



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



Recommandation de l'OCDE du Conseil sur la protection des infrastructures d'information critiques [C(2008)35]



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

Séoul, Corée, 17 ~ 18 juin 2008

Accueillie par



방송통신위원회
KOREA COMMUNICATIONS COMMISSION

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

L'OCDE est un forum unique en son genre où les gouvernements de 30 démocraties oeuvrent ensemble pour relever les défis économiques, sociaux et environnementaux, que pose la mondialisation. L'OCDE est aussi à l'avant-garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu'elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et les défis posés par le vieillissement de la population. L'Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays membres de l'OCDE sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, l'Italie, le Japon, le Luxembourg, le Mexique, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Suède, la Suisse et la Turquie. La Commission des Communautés européennes participe aux travaux de l'OCDE.

Avant-Propos

Cette recommandation a été élaborée par le Comité de la politique de l'information, de l'informatique et des communications (PIIC), et son Groupe de travail sur la sécurité de l'information et la vie privée. La recommandation a été adoptée par le Conseil de l'OCDE lors de sa 1172^{ème} session, le 30 avril 2008.

Recommandation du conseil sur la protection des infrastructures d'information critiques

LE CONSEIL

Vu l'article 5(b) de la Convention relative à l'Organisation de coopération et de développement économiques, en date du 14 décembre 1960 ;

Vu la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité [C(2002)131], ci-après dénommée les « Lignes directrices sur la sécurité » ;

Vu la Résolution 58/199 adoptée par l'Assemblée générale des Nations Unies sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information ;

Reconnaissant que le fonctionnement de nos économies et de nos sociétés est de plus en plus tributaire de systèmes et réseaux d'information qui sont interconnectés et interdépendants, au plan tant intérieur qu'international ; qu'un certain nombre de ces systèmes et réseaux sont d'une importance nationale critique ; et que leur protection est un domaine prioritaire pour la politique publique nationale et la coopération internationale ;

Reconnaissant que pour améliorer la protection des infrastructures d'information critiques au plan national et international, les pays Membres doivent partager leurs connaissances et leur expérience dans l'élaboration des politiques et pratiques, et coopérer plus étroitement entre eux, ainsi qu'avec les économies non membres ;

Reconnaissant que la protection des infrastructures d'information critiques nécessite une coordination au plan intérieur et international avec les propriétaires et opérateurs privés de ce type d'infrastructures, ci-après dénommés « le secteur privé » ;

Sur la proposition du Comité de la politique de l'information, de l'informatique et des communications :

CONVIENT que :

Aux fins de la présente Recommandation, les infrastructures d'information critiques, ci-après dénommées « IIC » s'entendent comme désignant les systèmes et réseaux d'information interconnectés, dont la perturbation ou la destruction aurait un sérieux impact sur la santé, la sécurité, la sûreté ou le bien-être économique des citoyens ou sur le fonctionnement efficace du gouvernement ou de l'économie ;

Les IIC sont identifiées par le biais d'un processus d'évaluation des risques et englobent en général un ou plusieurs des éléments suivants :

- Les éléments d'information sur lesquels reposent les infrastructures critiques, et/ou ;

- Les infrastructures d'information sur lesquelles reposent des éléments essentiels des activités gouvernementales ; et/ou
- Les infrastructures d'information essentielles à l'économie nationale ;

RECOMMANDE que :

Les pays Membres mettent en place et maintiennent un cadre efficace pour la mise en oeuvre des Lignes directrices de l'OCDE sur la sécurité en relation avec la protection des IIC, en tenant compte des orientations générales et opérationnelles spécifiques exposées ci-après ;

PARTIE I. Protection des infrastructures d'information critiques au niveau national

Les pays Membres devraient :

Démontrer l'engagement et le soutien des pouvoirs publics en faveur de la protection des IIC en :

- Adoptant au plus haut niveau du gouvernement des objectifs d'action clairs ;
- Identifiant les agences et organisations gouvernementales ayant des responsabilités et des pouvoirs dans la mise en oeuvre de ces objectifs d'action ;
- Tenant des consultations avec les propriétaires et opérateurs privés d'IIC en vue d'instaurer une coopération mutuelle pour la mise en oeuvre de ces objectifs ;
- Assurant la transparence sur les délégations de responsabilités aux autorités et agences gouvernementales afin de faciliter une coopération plus étroite au sein des pouvoirs publics et avec le secteur privé ;
- Revoir de façon systématique les cadres politiques et juridiques et les mécanismes d'autorégulation pouvant s'appliquer aux IIC, notamment ceux qui visent à contrer les menaces transfrontières, afin d'évaluer s'il est nécessaire d'améliorer leur mise en oeuvre, de les modifier ou d'élaborer de nouveaux instruments ;
- Prenant des mesures, s'il y a lieu, pour rehausser le niveau de sécurité des éléments des systèmes et réseaux d'information constituant des IIC ;

Gérer les risques à l'égard des ICC en :

- Élaborant une stratégie nationale recueillant l'engagement de tous les intéressés, notamment des plus hauts niveaux du gouvernement et du secteur privé ;
- Prenant en considération les interdépendances ;
- Procédant à une évaluation des risques basée sur l'analyse des vulnérabilités et des menaces concernant les IIC, afin de protéger les économies et les sociétés contre les impacts les plus préoccupants au plan national ;
- Élaborant, sur la base d'une évaluation des risques, et en réexaminant régulièrement un processus national de gestion des risques qui précise dans le détail l'organisation, les outils et les mécanismes du suivi nécessaires pour

mettre en oeuvre la stratégie de gestion des risques à tous les niveaux, notamment :

- i. La structure organisationnelle appropriée pour fixer des orientations et promouvoir de bonnes pratiques de sécurité au niveau national, et gérer et suivre l'évolution de la situation, de même qu'un ensemble complet de procédures pour assurer l'état de préparation, notamment la prévention, la protection, l'intervention et le rétablissement de la situation en cas de menaces naturelles ou malveillantes ;
- Un système de mesure pour évaluer et jauger les dispositions en place (notamment des exercices et des tests selon les besoins), et permettre la remontée d'informations dans un processus d'actualisation continue ;
 - Mettant en place des moyens d'intervention en cas d'incident, tels qu'une équipe de réponse et traitement des incidents informatiques (CERT/CSIRTs), ayant une mission de surveillance, de veille, d'alerte et de mise en oeuvre de mesures de rétablissement de l'IIC, et des mécanismes pour promouvoir la coopération et la communication entre les intervenants chargés de réagir aux incidents ;

Œuvrer en partenariat avec le secteur privé en :

- Établissant des partenariats public-privé de confiance centrés sur la gestion des risques, l'intervention en cas d'incident et le rétablissement de la situation ;
- Permettant des échanges d'information mutuels et réguliers en mettant en place des dispositions de partage de l'information qui prennent en compte son caractère parfois sensible ;
- Encourageant l'innovation par le biais de projets de recherche et de développement public-privé centrés sur l'amélioration de la sécurité des IIC et, le cas échéant, le partage de ces innovations avec d'autres pays ;

PARTIE II. Protection des infrastructures d'information critiques au niveau international

Les pays Membres devraient coopérer entre eux et avec le secteur privé aux niveaux de la stratégie, des politiques et de l'exploitation pour assurer la protection des IIC contