are identified by assessing the consequences of their loss including the impact of their loss on the operation of the sector (and other sectors). Owners and operators make decisions about safeguarding and assuring their own CI assets.

In general, the components of the risk management for CI include:

- Understanding and raising awareness of CI and its interdependencies.
- Assuring CI through threat and vulnerability assessments, mitigation and preparation, research and development.
- Managing response and recovery through facilitating cross-sector co-ordination, response planning and education.

Another key element of risk management is information sharing. The more information available to organisations about potential threats and vulnerabilities, the better they understand the risk and can ensure the continuity of essential services. Information that needs to be shared includes information about threats, vulnerabilities, incidents, protection, mitigation measures, good practices etc. On this basis, information sharing can be viewed as a means to better manage risk, and in turn, help deter, prevent, mitigate and respond to threats. To this end, new governance mechanisms, information integration centres and modernising legislation are being studied.

Risk management framework

As part of on-going work on the National Critical Infrastructure Protection Strategy, a national-level integrated risk management framework for critical infrastructure is currently under development by the Department of Public Safety and Emergency Preparedness (PSEP) in co-operation with other federal departments and agencies, the provinces and territories and the private sector. This will be closely aligned with the National Cyber Security Strategy, which is also in progress. Once developed, the application of the framework will be encouraged throughout the public and private sectors.

Having a strong situational awareness of the risks and interdependencies of CI and cyber CI in Canada is the first step towards a comprehensive and nation-wide risk management process. In order to achieve a better understanding of the threat environment, as well as promoting a better integrated response capability, Canada has established the Government Operations Centre housed within the Department of Public Safety and Emergency Preparedness. The role of the Government Operations Centre (GOC) is to provide strategic level co-ordination and direction on behalf of the Government of Canada in response to emerging or occurring threats that affect the national interest. This response includes all hazards be they natural or man-made, cyber or national security. Other departments and agencies report within their area of responsibility to the GOC for inclusion in the whole of government threat identification and co-ordinated response. The GOC provides support to the government in five key functional areas: 24/7 monitoring and reporting of threats and on-going events that affect the national interest; developing situational awareness, risk assessment, alerting and warning products; event-specific contingency planning; cyber security activities; and response co-ordination.

As part of the Government Operations Centre, the Canadian Cyber Incident Response Centre (CCIRC) focuses on reducing risks to national critical infrastructure from cyber security threats. The CCIRC monitors the cyber threat environment on a 24/7 basis and is responsible for co-ordinating the national response to cyber security incidents. CCIRC delivers timely warnings of cyber security vulnerabilities and regular analyses of cyber threats. CCIRC is also the international point of contact for incidents in Canadian cyber-space.

Canada has also established the Integrated Threat Assessment Centre (ITAC), staffed with representatives of a broad range of federal departments and agencies as well as representatives from provincial law enforcement. The Centre's primary objective is to provide comprehensive threat assessments related to terrorism which are then shared within the intelligence community, with other government departments, provinces/territories, municipalities, international partners, and relevant first responders, such as law enforcement.

The Government of Canada has made a commitment to connect Canadians and provide them with online access to federal government services. Security and privacy concerns have been identified as key issues in this initiative. To assure uninterrupted services to the public, the Government has established a framework of policies and standards for IT security measures applicable to the Government of Canada, designed to minimise risks to federal Government CII. These are outlined in the paragraphs below.

Like other important issues that affect all Government departments and agencies, CII security requires a good governance framework, one that defines leadership responsibilities, articulates the roles of various lead agencies and each department, and sets accountability relationships. The *Government Security Policy (GSP)* provides the governance framework for all aspects of federal Government security, including CII. The Treasury Board Secretariat is responsible for the *GSP*, as well as for directing and co-ordinating the creation and update of operational and technical standards for federal IT security. The *GSP* and the IT operational and technical standards apply to all federal departments and agencies.

The *GSP* and its directives have three levels. At the top is the overall security policy that sets out the requirements for protection of federal government assets and personnel and the roles and responsibilities of lead agencies. The second level sets out the operational security standards and practices, and the third level the technical security standards and practices. The Treasury Board Secretariat is responsible for monitoring and implementation of the *GSP* and the state of security in the federal Government, including security of federal systems and networks, and for reporting on the state of Government security to the Treasury Board Ministers.

One of the operational security standards under the umbrella of the *GSP* is the Management of Information Technology Security (MITS) standard, developed by the Treasury Board Secretariat in consultation with lead security organisations and departments and agencies. The MITS standard defines baseline security requirements that federal departments must fulfill in order to maintain secure IT systems in the following areas: management controls, risk assessments, dealing with security incidents and weaknesses in systems, auditing security, and business continuity planning.

To date, TBS has also developed the following operational security standards:

- Administrative procedures for the Security of Information Act

  The purpose of this standard is to provide administrative procedures for departments that are listed in the schedule of the Act for the designation by notice of employees permanently bound to secrecy.

- Business continuity planning

  Departments must establish a Business Continuity Planning Programme to provide for the continued availability of:

  Services and associated assets critical to the health, safety, security or economic well-being of Canadians, or the effective functioning of government.

  Other services and assets when warranted by a threat and risk assessment.

  This standard provides direction and guidance to departments in establishing such a program.

Risk management priorities

As noted above, one of Canada's key priorities is to develop a national integrated risk management framework. As Canada moves forward on its National Strategy for Critical Infrastructure Protection, it is developing the means to apply risk management principles and business continuity planning approaches to help identify, prioritise and target CIP and CIIP gaps.

In collaboration with CI and CII partners, and taking into consideration work already accomplished by the federal, provincial/territorial and municipal governments, as well as in the private and not-for-profit sectors, the Department of Public Safety and Emergency Preparedness is seeking to develop risk analyses that address all hazards, including analysis of interdependencies at the national, regional and sectoral levels, and share the results with CI and CII stakeholders.

The proposed national risk management framework would also include the development of tools to promote the systematic application of risk management throughout the public and private sectors. While these tools will be available to all stakeholders, their application would be voluntary, and stakeholders will have the flexibility to customise, develop and implement a risk management approach that is appropriate to their needs.

The Auditor General of Canada conducted a government-wide audit of IT security in 2002 and again in 2005. Improvements in oversight and monitoring is one of the key recommendations in the 2005 report, which recommended that departments submit their annual plan to review IT security to TBS. These reviews include self-assessments, internal audits, and vulnerability assessments.

The Government has established plans to fully implement the new MITS standard by December 2006. To facilitate senior management understanding and involvement, TBS requires that departmental implementation plans be signed by the Deputy Head and submitted to the Treasury Board Secretariat for subsequent follow up and review. TBS is also co-ordinating implementation of the standard through bi-monthly interdepartmental meetings to work together to resolve common concerns and requirements.

The initial priority for MITS implementation is for departments to establish the fundamental security management processes and organisation required to effectively manage IT Security risks. Subsequent priorities are under review, but include senior management awareness and understanding of security risks.

The government is also placing increased priority on active security measures based on the "Prevent, Detect, Respond and Recover" paradigm. This includes new measures such as vulnerability assessments, intrusion detection and response, and business continuity planning. PSEPC has established the Canadian Cyber Incident response Centre to issue alerts and advisories, and co-ordinate incident response across the Government of Canada (GOC). PSEPC is developing a new security incident management standard and a CSE-lead project team has developed the architecture for an integrated government-wide incident detection and response capability.

Priority is also being placed on protection of critical infrastructure within the GOC. Departments are required to maintain an inventory of critical systems and services, PSEPC has initiated the GOC Critical Infrastructure protection project, and the Business Continuity Planning (BCP) standard requires departments to complete BCP for all of their critical systems.

As part of its financial and management oversight role, the Treasury Board Secretariat requires departments to report security spending and budgets as part of the corporate administrative and IM/IT spending. The results of an expenditure review identified a requirement for more consolidation of common services to improve efficiencies in the overall IM/IT budget, including security. This programme will significantly increase the level of common infrastructure and services across the GOC. Plans are being developed to implement additional common security infrastructure and services.

The GOC has no plans to set targets for IT security spending. The objective of collecting information on spending is to improve overall financial management, ensure alignment with government priorities, and to identify possible efficiencies. The target level of resources required for IT security is established by department senior management as part of overall corporate risk management. However, TBS will establish target levels of investment in common security infrastructure and services to improve government-wide efficiency and effectiveness.

Japan

Risk management strategy

The government formulated its "Action Plan on Information Security Measures for Critical Infrastructures" on 13 December 2005 to address information security issues of critical infrastructures.[81]

The Action Plan aims to protect critical infrastructures from IT-malfunction due to failures occurring in each business sector of critical infrastructures, which may have a significant impact on people's social lives and economic activities. The Action Plan shall also define independent measures that should be formulated by each business entity engaged in critical infrastructures to enhance business continuity. To ensure continuing service maintenance and rapid resumption in the case of IT-malfunction occurrence,

81. www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf

business entities engaged in operating critical infrastructures should flesh out the details of the measures, by formulating measures that should be taken by the government and each critical infrastructure sector. This would ensure the information security measures of critical infrastructures are in close partnership with the public and private sectors.

Risk management framework

In Japan, the risk management framework including critical infrastructures issue is stated in the "First National Strategy on Information Security" decided by the Information Security Policy Council.

The National Strategy stipulates that it is effective to divide the implementing entities into four areas: namely *a*) central government/local governments, *b*) critical infrastructures, *c*) businesses, and *d*) individuals, in order to attain the basic objective of creating an environment for the safe use of IT. Suitable measures to be taken by each entity are then considered.

In these four areas, critical infrastructures are regarded as the basis for people's social lives and economic activities and the most important task is to ensure stable services by protecting them from any threats.

However, at the time when the National Strategy was established, the situation showed such problems as a lack of consideration for the measures against IT-malfunctions caused by incidents other than intentional acts, such as cyber attacks, etc., and an insufficiently structured information sharing system between public and private sectors.

Therefore, the government will exert efforts from FY2006 to FY2008 focusing on the following policies:

a) Improvement of "Safety Standards" on information security assurance for critical infrastructures.

b) Enhancement of information sharing system.

c) Implementation of analysis of interdependence.

d) Implementation of cross-sectoral exercises.

Meanwhile, information security measures for critical infrastructures are set forth separately in the "Action Plan on Information Security Measures for Critical Infrastructures" (decision made by the Information Security Policy Council), and more specific measures will be implemented in line with the Action Plan.

In addition, assuming that it is important to establish a PDCA (Plan-Do-Check-Act) cycle in information security policies in order to create an environment for the safe use of IT, the Information Security Policy Council is of the view that "An ideal society and a scheme of policy evaluation from information security perspective" which stipulates necessary components at every stage of PDCA cycle, etc.

In the critical infrastructures area, the benchmark has also been established towards the goal of the "First National Strategy on Information Security", which will terminate in 2009. The evaluation will be implemented by progress analysis in each fiscal year in each of the four policy areas which are stipulated in the "Action Plan on Information Security Measures for Critical Infrastructures", (a) – d) stated above). The analysis will be implemented by monitoring the extent of realisation of the objectives.

Risk management priorities

The risk management priorities are different by cases. The "Action Plan on Information Security Measures for Critical Infrastructures" stipulates that support should be provided by the public and private sector in strengthening information-sharing frameworks to make the business entities engaged in critical infrastructures work more smoothly.

Especially, regarding the information about IT-malfunction, the following three actions are critical: *i*) preemptive prevention of IT-malfunctions, *ii)* prevention of expansion of suffering and rapid resumption, and *iii)* prevention of recurrence through analysis/verification of causes of IT-malfunctions. The government and related entities should provide necessary information if requested, and every critical infrastructure ensures the information sharing frameworks within those business entities engaged in critical infrastructures and interdependent critical infrastructures sectors.

Korea

Risk management strategy

Korea has adopted a methodology of weakness analysis and assessment. Its purpose is to recognise the diversified risk factors including electronic intrusion incidents that affect the stable operation of the CII. It is also necessary to identify, analyse, and assess the susceptibility of the CII to threat factors, and the extent of any effects caused by intrusion incidents on the infrastructures (scale and size of damage).

Risk management framework

The Managing Authority shall execute a precise weakness analysis and assessment of the infrastructures concerned, and establish proper protection measures in accordance with the results every two years.

Stage 1: Planning weakness analysis and assessment

The Managing Authority organises a task force dedicated to the entire procedures for the weakness analysis. The task force is responsible for establishing and executing a weakness analysis and assessment plan that covers the scope, inspection items, procedures, output, period, human resources and budgets of the concerned CII. The Managing Authority is not required to organise a task force when the authority entrusts the weakness analysis and assessment to an independent institute.

Stage 2: Selection of targets for weakness analysis and assessment

The Managing Authority shall verify the configuration and the job details of the CII for weakness analysis and assessment, select the targets for the tasks, and compile the list and configuration charts of the infrastructures. The scope of the targets includes the systems, software, data, documents, and facilities of the critical information and telecommunication infrastructure as well as the systems for supporting operation of the facilities. Priority shall be assigned to the assets concerned taking into account the effects of risks such as damage to, disclosure of, or alterations to the assets in the tasks.

Stage 3: Analysis of threat factors and weakness

1. Analysis of threat factor

Identification of actual or potential threat factors to the CII. A threat factor is defined as a cause or an action likely to damage the infrastructures including fire, user error, worms and viruses. Then define the

threat level measurement criteria and measure the threat level taking into account the cause and frequency of identified threat factors and effects upon intrusion. A higher threat is the level to be allocated to threats newly identified or significant threats in the work environments.

2. Analysis of weakness

Analysis of weakness examines the infrastructure, and all technical, managerial and physical weaknesses:

- Checking technical weaknesses through automatic inspection, making use of the system/network weakness inspection tools, manual inspection with checklists, log analysis and simulated hacking.

- Inspection of managerial weakness by checking execution of the information protection policies, as well as the standards, guidance and procedures, through document reviews and interviews with responsible staff.

- Defining the weakness assessment criteria, taking into account the effects of incidents on the asset weakness in the tasks concerned, based on the inspection results of the weakness items, and measuring the level of the technical, managerial, and physical weaknesses.

- Understanding and analysing the appropriateness, efficiency and probable loopholes in the existing protection measures for the purpose of mitigating the threat factors and the weakness of the assets.

Stage 4: Weakness assessment (Assessing risk level)

- Comprehensive assessment of weakness based on the data obtained from analysis of the assets, threats, and weakness as well as the analysis results.

- Defining the criteria for determining the weakness assessment (risk level assessment) level taking into account the criticality of the assets, the threat and weakness level and the relationship between the threat factors and the weakness.

- The Managing Authority assigns the assessment level to the weakness taking into account the asset criticality, the threat level, the weakness level, and the appropriateness and execution of the existing protection measures.

- The Managing Authority records the actual meaningfulness of the assessment level, and the assessment opinion on the probability of risks to the tasks.

Stage 5: Establishing the protection measures

Defining efficient protection measures and adapting the execution methods of the measures taking into account the available assets, asset criticality, and the costs of protection measurement to the Managing Authority.

Risk management priorities

The priorities in Korea are reflected in the general planning for the future that includes:

- Perfecting the automation of Korean security management systems.

- Expanding the government sources for collecting cyber terror-related information by building strong co-operative relations with the United States, the United Kingdom, Germany, France, Japan, Australia, Canada, and other countries.

- Preparing tailored security countermeasures.

- Collaborating with the private sector to improve the ability to collect and analyse cyber threats.

- Investment in developing advanced technologies against cyber terror.

These priorities are reflected in specific national programmes including:

- Ministry of Defence: improve the response capability to cyber terror by building a solid national defence information security system that includes recruiting and training enough military information security specialists and expanding their ability to adapt to new technologies.

- Ministry of Information and Communication: consolidate its ability to analyse cyber terror using the Korean Information Security Agency (KISA) and improve public awareness of cyber terror by diverse means such as advertising and child education.

- National Police Agency: the "Digital Evidence Analysis Center" to facilitate advanced technology-based criminal investigation was established in December 2004. The NPA will continually enhance the structure, human resources and improve digital evidence-related laws and regulations.

The Netherlands

Risk management strategy

The Government is responsible for the continuity of the critical information infrastructure. For the part of the critical information infrastructure that is owned or controlled by public organisations the government has full authority to execute risk analyses and to implement measures.

For the part of the critical information infrastructure that is owned or controlled by private organisations or companies the government is responsible for ensuring that the respective parties carry out risk analysis and take appropriate protection measures. To what extent the government is able to fulfil that responsibility depends on the regulation in force for that specific branch of organisations/companies. If regulation does not oblige companies to perform activities on critical information infrastructure, such as risk management or implementing continuity measures, the government performs an advisory role regarding these issues.

One of the issues in this field is also the agreement between the government and large providers of public ICT services and/or infrastructures to report disruptions or outages (above a certain level of severity).

Risk management framework

Several recommendations described in the Letter to the NL Parliament (September 2005) on the Project on critical infrastructure protection implementation were started in 2006. A number of

recommendations on awareness raising were taken up by organisations such as ECP.nl[82] or through the national project Digit-aware ("Digibewust"). Related to raising awareness is the availability, for public parties, in particular SMEs, of advice on all kind of specific CIP matters. A dedicated advisory function was established under co-ordination of the Ministry of Interior: the National Centre for Advice on Critical Infrastructures (NAVI, Nationaal Adviescentrum Vitale Infrastructuren). All other ministries support NAVI by making expertise available through background information or human resources. ICT is one of the main topics covered by NAVI.

The recommendations on improving the continuity of public ICT services were taken on board by the National Forum on Continuity of Telecommunications (Committee chaired by Ministry of Economic Affairs with mandatory membership for providers of critical ICT services).

Also in 2006, an initiative was started with respect to cyber crime. Modelled along the lines of NISCC in the United Kingdom the National Infrastructure Cyber Crime (NICC) was established. The objectives of NICC are to bring together, in a confidential environment, public and private parties from each sector to exchange best practices, combine experience in fighting cyber crime and create information exchange points on threats or real life attacks based on information from national intelligence or CERTs. Since 2006 a number of information exchange points have been established to support the financial sector, the electricity sector and the sector providing drinking water.

At the beginning of 2006 the Project on National Security, co-ordinated by the Ministry of Interior and in which every ministry participates, was started. The project carries out activities in the field of strategy towards improving the robustness of critical infrastructures and creating the tools needed to achieve this. To the extent possible both public and private organisations are participating in working groups on selected subjects such as capacity planning. These working groups are focussed on public organisations at all levels to able them to carry out security measures, contingency planning best practices and such like.

One of the subjects under study in 2006 was Digital Paralysis that identified possible threats, risk, protection measures and resources where there might be gaps in government responsibilities. The ministry of Economic Affairs was the leading participant in this study, supported by representatives from users and the ICT sector. The recommendations included:

- Improving information security at the lower levels of public administration.
- Adapting legislation to be able to fight cyber crime more effectively.
- Increasing the effort on national policy on fighting cyber terrorism.
- Improving co-ordination between ministries and their agencies and/or lower level authorities on projects, activities, studies, international forums in order to minimise overlaps.

Most of the recommendations are already taken onboard by the ministries concerned (*e.g.* NICC, NCTb), others will be worked on during 2007/2008.

A CERT is operational for governmental organisations, GovCert.NL. One of its tasks is to monitor any suspicious developments (viruses, DDoS, etc) in Internet traffic and if one is discovered alert the

82. A public-private partnership to co-operate on important preconditions and breakthroughs regarding digital economy and society and can be seen at: www.ecp.nl

National Co-ordination Centre, which in its turn will inform all ministries. They are then responsible for how and when to alert their sector (public and private) organisations, including the public. This alert function is performed by the crisis management unit at each ministry.

Approximately 20 agencies in the Netherlands are involved in the fight against terrorism. The National Co-ordinator for Counterterrorism (NCTb) was appointed to improve co-operation between all these agencies. The NCTb is responsible for:

- Analysing intelligence and other information.
- Policy development.
- Co-ordinating anti-terrorist security measures.

By combining these tasks the capacity and effectiveness of the government effort to combat terrorism has been improved.

The office of the NCTb and its staff fall under the responsibility of two ministers: the Minister of Justice (the lead minister for counter-terrorism) and the Minister of the Interior and Kingdom Relations. For the more physical threats there are sufficient legal and non-legal instruments to intervene in a timely fashion and adequate security is provided for potential targets. Supplementary legislation is also being prepared to disrupt potential acts of terrorism.[83]

One of the activities of the NTCb is the Counterterrorism Alert System which is an alert system for the government and economic sectors. It sends out an alert to the operational services and economic sectors in the event of an increased threat. This enables pre-emptive measures to be taken quickly in order to minimise the risk of terrorist attacks and limit the potential impact. Information to the public is given when and if necessary.

In case a terrorist threat is aimed at ICT infrastructure or ICT usage an alert message is sent out by the NCTb. Appropriate action then starts in co-operation with the organisations most relevant to the threat. This includes the crisis management department of the ministry of Economic Affairs (responsible for national policy on public telecommunications service provisioning), GovCert.NL (Cert supporting governmental organisations) and other relevant ministries responsible for the threatened sector.

For the use of ICT in public organisations, the Ministry of the Interior has put into place requirements with regard to the security of ICT components that are used in public organisations. In addition it has put in place requirements on procedures for information systems in the field of exchange, storage, retrieval, etc. ("Requirements on Public Service Information Security" (in Dutch: "Voorschrift Informatiebeveiliging Rijksdienst").

In addition the Ministry of the Interior has put in place requirements on information systems that support applications in the e-Government field. These requirements address all aspects of the communication between users and the government administration such as: privacy, availability, integrity, accessibility, reliability and alike. These requirements are mandatory at national government level. Co-ordination takes place in working groups made up of the IT managers from individual ministries.

On other levels (regional, local, independent authorities etc.) compliance is the responsibility of the individual public organisation. There are no central government compliance audit or approval procedures.

83. http://english.nctb.nl/about_the_nctb/

The Ministry of the Interior uses agreements between the Ministry and the lower level organisations to satisfy itself on compliance.

A Government-wide Shared Service Organisation for ICT called "GBO.Overheid" has been established to take on a number of tasks related to electronic government (e-government). GBO.Overheid is responsible for the tactical and operational management and maintenance of generic key shared services for e-government. These concern the following:

- The administration of DigiD, a national governmental authentication service.
- An infrastructure for the exchange of data through the government transaction portal (GTP); and
- Forum standardisation; Security tasks (GOVCERT.NL and the policy authority for PKI based security services).

GBO.Overheid guarantees cost-effective management of key generic services for e-government, enforces integration of the different services and provides for a constant quality in the provisioning of government services. GBO.Overheid is a single unit within the Ministry of the Interior, enabling the direct control and central auditing of the activities of GBO.

Risk management priorities

The scope of activities carried out by several projects concerning CIP includes an all-hazards approach. There is no specific priority for ICT subjects. For 2007, the activities on raising awareness on information and IT security will continue on from 2005 and 2006. The project on National Security for 2007/2008 will focus on contingency planning, best practices and on agreements on Notice and Take Down (closing down by ISPs or hosting providers of websites which spread malicious software, SPAM, harmful content etc.)

Performance and achievements are reported by the responsible ministry to Parliament annually, generally in co-operation with the Ministry of the Interior.

United Kingdom

Risk management strategy

The PROTECT strand of the UK CONTEST strategy is concerned with reducing the vulnerability of the United Kingdom and UK interests overseas. This covers a range of issues including:

- Strengthening border security – so that terrorists and those who inspire them can be prevented from travelling to the United Kingdom and the United Kingdom can get better intelligence about suspects who travel, including improving identity management, for example by the use of biometrics.
- Protecting key utilities – working with the private sector.
- Transport – reducing the risk and impact of attacks through security and technological advances.
- Crowded places – protecting people going about their daily lives.

Risk management framework

The UK Government aims to ensure that all organisations have clear and effective risk assessment processes in place. They work at all levels to assess and mitigate the risk from emergencies facing the country as a whole.

In the context of emergency preparedness, risks are those hazards (*i.e.* non-malicious events such as flooding) or threats (*i.e.* malicious events such as terrorist attacks) which could adversely affect an organisation and its ability to carry out its functions. Risk is a function of the likelihood and impact of a given hazard or threat. This reflects, on the one hand, the possibility of an emergency occurring which could adversely affect the organisation *(e.g.* flooding or nuclear accident). And, on the other hand, the extent to which the event impacts upon the organisation (*e.g.* lack of staff, disruption to power supply, damage to facilities).

Risk assessment

Effective identification and assessment of the risks which could potentially seriously obstruct an organisation in the performance of its functions should underpin all other emergency planning and business continuity management processes. The Government advocates a six-step risk assessment process, which is widely recognised as being good practice. The steps can be split into three phases:

4. **Contextualization** involves defining the nature and scope of the risk and agreeing how the risk management process will be undertaken.

5. **Risk evaluation** covers the identification of those threats and hazards that present significant risks, analysis of their likelihood and impacts, and the combination of these values to produce overall risk scores.

6. **Risk treatment** involves deciding which risks are unacceptably high, developing plans and strategies to mitigate these risks, and then testing the plans and any associated capabilities.

Risk assessment should drive a standard emergency planning process in forming emergency plans (and Business Continuity plans) which are then tested through audit and validation exercises. Regular updating of the risk assessment in turn leads to revision of plans and further testing. The risk assessment should also respond quickly to changes in the risk environment. This means that the process should be iterative and contain risk monitoring and updating mechanisms.

Risk assessment at the local level

The Civil Contingencies Act places a risk assessment duty on all Category 1 responders. Category 1 responders assess risk as often as is necessary to ensure that they are in a reasonable position to maintain and update their emergency plans and to perform the civil protection duties under the Act, including the duty to maintain business continuity plans.

As part of the Local Resilience Forum[84] (LRF) process (see the Co-operation section), Category 1 responders must co-operate with each other in maintaining the Community Risk Register (CRR). The CRR provides an agreed position on the risks affecting a local area and on the planning and resourcing priorities required to prepare for those risks.

84. Details of local resilience forums.

It is recognised that requiring each Category 1 responder to perform the risk assessment duty in isolation would lead to a wasteful duplication of resources. It is more efficient, and effective, for individual Category 1 responders to fulfill their risk assessment duties by participating in a collaborative exercise that results in a single, collective risk assessment.

Category 1 responders also have a statutory duty to publish their risk assessments, to the extent necessary to reduce the impact of an emergency on the community.[85]

Risk assessment at the regional level

The regional tier is a crucial part of England's civil protection framework, ensuring co-ordination between representatives of Category 1 and 2 responders and central government bodies. For more information on the regional tier, go to the English Regions[86] section.

Regional Resilience Forums (RRFs) have a key role in developing regional risk assessments which provide a judgement on the likelihood and impact of emergencies that could occur in the region. The regional risk assessments build on the local risk assessments produced by LRFs, and equally ensure consistency and co-ordination with the central guidance provided by the Government on the risks facing the United Kingdom as a whole. Risk likelihoods are assessed for a five-year period so that the risk assessment will support strategic planning for the medium term, informing decisions about capability development.

Risk assessment in the Devolved Administrations

It is equally important that organisations within the devolved administrations conduct effective risk assessment. The Devolved Administrations section provides more detail on the extent to which the Civil Contingencies Act duties apply in the Devolved Administrations, and their individual emergency planning arrangements.

In practice, the Government works closely with the Scottish Executive, Welsh Assembly Government (WAG) and Northern Ireland departments to promote effective risk assessment work that is, as far as possible, consistent with that of the rest of the United Kingdom. The Local Risk Assessment Guidance (LRAG), for example, is provided to Wales, Scotland and Northern Ireland emergency planning departments. In Northern Ireland, only a limited number of organisations have duties under Part 1 of the Act. Most organisations in Northern Ireland deliver civil contingencies activities in line with the Northern Ireland Civil Contingencies Framework, which requires organisations to carry out individual risk assessments, and encourages them to co-operate in producing risk assessments and sharing information.

Risk assessment at the UK government level

The UK Government has a national risk assessment capability[87] which identified risks to the United Kingdom as a whole over a five-year period, and assesses their likelihood and impact. This forms the basis for decisions about emergency preparedness and about capability planning. The section on the UK Government provides more detail on national risk assessment processes.

85. Click here to see guidance on Communicating Risk [PDF, 80 Pages 4.2MB].

86. www.ukresilience.info/preparedness/englishregions/index.shtm

87. “Capability” is a military term which includes both personnel, equipment and training and such matters as plans, doctrine and the concept of operations.

This national risk assessment process feeds into the Devolved Administrations, regional and local levels to ensure fully integrated risk assessment processes at all levels which underpin coherent emergency planning throughout the United Kingdom. The Government provides guidance to LRFs and RRFs on the likelihood of emergencies based on national assessments, which can then be flexibly tailored to meet local and regional judgements of the risks facing their areas.

The UK National Capabilities Survey was launched on 2 February 2006. The Survey is part of the Government's programme to make the country more resilient to disruptive events. Conducted every other year, it will provide an up to date picture of preparedness, and help plan improvements.

The first full Survey followed a few months after the provisions of the Civil Contingencies Act 2004 came into effect, in November 2005. It shows that there have been improvements since a more limited 'mapping exercise' first examined the preparedness of local responders for emergencies, in 2003/04.

The survey suggests that:

- The United Kingdom has a good level of preparedness overall. Where comparisons can be made with the more limited 2003 mapping exercise the local response results demonstrate clear signs of improvement in specific areas, such as in planning to respond to a 'flu pandemic.

- Preparedness for less clear-cut eventualities is well developed: 'generic' capabilities (for example: against the event of a chemical, biological or radiological (CBR) incident; for urban search and rescue tasks) have benefited from investment and heightened interest.

- Likewise, multi-agency co-operation seems to have benefited from encouragement in the Civil Contingencies Act: for example in local authorities' plans to assist NHS in dealing with mass casualties and mass fatalities; and co-operation also with DEFRA/State Veterinary Services in dealing with infectious animal diseases.

- Although planning for emergencies at the local level is well-established and has improved significantly, there is scope for making the review and exercise of plans more systematic.

- Within the essential service work streams [linked] there is a good level of business continuity and crisis management. Planning for specific scenarios is also good but less developed than generic planning.

- There is little regional variation in preparedness; however there are differences at the local level within regions. This suggests that there are more significant differences in the challenges faced at a local level within any given region, than between regions.

- Central government's core response capabilities are well-developed. Departmental business continuity plans are in place and are being exercised.

Private sector companies have their own processes for assessing risk.

Risk management priorities

Risk management for information systems can be divided into the general method advocated for the UK government itself and the work done on nationally critical systems and networks by NISCC in support of any outcomes from the national risk process.

For government systems there is a standard called Information Security Standard No. 1 which deals with risk assessment and risk treatment, and a companion standard which deals specifically with the risk management cycle, called Information Security Standard No 2.[88]

CNI priorities are set by two convergent means. The first is operationally sector by sector by the NISCC outreach teams. In this process, typically, NISCC outreach staff constructs a sector overview to understand the types of organisations in the sector and to identify organisations that operate nationally critical services that have information systems' support. The respective organisations are then approached to perform a one-to-one assurance process, typically resulting in an assurance report, or engaged in a one-to-many way process, for example by membership of an information exchange. Assessments of criticality are based on impact rather than risk; and in general the higher the criticality, the higher the priority in NISCC terms. Criticality is currently assessed qualitatively by assessing the time-dependent impact on life, society, the economy and the functioning of government.

These priorities are then fed into the TIDO (PROTECT) process in determining, with the leading government departments, that correct countermeasures have been taken to address the electronic attack risks associated with the worst case scenarios identified in the national risk assessment.

United States

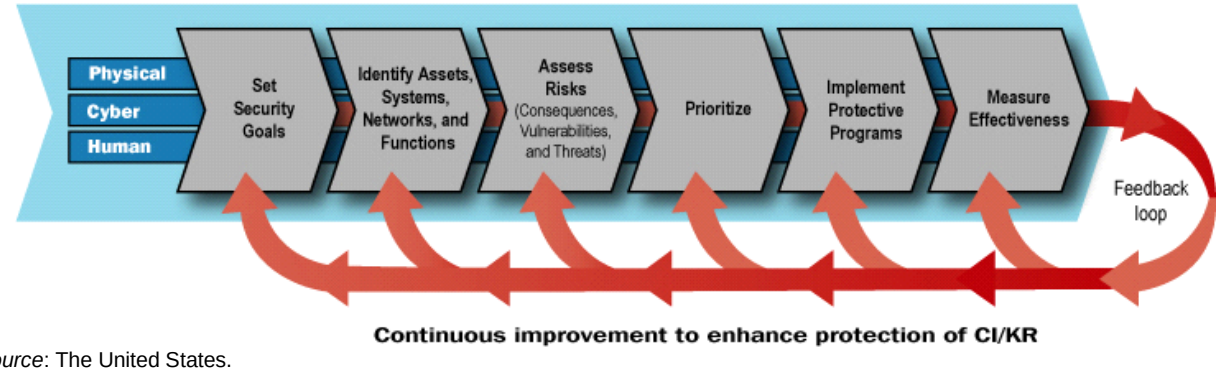
Risk management strategy

In response to HSPD-7, DHS created the NIPP in co-ordination with the private sector. The NIPP details how the public and private sectors will work together to identify, prioritise, and co-ordinate CI/KR protection in their respective sectors. DHS's risk-based approach is described in detail in the NIPP Base Plan that provides the unifying structure for the integration of CI/KR protection efforts into a single national programme. It sets forth a Risk Management Framework for public and private sector partners to work together to produce a comprehensive, systematic, and rational assessment of national or sector risk, which drives CI/KR risk reduction activities. The NIPP includes a cross-sector cyber element that is a component of each sector and recognises the IT Sector specifically as one of the 17 CI/KR sectors.

Risk management framework

The cornerstone of the NIPP is the Risk Management Framework shown below, which establishes the process for combining threat, vulnerability, and consequence information to assess risk.

Figure 2. The NIPP Risk Management Framework



Source: The United States.

88. See www.niscc.gov.uk/niscc/docs/re-20050804-00653.pdf?lang=en.

The NIPP framework is composed of six specific activities:

- Set security goals: Define specific outcomes, conditions, end points, or performance targets that collectively represent an effective security posture.

- Identify assets: Develop an inventory of the individual assets and systems that make up the Nation's CI/KR, some of which may be located outside the United States, and collect information on them, including dependencies, interdependencies, and reliance on cyber systems.

- Assess risks: Determine which assets and systems are critical by calculating risk, combining potential direct and indirect consequences of an attack (including dependencies and interdependencies associated with each identified asset), known vulnerabilities to various potential attack vectors, and general or specific threat information.

- Prioritise: Aggregate and order assessment results to present a comprehensive picture of national CI/KR risk in order to establish protection priorities and provide the basis for planning and the informed allocation of resources.

- Implement protective programmes: Select appropriate protective measures or programmes and allocate funding and resources designed to address targeted priorities.

- Measure effectiveness: Incorporate metrics and other evaluation procedures at the national and sector levels to measure progress and assess effectiveness of the national CI/KR protection programme.

A common approach is needed to assess risk so that protection priorities can be set across the CI/KR sectors. The first step towards achieving this common approach is to establish common definitions and analysis of the basic factors of risk: threat analysis, vulnerability assessment, and consequence analysis.

When the three basic factors of risk are combined, they form the risk associated with an asset, system, network, or function such as the potential for loss of or damage to an asset or system. As risk assessments are completed the results are prioritised to help identify where risk-reduction activities are most needed, and subsequently determine what protective actions should be targeted first. Effective implementation of the NIPP requires integrated and effective public-private partnerships, as well as communication and co-ordination at all levels. The NIPP provides a sector partnership model that encourages the following two partnerships to enable government and private sector partners to undertake the full range of protective activities:

- Sector Co-ordinating Councils – Provides a framework for private sector infrastructure owners and operators and supporting associations to engage with Homeland Security and SSAs.

- Government Co-ordinating Councils – Provides a forum for interagency communication, co-ordination, and partnership with Homeland Security, SSAs, and the supporting Federal departments and agencies that have a role in protecting the respective sectors.

The highly distributed and interconnected nature of cyber infrastructure, both physically and logically, requires that cyber risk reduction activities and programmes be implemented both within and across sectors. DHS is committed to identifying and supporting a variety of protective initiatives and fostering international co-operation to help secure the US cyber infrastructure. As mentioned above, the responsibilities for securing cyber infrastructure are dispersed and include both the producers and users of

the infrastructure. In the United States, DHS is the SSA for the IT Sector and charged with the responsibility to develop cross-sector cyber guidance that applies to all sectors under the NIPP.

Information Technology sector

The IT sector comprises the producers and providers of hardware, software, and IT systems and services, and the Internet. DHS is working collaboratively with its private and public sector partners in the IT Sector through the IT Sector Co-ordinating Council (IT SCC) and Government Co-ordinating Council (IT GCC) set up under the NIPP partnership framework. The IT GCC and IT SCC are working together to develop the IT Sector Specific Plan (SSP). As with all infrastructure sectors, private stakeholder participation in the process is essential to developing and implementing an efficient and effective IT SSP. Furthermore, the Internet has been identified as a key resource comprised of assets within both IT and Telecommunications sectors which all sectors rely upon and utilise the Internet in varying degrees. The availability of the service is the responsibility of both the IT and Telecommunications Sectors.

Cross-sector cyber element

While the producers of cyber infrastructure are addressed in the IT Sector, the cross-sector cyber element of the NIPP focuses on "consumers" of cyber infrastructure, including CI/KR sectors and their associated security partners. Each sector is responsible for securing its cyber infrastructure. The NIPP addresses cyber security and the cross-sector cyber element of CI/KR protection across all 17 sectors. The NIPP also addresses specific cyber responsibilities for sector security partners, processes, and initiatives to reduce cyber risk, and provides milestones and metrics to measure progress on enhancing the Nation's protection of our cyber infrastructure. The 17 CI/KR SSPs will further detail risk reduction strategies related to their respective critical cyber infrastructure.

Risk management priorities

The NIPP encourages all public and private sector organisations to develop and implement a cyber risk management strategy to reduce the risk to the cyber infrastructure. Elements of such a strategy should include the following three components:

Identifying cyber assets, systems, networks, and functions – A process should be defined and implemented to identify cyber assets and cyber elements of physical assets of potential sector, regional, or national importance. Cyber assets represent a variety of hardware and software components including business and control systems, networking equipment, database servers and software, and security systems. The process for identifying cyber assets should be scalable, distributable, and repeatable to ensure that it is practical, efficient, and provides accurate results.

Assessing cyber risk – Consequences, vulnerabilities, and threats should be identified and analysed to assess risk. Potential consequences should include those that result from reliance on cyber assets. Vulnerability assessments can be conducted on cyber assets using a variety of approaches, methodologies, or criteria. Threat analysis should address those scenarios that are of highest concern.

Implementing protective programmes to reduce risk – Organisations should make decisions to implement protective programmes based on their risk assessments and their desired security posture. While some risk may be acceptable, appropriate and effective protective measures will be necessary to balance risk and associated costs.

An organisation's cyber risk mitigation strategy should be realistic and actionable with stakeholders fully engaged in the implementation. The NIPP framework is flexible enough to allow individual organisations to tailor it to meet their requirements. By securing portions of the cyber infrastructure across

multiple organisations and the public and private sectors, the overall infrastructure will become more resilient.

No single entity can protect the entire cyber infrastructure alone. DHS continues to partner with state, tribal, local and international governments, businesses, industries, to mitigate the risk associated with cyber consequences, vulnerabilities, and threats. DHS recognises the efforts of businesses and government agencies thus far, and encourages them to continue – or begin – partnering with their Sector Specific Agencies and respective co-ordinating councils. Together, all infrastructure stakeholders can reduce risk and improve the overall security of our cyber infrastructure.

Question 3: What are the information sharing and other mechanisms used within your government and with other stakeholders to address critical information infrastructure?

The volunteer countries' responses have been collected under four headings to reflect different stakeholder and interest groups:

- Information sharing at the national and international levels.
- Information sharing with the private sector.
- Education and awareness.
- Research and development.

Australia

Information sharing at the international and national levels

Within the Australian Government, the e-Security Policy and Co-ordination Committee is the core policy development and co-ordination body on e-security matters. It also serves as the Government's core strategic policy body for providing expert advice in relation to threats to the NII and it is responsible for strategic policy co-ordination on incidents of a critical nature to the information economy. It is attended by all relevant Australian Government agencies.

Information sharing with the private sector

Outside of government, the major mechanism used by the Australian Government to share relevant information and progress work that relates to the protection of the NII is the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).[89] The TISN was established in 2004 to enable the owners and operators of critical infrastructure to share information with each other and government on important security issues that may impact on the protection of Australia's critical infrastructure.

The TISN is made up of nine sector-specific advisory groups, three expert advisory groups and the Critical Infrastructure Advisory Council (CIAC)[90] – the principle body which oversees the work of the advisory groups. The nine sector-specific advisory groups cover banking and finance, communications, energy, emergency services, food chain, health, transport, water services and mass gatherings. All sector groups formed under the TISN have representation from industry and all relevant Australian, State and

89. www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~Brochure+6+Hune+06.pdf/$file/Brochure+6+Hune+06.pdf

90. www.ag.gov.au/agd/WWW/tisnhome.nsf/Page/RWPB3DF7231AB434697CA25717000240E2E

Territory government agencies. The participation of government agencies in the sector groups assists in a greater understanding of issues by the government and allows industry to be briefed on government activity. As chair of the CIAC, the Attorney-General's Department assists sector groups in the TISN to collaborate on issues of common threat or vulnerability and interdependencies.

The CIAC is focused on the medium-to-long-term issues concerned with the prevention, preparedness and recovery aspects of CIP, particularly those matters requiring co-ordination with the private sector. The CIAC will also assist in identifying research issues requiring priority attention. The CIAC provides an avenue for critical infrastructure owners and operators to communicate with the Australian Government at a high level.

The Information Technology Security Expert Advisory Group (ITSEAG)[91] has been established under the TISN to provide government and owners and operators of critical infrastructure with information on IT security issues that impact on the protection of Australia's critical infrastructure. The group is comprised of IT security vendors, academics, research institutions and government agency representatives who are leaders in the information technology/e-security field.

AusCERT[92] is the national Computer Emergency Response Team for Australia. It provides an alert service, as well as computer incident prevention, response and mitigation advice for subscribers. The Australian Government has purchased a whole-of-government subscription to the alert service

To further enhance Australia's readiness, in 2005 the Australian Government established GovCERT.au - the Australian Government Computer Emergency Readiness Team. GovCERT.au is responsible for:

- Providing an entry point to the Australian Government for foreign computer emergency response teams.
- Developing policy for co-ordinating a national response to a computer-based attack on Australian critical information infrastructure.
- Co-ordinating exercises to test Australia's critical information infrastructure's preparedness, prevention, reporting, response and recovery mechanisms.
- Providing an entry point to the Australian Government for security and other issues raised by AusCERT and other members of the international CERT community; and
- Providing a trusted line of communication into the international CERT community for Australian Government operational agencies dealing with computer incidents.

Education and awareness

In 2006, the Australian Government held a National E-Security Awareness Week to encourage Australian Internet users to 'stay smart online'. A website (Stay Smart Online) was launched concurrently to provide Australians with advice on how to secure their computers, how to transact safely online and how to access a range of resources including top tips, quizzes and guides to help them stay smart online. The website also hosts an e-security alert service that will provide users with simple, up-to-date information on

91 www.dcita.gov.au/communications_and_technology2/publications_and_reports/2006/magazines/data_magazine/issue_8/it_security_expert_advisory_group

92. www.auscert.org.au/

the latest e-security threats and what to do about them. These initiatives recognise that, due to the growing interconnectedness of the Internet, it is becoming increasingly important to ensure that all Australians using the Internet are protected from online threats in order to protect the NII.

Research

The e-security industry is experiencing substantial growth.[93] R&D is an important link in the innovation chain driving developments in this industry sector. The Government has an important role to play ensuring that Australia is a global supplier as well as a consumer of e-security products and services.

In Australia, e-security R&D is undertaken by Commonwealth Government agencies, the academic community and commercial e-security businesses.

The Commonwealth has a number of industry development policies and programmes which positively impact on e-security R&D in Australia. In order to position e-security R&D as a national priority, the Department of Communications, Information Technology and the Arts (DCITA) is presently investigating additional means of augmenting these policies and programmes, including through facilitating linkages between researchers in commercial, government and academic sectors, and increasing awareness of funding opportunities. Defence Signals Directorate (DSD) and Defence Science and Technology Organisation (DSTO) are looking to establish regular, targeted funding of specific e-security R&D projects.

Canada

Information sharing at the international and national levels

International

Recognising that effective information sharing is a key success factor in CI and CII protection, the Government of Canada has been working intensively to identify better ways to achieve this goal, engaging all levels of government, the private sector, academia and international partners. Some of the mechanisms in place are outlined below.

Canada-United States: The cross-border interconnectedness and interdependency between Canada and the United States underscores the importance of strategic partnerships and timely information sharing between governments and the private sector on both sides of the border. Canada has developed strong working relationships with the Department of Homeland Security and with other key United States departments and agencies responsible for critical infrastructure including cyber, such as the Departments of Commerce, Energy, Defence and the State Department. Joint Canada-US strategies to enhance co-operation and information exchange find expression in a number of agreements and collaborative mechanisms. Examples include:

> *Smart Border Declaration and Action Plan*: The Smart Border Declaration outlines a set of initiatives, called the 30-point Action Plan, to secure the flow of people, secure the flow of goods, secure shared infrastructure, and co-ordinate the sharing of information. Joint programmes to implement the plan are under development, including a joint framework for assessing threats to critical infrastructure and joint training and exercises.

93. www.dcita.gov.au/communications_for_consumers/security/e-security/agenda#current

Security and Prosperity Partnership: The Security and Prosperity Partnership of North America (SPP) was launched in March 2005 as a trilateral effort to increase security and enhance prosperity among the United States, Canada and Mexico. The SPP framework, from an emergency management perspective, committed the three countries to, among other initiatives, creating a secure and sustainable energy supply, developing a common approach to critical infrastructure protection, including CII, and response to cross-border incidents; as well as conducting co-ordinated exercises and training in emergency response through mechanisms like the Top Officials series of exercises (TOPOFF). A number of bilateral working groups have been established to implement these commitments.

Canada-United States Infrastructure Protection (CIP) Framework for Co-operation ("Joint CIP Framework"): The Joint CIP Framework has been established in alignment with the SPP and was the result of a commitment made in the Smart Border Declaration. It established the structure for ongoing co-operation by identifying strategic objectives for both governments. The objectives include the development and implementation of compatible protective and response strategies and programmes for shared critical infrastructure in mutually agreed priority areas, including cyber systems.

Agreement for Co-operation in Science and Technology for Critical Infrastructure Protection and Border Security: This bilateral Agreement, signed in 2004, allows collaborative security science and technology projects to move forward through the Public Security Technical Programme (PSTP), addressing operational and science and technology gaps and priorities that have been identified in both Canada and the United States. The PSTP aims to be the premier forum for bi-national collaboration in science and technology that advances the national public safety and security strategies of both countries.

Multilateral: Canada is an active contributor to international fora for information exchange in the area of emergency management and critical infrastructure protection including cyber security. Some examples include:

NATO Civil Emergency Planning and Critical Infrastructure Protection: In this forum Canada collaborates with other NATO member countries to support national authorities in civil emergency planning and to co-ordinate and manage the availability of civilian resources during emergency situations. In light of the importance that the protection of critical infrastructure (CIP) has taken on in the security environment since 11 September 2001 and its vital link to emergency management, an Ad Hoc Group (AHG) on CIP, which Canada chairs, has been established. The principal goal of the AHG is to support nations in maintaining their ability to ensure the continued functioning of critical infrastructure and ensure that any disruption of services provided by critical infrastructure is infrequent and of minimal duration.

Organisation of American States (OAS): The Canadian International Development Agency, in collaboration with the Pan-American Health Organisation and the Caribbean Disaster and Emergency Response Agency, works to improve the ability of disaster management bodies in the Caribbean region to prevent and reduce the impact of recurrent natural disasters and to provide assistance following major disasters. Canada also has actively supported the inclusion of a strong commitment on disaster reduction in the *Plan of Action of the Americas* (April 2001) under which leaders agreed to strengthen hemispheric co-operation and national capacities to develop a more integrated approach to the management of natural disasters.

Group of Eight (G8): The G8 Summit brings together the leaders of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States, as well as the European Union

which is represented by the President of the European Council and the President of the European Commission. Established because of concerns over the economic problems that faced the world in the 1970s, Summits have evolved from a forum dealing with macroeconomic issues to an annual meeting with a broad-based agenda that addresses a wide range of international economic, political, and social issues that have included improving worldwide emergency response systems, preparedness for human/animal pandemics, securing world energy supply and infrastructure, building peace and countering terrorism, and addressing environmental matters such as climate change.

Canada participates in the G8 24/7 network and provides a point of contact in the Royal Canadian Mounted Police (RCMP) to assist other countries in the investigation of computer crime. Canada also participates in international law enforcement activity such as the G8 High Tech Crime Group (The Lyon Group) and it has chaired meetings and hosted activities. Canada is also a signatory to the Council of Europe Convention on Cyber crime and was active in its drafting.

European Union (EU): Canada supports the European Security and Defence Policy (ESDP), which is being developed by the EU to enhance its ability to undertake international crisis management operations such as humanitarian assistance, search and rescue missions, as well as the conduct of peacekeeping or peacemaking operations, *i.e.* contribute to strengthening trans-Atlantic security. The ESDP is being developed in a strategic partnership with NATO, which supplies assets, capabilities and planning assistance to ESDP operations. In return, enhanced EU national capabilities are intended to strengthen NATO's overall capabilities, in particular with regard to crisis management operations.

Organisation for Economic Co-operation and Development (OECD): The events of 11 September 2001 in the United States marked a turning point for the OECD's efforts to protect critical information infrastructure. In order to better counter cyber terrorism, computer viruses, and hacking, the OECD drew up new guidelines, which, at their 1037th session on 25 July 2002, OECD members, including Canada, adopted the new "*Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*". These Guidelines were designed to develop a 'culture of security' among the government, businesses, and users with respect to the rapid worldwide expansion of network communication systems. Canada, as a member country of the OECD, was involved in reviewing and approving the Guidelines.

Across Government Sectors

Governments in Canada have reaffirmed their collective commitment to better assess, manage and mitigate risks to Canadians, and ensure better emergency preparedness and critical infrastructure protection, including protection of cyber CI, from coast to coast. Governments have learned important lessons from recent natural disasters and infrastructure failures such as ice storms, electricity blackouts, forest fires and medical emergencies such as SARS, leading to a commitment to continue close co-operation to increase the level of preparedness in all communities against all hazards.

Recognising the importance of regular discussions among federal-provincial-territorial (FPT) Ministers responsible for emergency management, Ministers have established a permanent forum and meet annually to collaborate on improving emergency management, CI protection. Ministers agreed to an eight-point work plan that includes, among other initiatives, a national-level emergency response framework, disaster mitigation and critical infrastructure protection including cyber CI.

The Department of Public Safety and Emergency Preparedness continues to work with individual provinces and territories on the development of provincial and territorial CIP programmes. The

Department has a network of Regional Directors and Regional CIP Co-ordinators who play a key role in this area. Examples of regional initiatives include the development of a Provincial Critical Infrastructure Programme Model that will benefit the provinces and territories that do not have CIP programmes, and working to establish and develop partnerships between provincial governments and the private sector.

In addition, the Department of Public Safety and Emergency Preparedness has contributed to and produced a number of CIP tools and products to assist stakeholders. It is also working with federal departments and agencies such as Natural Resources Canada, Transport Canada, Agriculture and Agri-Food Canada and with security experts in the RCMP and the Canadian Security Intelligence Service to undertake vulnerability and risk assessments for identified key critical infrastructures. The Department has established a Joint Infrastructure Interdependencies Research Programme (JIIRP) with the Natural Sciences and Engineering Research Council to provide a greater understanding of and solutions to infrastructure interdependencies.

Business continuity planning is a key component of CIP and CIIP. Under the *Government Security Policy*, the Department of Public Safety and Emergency Preparedness has the responsibility to provide advice to federal departments on the preparation and maintenance of their business continuity plans. It also has the responsibility under the *National Security Policy* for "strengthening the testing and auditing of key capabilities and conducting assessments of other departments" in relation to business continuity planning.

The Public Sector Chief Information Officer (CIO) Council has had a National Sub-Committee on Information Protection (NCSIP) in place for at least five years. This group, comprised of representatives from the federal government, provincial CIO offices and municipalities, is a forum for exchanging information and sharing good practices. Industry Canada works with this group to obtain views and input to its policy work in areas of security. The NCSIP meets three times a year and regularly holds teleconferences to discuss emerging threats, vulnerabilities and incidents. These calls are co-ordinated by the federal Department of Public Safety and Emergency Preparedness (PSEPC).

Information sharing with the private sector

The Government is committed to developing and implementing a National Cyber Security Strategy to reduce Canada's vulnerability to cyber attacks and cyber accidents. Consultations are ongoing with key critical infrastructure sectors on the composition and mandate of the National Cyber Security Task Force that will examine the current state of cyber security in Canada, evaluate the nature and scope of the threat to Canada's cyberspace, encourage a broad exchange of information and collaboration between the public and private sectors, and develop Canada's National Cyber Security Strategy.

In January 2005, CSE held a Cyber Security Forum, which brought together government decision makers, information technology (IT) security professionals and industry to more effectively align IT security efforts within the Government of Canada with the National Security Policy.

The federal Government has also become a signatory to an agreement to participate in Microsoft's Security Co-operation Program[94] (SCP), a global initiative launched by Microsoft. Through the SCP, Canada's CCIRC and Microsoft will collaborate in responding to computer security incidents and proactively seek to reduce the effects of cyber attacks. The SCP initiative reinforces the Department's commitment to collaborate with the private sector to enhance Canada's cyber defences, as outlined in the National Security Policy.

94. www.microsoft.com/industry/government/SCP.mspx
See also www.microsoft.com/Industry/government/governmentsecurityprogram.mspx

Education and awareness

Emergency management and critical infrastructure protection training is a responsibility shared by the federal and provincial governments and the private sector. Federally, the existing *Emergency Preparedness Act* as well as the (proposed) new *Emergency Management Act* assign the Minister responsible for public safety to provide education and training related to civil preparedness and emergencies. Accordingly, the Government of Canada delivers emergency management training through the Canadian Emergency Preparedness College (CEPC), part of the Department of Public Safety and Emergency Preparedness, and assigns Ministers the responsibility for conducting training in relation to emergency plans for contingencies within or related to their area of accountability. CEPC and federal partners have also begun to address awareness training in critical infrastructure protection. The Government of Canada is committed to co-operating with the provinces and territories in order to deliver a progressive and sustainable education and training programme in support of emergency management in Canada.

Education and awareness activities are underway within the private sector and the various levels of government. While there are no single entity co-ordinating these initiatives, there are mutually supporting elements among them given that each sector is focussing on its particular areas of interest. For example, governments have introduced numerous initiatives aimed at ensuring the level of security in their networks is appropriate and at ensuring that employees are aware of the need for good security practices in the work environment. In addition, those departments that have consumer protection mandates have embarked on various campaigns to provide consumer education relative to reducing identity theft on line, the need to keep passwords/PINs confidential, the threats posed by phishing, and spyware etc. Such information can be found at: consumerinformation.ca or www.stopspamhere.ca, a joint effort of the Government of Canada, industry and several non-governmental organisations, which offers consumers and businesses information on spam, phishing, spyware and identity theft.

Research

The Department of Public Safety and Emergency Preparedness (PSEP) promotes research in the areas of critical infrastructure protection and emergency management, working to bring together researchers from across government and academia who have the expertise to help the CI community better understand, manage, and reduce exposure to risk, to reduce the likelihood or severity of losses, and to develop national capabilities for effective emergency and threat response. The research provides expertise, tools, and applications to address the hazards and vulnerabilities that threaten the critical infrastructure, including the cyber infrastructure, and the health, safety and security of Canadians.

PSEP also works in partnership with other government departments to conduct research on topics of shared interest. Collaborative projects have included work on issues related to cyber security, geographical information systems, landslide dynamics and incident analysis. One example of such a partnership is the Memorandum of Understanding between PSEP and the Department of National Defence (DND) under which DND, through its broad scientific programme undertaken by its subsidiary agency, Defence Research and Development Canada (DRDC), seeks to provide science and technology solutions in the area of public safety and national security.

In addition, a cyber research project was undertaken with the Natural Sciences and Engineering Research Council, and other opportunities are being explored with the granting councils and academic institutions. The development of a new all-hazards risk assessment model is currently underway that will include new features such as critical infrastructure (including cyber CI) interdependencies. The knowledge acquired through government-supported research helps emergency managers, decision makers and ultimately all Canadians, to better understand the risks to their environment and to reduce the severity or duration of the impacts when an emergency or critical infrastructure failure does occur.

Within Canada, the Computer Science faculties of various universities are examining issues associated with security and privacy in information networks. A number of these universities have launched collaborative initiatives with the private sector to identify research needs and together, they are defining a research agenda for Canada in this area. Recently, Dalhousie University (Province of Nova Scotia) has established a centre for privacy and security. The University is partnering with the private sector in this initiative (*e.g.* Symantec) as well as the various levels of government. To complement the centre's various education initiatives, a lab has been established where research is conducted. The University of New Brunswick has also launched a similar initiative.

Canada has also provided significant leadership in developing a National Computer Security Incident Response Team (CSIRT) Watch and Warning Network in the Americas through efforts in the Organisation of American States (OAS).

Japan

Information sharing at the international and national levels

The Cabinet Secretariat co-operatively works with relevant agencies and related organisations to collect and provide information from the presiding Ministries and Agencies of the relevant critical infrastructures to the business entities engaged in critical infrastructures:

a) Collect a wide range of information provided from central government agencies concerning information security, central government agencies dealing with individual cases, and related organisations.

b) Provide damage information on the attack, in the case of it being caused by terrorists, to the central government agencies dealing with individual cases, and information on attack methods to the central government agencies concerning information security.

c) Collect and analyse information, and request support from related organisations if necessary.

d) Collect information regarding disasters under the current information-sharing frameworks among Cabinet Secretariat, Cabinet Office, and other relevant agencies.

Information sharing with the private sector[95]

In addition, the government makes an effort to promote the development of "Capability for Engineering of Protection, Technical Operation, Analysis and Response" (CEPTOAR) within each critical infrastructure sector.

CEPTOAR is being established[96] for the reason that the Japanese government considers that information provided by the government for pre-emptive prevention of IT-malfunctions, prevention of expansion of damage, rapid resumption, and prevention of recurrence will be appropriately made available to business entities engaged in operating critical infrastructures and is being shared among them. This will

95. Japan did not provide input on information sharing regarding education and awareness or research.

96. Consultations between the presiding Ministries and Agencies of the relevant critical infrastructures and the business entities will be started to complete the establishment of CEPTOAR for each critical infrastructure sector by the end of FY 2006. Regarding newly added sectors, mutual agreement between presiding Ministries and Agencies of the relevant critical infrastructures and the business entities should be made by the end of FY 2006 (To be established in FY 2007).

eventually contribute to upgrading of the capacity to maintain and reconstruct services of each business entity engaged in operating critical infrastructures.

Moreover, "CEPTOAR-Council" (tentative name) is being established as a council for cross-sector information sharing between CEPTOAR in order to enhance information security measures for critical infrastructures throughout the whole country, and business entities engaged in operating critical infrastructures should encourage cross-sector information sharing with other providers to utilise a wide range of knowledge for their maintenance and recovery.

"CEPTOAR Council" (tentative name) is a council formed by representatives from each CEPTOAR and aims to share common information among several sectors and cross-sector best practices taken from the information regarding maintenance and recovery of services provided by each critical infrastructure sector.

Korea

Information sharing at the international and national levels

There are two ways for the Korean government to promote and mediate information sharing. The Korean government established CPII (Committee on the Protection of II) chaired by the Minister of the office for Government Policy Co-ordination. One of the main roles of CPII is to promote collaboration and exchange recent incidents in public and private sector institutions. Since the Minister of the office for Government Policy Co-ordination is the chairman and all the necessary vice-ministers are involved in the committee, any kind of important issues such as nation-wide planning for CII and dissemination of cyber terror incidents can be discussed and proper countermeasures could be put into place.

Information sharing with the private sector

The public institutions as well as private institutions that carry out the protection of information and communication infrastructures can establish an ISAC (Information Sharing and Analysis Centre). An ISAC analyses any cyber terror-related incidents and disseminates incidents to other institutions. The government provides technical assistance for these institutions.[97]

The Netherlands

Information sharing at the international and national levels

At the national level information sharing is done in several forums: the National Crisis Centre regular meetings, NICC, NAVI, National Continuity Platform, etc. (see paragraphs above "Risk management framework").

At the international level, the Ministry of Economic Affairs participates in several committees on ICT and/or information security in the EU (EPCIP, CIIP, ENISA MB), OECD (WPISP) and NATO (CEP/CCPC). The Netherlands also supports the International Watch and Warning Network.

97. Korean Cert: www.krcert.or.kr/index.jsp

Information sharing with the private sector

Information sharing with the private sector is an integral part of the risk management framework described earlier in this report which includes the activities of ECP.nl, the project Digibewust, the National Forum on Contingency planning, GovCert.NL and alike.

Education and awareness

Information sharing in terms of education and raising awareness is also an integral part of the risk management framework described earlier in this report.

Research

SURFnet[98] is a high-grade computer network specially reserved for higher education and research in the Netherlands. Staff and students of connected organisations can communicate through SURFnet with other Internet users all over the world. SURFnet-CERT[99] is the Computer Emergency Response Team of SURFnet that was known as CERT-NL up to 2003. SURFnet-CERT handles all cases of computer security incidents in which a SURFnet customer is involved, either as a victim or as a suspect. SURFnet-CERT also disseminates security related information to SURFnet customers, on a structural basis (*e.g.* distributing security advisories) as well as on an incidental basis (distributing information during calamities).

To obtain more focus and mass in Dutch scientific research into the security of network and information systems a programme called Sentinels has been established. The programme is funded by both public and private partners. Sentinels started in 2004 for at least six years with a budget of EUR 10M and aims to boost security expertise in the Netherlands. One goal is to build a national ICT security research community and to disseminate the results to industry and government. Links with European and international partners will also be expanded. Sentinels have two parts: the first involves scientific research, with results obtained in collaboration with industry; the second ensures that knowledge generated from these projects is exchanged with industry and government in the Netherlands and, possibly, abroad. A Sentinels ambassador was appointed to ensure that the research results from Sentinels remain visible and accessible to industry.[100]

As a result of giving priority to the national innovation policy, the ICT Research and Innovation Authority of the Netherlands launched an ICT Innovation Platform for Security and Privacy in the spring of 2007. This is an open-interests group with experts from industry, government and the Dutch academic research community. Recently a first agenda called Veilig Verbonden (Secure Connected) was issued with the goal to evolve to a full-fledged research agenda for the near future. The agenda is focussing on seven application areas which are considered crucial for the Dutch economy and has a high potential for further economic growth. One of these areas is Internet and telecom because they are merging to become more and more an ALL-IP environment, where traditional telephony (voice), television (video) and data exchange are integrated into a multi-channel system. Service providers however are expected to initiate innovations, manage issues such as cyber crime and ensure consumer privacy and the availability of services.[101]

98. www.surfnet.nl/info/en/organisation/home.jsp

99. http://cert.surfnet.nl/home-eng.html

100. For detailed information on the programme and its 11 projects see: www.sentinels.nl (text in English available).

101. For more information see website: www.ictregie.nl/index.php?pageId=1&l=en.

United Kingdom

Information sharing at the international and national levels

The United Kingdom uses information exchanges, formal stakeholder groups and the TIDO system to share information.

Information exchanges are closed industry sector groups with a common interest that share incident and vulnerability information following a concept developed by NISCC. There are seven information exchanges, covering sectors such as finance, telecommunications, transport, pharmaceutical, vendor services, managed service providers as well as technologies such as SCADA and process control. There is a complete list on the NISCC website.

The sharing of confidential information occurs through regular face-to-face meetings. Each organisation provides two representatives who cannot be substituted. Members of the exchanges sign an agreement on membership guidelines that requires them to keep confidential all discussions at these meetings unless they agree to share. Trust is essential; this is built up through personal relationships and encourages reciprocal information sharing.

NISCC provides both rules on information sharing and an interface within and between the exchanges, using a traffic light protocol to define the level of information flow in trusted meetings.

To encourage communication among the managers of the government IT systems there is the IT Security Officers' Forum (ITSOF). Each lead government department will also have relationships with companies in the CNI sector and may run crisis management schemes within that sector.

The Government Secure Intranet (GSi) also has a stakeholders' forum facilitated by NISCC. This forum feeds into the code of connection for all allied organisations. This group can also influence the standard for interconnection with other large networks. Operators and managers of government systems and applications participate indirectly in key decisions about domestic critical information infrastructures that have cross-border interfaces through the GSi.

The United Kingdom has an eGovernment Interoperability Framework, developed by the eGovernment Unit of the Cabinet Office. In its development other areas of government have been consulted. The current mechanisms for consultation are the Chief Information Officers' Council and Chief Technology Officers' Council, and the Senior Information Risk Owners' Forum, representing roles in central government departments. The Cabinet Office website has the "Information Assurance Governance Framework" written by the Central Sponsor for Information Assurance.

NISCC supports three main types of Information Sharing model – CERTs, WARPs and Information Exchanges as described below.

CERTs (Computer Emergency Response Teams, *a.k.a.* CSIRTs, Computer Security Incident Response Teams) play an invaluable role in protecting their communities and others against electronic attack. NISCC encourages the formation, development and co-operation of CERTs by supporting existing associations (TF-CSIRT, FIRST) and by helping to develop new ones (*e.g.* UK CERTs Forum, European Government CERTs group). NISCC also shares information with CERTs through UNIRAS, the UK Government CERT, which is part of NISCC.

NISCC recognises that CERTs can require extensive financial and technical staffing resources and such costs are not viable for many communities who nonetheless could benefit from CERT-type services and support. NISCC has consequently developed a new model, similar to a CERT, but realisable at a

fraction of the cost. This alternative concept, which is better suited to the needs of small communities, including small and medium-sized enterprises (SMEs) and citizens, is the Warning, Advice and Reporting Point (WARP).

Information sharing with the private sector

The United Kingdom Government believes that the protection of the critical information infrastructure can only benefit from a wider adoption of a culture of security around the use of information. Previous returns to the OECD on the culture of security have highlighted the wide range of UK players involved in creating such a culture; this has culminated in the creation of the Information Exchanges (as described above).

It is for that reason that the organisation that co-ordinates efforts on the protection of the CII, NISCC, also has activities such as the creation of the UNIRAS CERT and the WARP network, designed to impact on the security posture of much smaller businesses and citizens.

NISCC has developed the WARP model; similar to a CERT, because this alternative concept is better suited to the needs of small communities, including SMEs and citizens. The WARP performs some of the tasks of CERTs but they are not expected to provide the technical response service directly.

A WARP provides to its community a service of early warnings of alerts and vulnerabilities, specifically tailored for its community; this can avoid the duplication of each member sorting through dozens of sources, or even worse, not having time to monitor developing threats.

The WARP also provides a limited help-desk service for the community, geared to the specialised needs and building on the knowledge of the community membership. It also provides a trusted focus for incidents and attacks to be reported, to help find assistance or co-operation in dealing with the problem. Such reports will be valuable to members, but when sanitised and anonymised, sharing them with other WARP communities can be equally valuable.

Considerable funds are being made available in DTI's Innovation Programme to create a platform for network and information security. This activity also encompasses a Knowledge Transfer Network that is designed to increase the effectiveness of the uptake of secure technologies.

To encourage communication among the managers of these government systems and non-government systems there are two separate forums; the IT Security Officers' Forum and the NISCC information exchanges. NISCC provides the interface between the two, using the traffic light protocol to define the information flow. Each lead government will also have relationships with companies in the CNI sector and may run crisis management schemes within that sector.

CSIA/Cabinet Office operates the www.itsafe.gov.uk site which notifies subscribers of immediate threats. Get Safe Online (www.getsafeonline.org) an industry/government initiative is aimed at the citizen market primarily in terms of computer security advice.

Cabinet Office/CSIA (GIPSI) run quarterly events which bring together IT security specialists and vendors to discuss security issues relating to specific topics such as VOIP, flexible working and identity management. Various Government organisations are actively involved in the largest UK trade event INFOSEC in arranging ministerial keynote speeches and participating in panel sessions as well as having stalls in the main exhibition area. 2006 saw the inaugural Information Assurance event in Brighton hosted by CESG. There are also a number of police/business initiatives raising awareness of cybercrime issues at a local level.

DTI provides a website with good practice advice on information security, produces advisory booklets, commissions a biennial security breaches survey and participates in a number of promotional activities with organisations such as the Regional Development Agencies, CBI and the IoD as well as promoting the use of BS7799 (ISO 270001).

Industry also has a number of organisations which actively promote Information Security issues via events and newsletters: IAAC, EEMA, ISPA, ISF to name but a few. Organisations such as Symantec and Messagelabs also provide an alert system for clients. Websites like the BBC and The Register will also carry information on latest security threats. Industry magazines like *Computer Weekly* often carry articles on security threats and business continuity.

Finally there is transfer between Knowledge and Network on Cybersecurity[102] which encourages debate and innovation in the cyber security area.

Education and awareness

DTI and CSIA have provided support in developing and launching the Institute for Information Security Professionals in February 2006. Also in 2006 there was a GlobalWatch mission to the United States with the aim of sharing knowledge between industry leaders and the US information security sector. http://www.dti.gov.uk/innovation/globalwatch/index.html

Infosec Training Paths and Competencies (ITPC) qualifications offer recognised formal training and development for IT security professionals working for the UK Government and related organisations.

The ITPC Scheme develops and supports Infosec core competency profiles for key security roles within UK Government and related sectors. It also manages a formal practitioner qualification and quality-assures development paths assembled from leading training providers in the UK public and private sectors.

The Certificate of Infosec Competency qualification offered by the Scheme is recognised by IT professional bodies and leading UK universities that offer MSc degrees in Information Security.

Research

The Foresight[103] website provides insight into what DTI is involved in with Foresight and the Research Councils via the Technology Strategy board. Other government departments have similar projects looking at security from their particular perspective.

United States

Information sharing at the international and national levels

International

NCSD has developed an International Affairs Programme to further its goals of establishing a national cyber security response system and managing cyber risk. Information sharing among countries is largely based on: *i)* non-sensitive information; *ii)* willingness to share; *iii)* existence of an entity with which to share information in another country (*i.e.* government CIIP organisation or CSIRT with national

102. http://cys.globalwatchonline.com/epicentric_portal/site/cys/menuitem.f9ec00729359aba7ba255921eb3e8a0c/%3Bjsessionid%3DGLL4gLwgQLk78rTfRbDrp1bGn1yJ2lp5V6lY3wTHGqhCr2spgkhy!436901981

103 www.dti.gov.uk/science/Foresight/page25873.html

responsibility). International co-operation and collaborative action are imperative to building the relationships needed to increase situational awareness and improve co-ordinated response mechanisms to detect, protect against, respond to and recover from cyber incidents in the global cyber environment.

National

DHS/NCSD created the US Computer Emergency Readiness Team (US-CERT) – a partnership between NCSD and the public and private sectors. US-CERT is NCSD's cyber analysis and incident response capability. NCSD had made significant progress in this area by:

1. Leveraging the existing capabilities and expertise within DHS.

2. Facilitating and systematising information sharing and preparedness collaboration with other federal and military agencies.

3. Fostering greater information sharing and collaboration between the private and public sectors.

4. Providing a service to the public on cyber security issues.

5. Fostering relationships with the international community.

NCSD/US-CERT has established several important components for co-operation and information sharing. The US-CERT Operations Center serves as a real-time focal point for cyber security, conducting calls with US-based and international watch and warning centers to share important security information. The US-CERT Control Systems Center serves as an operational and strategic component of the US-CERT's capability to address the complex security issues associated with the use of control systems. The US-CERT Public Website provides government, the private sector, and the public with information needed to improve their ability to protect their information systems and infrastructures. The National Cyber Alert System (NCAS) delivers targeted, timely, and actionable information to the public and private sectors as well as to all Americans to allow them to secure their computer systems. For additional details, please visit www.us-cert.gov.

The National Cyber Response Co-ordination Group (NCRCG) was developed to support the President's National Strategy to Secure Cyberspace. The NCRCG facilitates co-ordination of the federal government's efforts to prepare for, respond to and recover from cyber incidents. It serves as the federal government's principal interagency mechanism for operational information sharing and co-ordination of federal government response and recovery efforts during a cyber crisis.

The NCRCG addresses both sudden cyber incidents of limited duration and gradually escalating cyber crisis. As referenced in the National Response Plan, the NCRCG supports the Department of Homeland Security (DHS) DHS Incident Management Planning Team (IMPT) member-agency department heads, and the Executive Office of the President, as appropriate, in regard to cyber-related issues. It also supports the federal agencies whose missions include securing cyberspace, combating cybercrime, and protecting segments of the critical information infrastructure and key assets.

Government agencies

DHS's NCSD focuses significant attention on the security of the Federal cyber infrastructure through its support of a National Cyberspace Security Response System and the related activities of the United States Computer Emergency Readiness Team (US-CERT). NCSD/US-CERT is a partnership between DHS and the public and private sectors to protect the nation's infrastructure and co-ordinate defence against and responses to cyber attacks. NCSD/US-CERT maintains a 24x7 secure incident handling and

response center; a public website at www.us-cert.gov; a secure portal for stakeholders; and the National Cyber Security Alert System (NCAS),[104] which sends timely, actionable information to technical and non-technical users – all of which are resources available to Federal government agencies.

With respect to collaboration with other Federal government agencies and securing government cyberspace, NCSD/US-CERT established and co-ordinates the Government Forum of Incident Response and Security Teams (GFIRST) and Chief Information Security Officer (CISO) peer groups for sharing cyber incident information, best practices, and other cyber security information. GFIRST meets regularly, and DHS has hosted two GFIRST conferences to enhance information sharing and collaboration. The purpose of the GFIRST peer group is to:

- Provide members with technical information, tools, methods, assistance, and guidance.
- Co-ordinate proactive liaison activities and analytical support.
- Further the development of quality products and services for the federal government.
- Share specific technical details regarding incidents within a trusted US government environment on an agency peer level.
- Improve incident response operations.

US-CERT provides an Internet Health Service (IHS) tool to GFIRST members through the US-CERT secure portal. IHS is a web-based application that provides members with access to several commercially available Internet and security products for use in building their situational awareness capabilities through the monitoring of their respective networks and the overall health of the Internet. In addition, as part of its Situational Awareness Program, US-CERT also leverages information technology for the automated sharing of critical information across the federal government and analysis of traffic patterns and behaviour.

In addition, NCSD has established a relationship with the Multi-State Information Sharing and Analysis Center (MS-ISAC) for information sharing and outreach to state and local governments regarding cyber security issues. One specific joint NCSD and MS-ISAC initiative is a series of national webcasts that examine critical and timely cyber security issues.

Law enforcement, intelligence and military services

NCSD maintains a Law Enforcement and Intelligence Branch with representatives from other US government law enforcement and intelligence departments and agencies. NCSD co-ordinates with the Department of Justice, the Department of Defense and the law enforcement and intelligence communities to address cyber security issues. To maximise collective knowledge about possible threats and malicious activity on an on-going basis, the law enforcement community has created a successful mechanism for sharing information with known partners. US-CERT Operations has a robust relationship with their Department of Defense operational counterpart, the Joint Task Force for Global Network Operations (JTF-GNO).

Information sharing with the private sector

HSPD-7 outlines "Sector Specific Agencies" (SSAs) for each of the 17 CI/KR sectors. The private sector-led Sector Co-ordinating Councils (SCCs) work with each SSA; and the SSAs are the chairs of the

104. More information is available at www.us-cert.gov

respective Government Co-ordinating Councils (GCC), which represent the government agencies that have a role in protecting their sectors. DHS SSA responsibilities include the IT Sector and the Telecommunications Sector, among others. Although various information sharing mechanisms currently exist, information sharing will be addressed in detail in each sector's SSP.

Another mechanism for information sharing with the private sector is through Information Sharing and Analysis Centers (ISACs). ISACs were established by Presidential Decision Directive (PDD 63) as a new type of public-private forum designed to promote dialogue within and between critical infrastructure sectors and the government by encouraging sector members to share information about potential existing vulnerabilities, threats, intrusions and other anomalies. ISACs are typically self-organised and managed by the private sector and differ from SCCs in that their role is operational while SCCs focus on policy issues. The Information Technology Information Sharing and Analysis Center (IT-ISAC) and others from other industry sectors share information with US-CERT on a regular basis.

NCSD/US-CERT created the US-CERT Portal as a method for sharing information related to cyber security among government, industry, and the ISACs in a secure, collaborative platform that is trusted and easily accessible by all participants. The US-CERT Portal contains a set of collaboration features to include secure messaging, libraries, forum discussions, alerts, chat rooms, calendars, online meetings, surveys, task tracking, and a user locator. NCSD/US-CERT also works with the IT ISAC, and to obtain and share cyber security information between IT GCCs IT SCCs, other ISACs, and other private critical infrastructure information-sharing entities. Through these mechanisms US-CERT and the private sector stakeholders share information and collaborate on cyber security issues.

An additional mechanism of disseminating information to the private sector and general public is the National Cyber Alert System (NCAS). NCAS is part of the US-CERT Response System that delivers targeted, timely, and actionable information to Americans to allow them to secure their computer systems. The alert system targets all levels of computer user sophistication, from the technical professional to the non-technical home user. It reflects the broad usage of the Internet in today's society. Launched in January 2004, the alert system provides not only cyber guidance for users but the ability to reach millions of users at one time as well. More than 300 000 users have subscribed to the system and received regular alerts and updates. For more information about the alerts, see: http://www.us-cert.gov/cas/. Timely and actionable alerts and warnings are communicated to government departments, Internet Service Providers (ISPs), ISACs, managed service providers, network operators, and private system owners and operators, so they can take protective action on their systems and those of their customers. This helps to prevent potentially serious problems from spreading throughout the Internet with cascading consequences to the critical infrastructures and to US citizens.

In addition to the NCAS, the US-CERT Public Website provides government, private sector, and the public with information needed to improve their ability to protect their information systems and infrastructures. For additional information please see the US-CERT website at: www.us-cert.gov.

Education and awareness

The Strategy calls for promoting a comprehensive national awareness programme to empower all Americans – businesses, the general workforce, and the general population – to secure their own parts of cyberspace. NCSD maintains an Outreach and Awareness programme that includes working with stakeholders to raise the cyber security awareness of the general public. NCSD formally partners with the National Cyber Security Alliance (NCSA) to reach home users, small businesses, and K-12 and college students, and with the Multi-State ISAC (MS-ISAC) to reach state information security professionals and the general public. Formed in 2003, the Multi-State Information Sharing and Analysis Center (MS-ISAC) is an information sharing organisation among representatives of state and local governments that analyses,

sanitises, and disseminates information pertaining to cyber events and vulnerabilities to its constituents and private industry. DHS has a strong relationship with MS-ISAC to help enhance the nation's cyber security preparedness and response capabilities at the State and local levels. In collaboration with NCSA and the MS-ISAC, NCSD promotes the National Cyber Security Awareness Month annually in October. The partnership seeks to reach all 50 states and the general public through special activities as well as TV, radio, print, web and other media.

DHS/NCSD actively partners with the FTC on consumer outreach. The most successful collaboration thus far has been the creation and ongoing growth of www.OnGuardOnline.gov. DHS provides about half the cyber security content through US-CERT Tips and other content contributions. This site is designed to educate consumers/home users with current information on cyber security issues such as phishing and identity theft.

The National Cyber Security Alliance (NCSA) is an important resource for cyber security awareness and education for home users, small businesses, and education audiences. A 501(c) (3) public-private partnership, NCSA sponsors include the Department of Homeland Security, Federal Trade Commission, and many private-sector corporations and organisations. NCSA provides tools and resources to promote online safety to home users, small businesses, and schools, colleges, and universities. DHS supports NCSA by providing guidance and input into National Cyber Security Awareness Month, NCSA working group meetings, campaign efforts, and by providing messaging for the NCSA Executive Director on cyber outreach and awareness initiatives.

NCSD established a Training and Education Programme to meet the training, education, and certification needs of IT security professionals within the Federal government and private industry. While DHS does not specifically provide grant funding to institutions, DHS co-sponsors and supports a variety of initiatives targeted towards enriching the pool of current and future IT security professionals.

NCSD co-sponsors the Federal Cyber Corps: Scholarship for Service (SFS) Programme with the National Science Foundation (NSF) and the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) programme with the National Security Agency (NSA). NCSD also works with the NSF, NSA, the Office of Personnel Management (OPM), and the Federal Chief Information Officers (CIO) Council IT Workforce Committee to identify ways of leverage in the SFS and CAEIAE programmes to address IT security training and education workforce issues. NCSD also partnered with the DHS Risk Management Division (RMD) to create "Project MBA" which incorporates the physical and cyber security curriculum into graduate business programmes. Additionally, NCSD is leading efforts to establish a national skill baseline for the IT security workforce including both public and private sectors. The initial effort is to develop an IT Security Professional Essential Body of Knowledge (CBK) to provide one consistent baseline resource to validate vendor-neutral, industry certification content.

Research and Development

Cyber-related R&D is vital to improving the resiliency of the Nation's critical infrastructures. This difficult strategic challenge requires a co-ordinated and focused effort from across the Federal government, state and local governments, the private sector, and the American people to advance the security of critical cyber systems.

A critical area of focus for DHS is the development and deployment of technologies to protect the nation's cyber infrastructure, including the Internet and other critical infrastructures that depend on IT systems for their mission. Two components within DHS share responsibility for cyber R&D, with the Science & Technology (S&T) Directorate serving as the primary agent responsible for executing cyber

security R&D programmes. NCSD has responsibility for developing requirements for cyber security R&D projects.

Question 4: What does your government consider to be the major challenges facing cross-border management of CII issues? What is your government doing to address them?

The volunteer countries' responses have been grouped under:

- Cross-border challenges.
- Government response.

Australia

Cross-border challenges

The borderless nature of the Internet means that e-security threats affecting critical information systems and networks in Australia can arise from anywhere. Therefore, the Australian Government considers that mechanisms which facilitate international collaboration and create a global understanding of e-security risks and solutions are essential in addressing e-security issues in an effective manner.

It is also recognised that there is need for better co-ordination of law enforcement of e-security related offences internationally, including greater consistency in e-crime related legislation and regulations.

Issues such as increasing globalisation and cross-border data flows are also significant challenges. For example, large companies increasingly store large volumes of data in different legal jurisdictions and this raises data protection issues for the Australian Government. In particular, national security and privacy concerns arise when data originating in Australia is housed in countries that have different data protection and retention requirements to Australia.

Government response

The Australian Government engages on e-security issues through a number of bilateral and multilateral forums. These arrangements provide the Australian Government with an opportunity to share intelligence and to work co-operatively on addressing significant e-security issues.

The Australian Government is also an active member of several international policy setting forums, such as the International Telecommunication Union, the OECD, and APEC. These forums aim to ensure a common understanding of international e-security issues, trends and practices amongst member nations. They also provide a mechanism to develop frameworks that facilitate consistent policy and regulatory approaches to, and improved co-ordination of, e-security issues across member economies.

Besides efforts at the Government level, the considerable amount of international collaboration that occurs within and between non-government organisations also makes a significant contribution to Australia's capacity to manage e-security issues. For example, the ICT industry plays a significant role in the global warning process as it is able to identify, notify and respond to current and emerging e-security threats and vulnerabilities on an international level. Many ICT industry members in Australia have strategic alliances and networks with both international counterparts and other Governments, thereby providing the relevant conduit for early warning response and detection. The TISN and GovCERT.au provide important mechanisms for allowing this information to be shared between critical infrastructure sectors and with governments.

From a law enforcement point of view, Australian law enforcement agencies are taking a lead role in international efforts, such as the G8 Cybercrime Network, to combat e-crimes which are facilitated by the borderless nature of the Internet. They also have mutual assistance arrangements in place with other countries which enable them to acquire relevant data necessary for investigating and prosecuting e-crimes that transcend national borders.

Canada

Cross-border challenges

The Government of Canada has been concerned for some time with the threats as well as the opportunities presented by rapid advances in technology and communications. The borderless nature of communication on the Internet has caused law enforcement to focus more on international issues because of the new ways crime can be committed and the new possibilities for electronic investigation and evidence-gathering. In addition, the increasing significance of the cyber CI in critical areas of national life has led the Government of Canada to treat its protection as a matter of public safety and national security.

Canada and the United States share the longest undefended border in the world, along with economic interdependencies, interconnected infrastructure and a common threat environment. Collaboration and information-sharing are longstanding traditions connecting the governments of both countries, which translate into a common commitment to enhance the security, prosperity and quality of life on both sides of the border. An important shared goal is to enhance the security of the critical systems that span both countries, *e.g.* energy, communications including the Internet, finance, transportation, water systems, as well as the information technology networks and systems (*i.e.* the CII) that are essential to their continuity.

Some of the cross-border challenges in the North-American CIP and CIIP context include, among others:

- Wide diversity of interests and actors for any given issue.
- Delegation by federal governments of a variety of policy issues to the provincial or state governments, including regulation of some CI sectors resulting in diverse regulatory schemes.
- Local officials in both countries, in partnership with local/regional business interests and community-based groups, need to play a more significant role in bi-lateral discussions about policies affecting their lives.
- Federal policy makers in both Canada and the United States need to become more aware of "facts on the ground" and of local and regional initiatives.
- The central governments need to solicit more regional and local involvement, as well as that of the private sector, non-government organisations, academia and other interests.
- Concern on the part of private sector CI and CII owners/operators, in both Canada and the United States, about the potential for inappropriate release under disclosure of information laws of sensitive emergency management, CI or CII information shared with governments, leading to diminished information sharing.

Government response

Canada-United States: Given the long history between Canada and the United States of co-operating on matters relating to public safety and emergency management, a number of agreements articulate a level of co-operation that is unmatched anywhere in world. These include the *Smart Border Declaration and Action Plan*, the *Security and Prosperity Partnership*, and the *Canada-United States Infrastructure Protection (CIP) Framework for Co-operation* as but three examples. The characteristics of these, as well as several other major bilateral agreements, are outlined in the response to question 3 above.

Multilaterally: Canada is an active participant at the international level in efforts to develop comprehensive approaches to emergency management and critical infrastructure protection, including protection of CII. Examples of Canada's major international involvements are outlined in the response to question 3 above.

CSE, Canada's lead technical agency on IT security, has taken a number of steps to better protect Canada's information infrastructure through building capacity, raising awareness and enhancing collaboration, both within government and with their international and industry partners.

Canada has signed the Council of Europe Convention on Cybercrime with the goal of eventual ratification. Canada also played a role in the formulation of the Convention's articles.

Japan

Cross-border challenges

In general, the Japanese government has been making best efforts on improving international co-operation, for example, joining international organisations such as the Meridian Conference to share information and good practice.

But in reality, sharing sensitive information with other countries is a major challenge. Moreover, language barriers and time lag must be overcome to cope with cyber incidents.

Korea[105]

Cross-border challenges

The government has been working on improving international co-operation, but the importance of the CII and the risks related to sharing sensitive information with other countries are a challenge.

Government response

The Korean government has worked with global communities to make cyberspace safer and trustworthy. Since Korea experienced 1.25 Internet disturbances in 2003, the government considers that national cyberspace security can only be realised by both its own efforts and close co-operation with other countries. To successfully co-operate more closely with other countries and meet the needs of the CIIP Act, the government considers it necessary to:

- Follow up the new trend of CII technologies and outreach activities to collaborate with other countries.

105. Cut and paste from Korean input. Represents the challenges Korea is addressing.

- Exchange CII related technologies and specialists to encourage international co-operation.

- Participate in research and development initiatives for establishing international standards and joint studies.

The Netherlands

Cross-border challenges

The Internet has created the possibility to connect to user computer services from anywhere in the world. In this respect crime-related activities on the Internet are not bound by national borders. This requires nations to put into force international measures and agreements on law enforcement and investigations to fight cyber-related offences or crimes.

Software development and operations are increasingly transferred to lower-salary-countries. Also some managing centres of ICT are transferred beyond the jurisdiction of The Netherlands. As a consequence some critical (ICT-) services, systems, processes and centres and development are beyond the control of The Netherlands government authorities that rely on them. In the absence of political and judicial agreements on the quality and security levels between countries using these systems and those providing them there is concern that this is likely to increase vulnerabilities to the critical information infrastructure in The Netherlands.

The Netherlands is concerned about the possibilities that parts of the critical infrastructure will become owned or controlled by un-trusted (for example foreign) parties. One example could be the silent acquisition of an ISP which provides critical services in The Netherlands by a little-known company based in an un-trusted country.

Government response

The Netherlands government participates in several international policy settings.[106] The Ministry of Economic Affairs and Ministry of Interior (incl. GovCert.NL) actively co-operates with partner organisations in other countries to develop measures and/or co-operation in the field of information security and/or fighting cyber crime.

An important activity is the implementation of NICC detailed earlier in this report. The Ministries of Justice and Interior (the latter as being responsible for National Police Forces) participate in international forums to promote international co-operation on investigation of and legal actions against cyber criminals.

No position has been taken on what steps the government should take if a CI provider is acquired by an un-trusted party.

106. EU including Enisa, OECD WPISP, NATO, CEPT, Terena (Trans-European Research and Education Networks Association), I4 (International Information Integrity Institute), ISF (Information Security Forum), First (worldwide Forum of Incident Response and Security Teams), EGC (European Governmental CERTs) and standardisation fora such as ETSI and ITU.

United Kingdom

Cross-border challenges

The UK government considers increasing globalisation, off-shoring and foreign ownership of infrastructure as challenges. So are legal issues, in particular data protection that may limit the flow of information across national or economic boundaries. Likewise, prioritising work so that international interdependencies are identified is a practical requirement, which is not being addressed uniformly to date.

There is also the challenge of cultural differences in the perception of risk. This is more obvious in economic and social issues where the country has different economic dependencies or where social concerns such as privacy and individual rights play a role in how far governments can intervene. Identifying elements of the decision-making process is also a challenge and would contribute to the development of a model for cross-border collaboration among governments.

Government response

The UK government is working with organisations such as the European Government CERT Group.[107] the International Watch and Warning Network and CII protection organisations internationally to share information and good practice. As part of this, the United Kingdom held the inaugural Meridian Conference where the traffic light system of rating warnings was adopted.

United States

Cross-border challenges

The global and borderless nature of cyberspace makes international co-operation and collaborative action imperative to building the relationships needed to increase situational awareness and improve co-ordinated response mechanisms to detect, protect against, respond to and recover from cyber incidents in the global cyber environment. International co-operation for CIIP helps to foster national and international activities that promote a global culture of security and improve global incident preparedness and response posture.

The United States faces several challenges in addressing cross-border CIIP issues, including the following:

- Capability: Information sharing for watch, warning and incident response is an important operational aspect of cyber security/CIIP co-operation. Computer security incident response teams (CSIRT) play an important role in mitigating cyber incidents. Because CSIRTs require specialised capabilities and resources, developing a CSIRT with national responsibility is important, but can prove challenging.

- Information Sharing: The ability to share information across-borders may be difficult due to classification of information, legal constraints, or uncertainty regarding the further distribution of shared information.

- Private Sector: Countries may have different levels of private sector ownership of the critical infrastructure and different mechanisms for engagement which have an impact on their government structure and policy for addressing CIIP.

107. www.enisa.eu.int

- Law Enforcement: Legal frameworks for cyber crime are important for co-operation. Thus it is challenging to address cross-border cyber crime issues without established legal frameworks.

- Culture: Recognising the importance of building and maintaining a culture of security in the face of rapid technological advances and competing priorities for time and resources is complex and challenging for many countries.

Government response

To address the challenges of international co-operation for CIIP, NCSD has incorporated collaboration with international entities into an International Programme towards its goals to establish a national cyber security response system and reduce cyber vulnerabilities. Specifically, a three-part strategy guides NCSD's international engagement in accordance with the overall mission of securing national cyberspace. The strategy includes the following elements:

- Engage in international outreach activities to build awareness about the global cyber risk and encourage national cyber security frameworks to share information about the role and activities of computer security incident response teams to mitigate the risk, and to build relationships among governments towards global co-operation on cyber security.

- Establish information-sharing relationships, communications mechanisms, and collaborative arrangements to increase our global cyber situational awareness; take advantage of global expertise; share good practices, experiences, and specific vulnerability information and analysis; and co-ordinate global cyber incident response.

- Establish collaborative arrangements for addressing the cyber component of critical infrastructure protection issues.

In general, NCSD is seeking to strengthen and build on existing bilateral, regional, and multilateral efforts to facilitate co-operation on CIIP issues which includes the exchange of information to build situational awareness and share expertise, and collaboration on priority efforts to manage the global cyber risk.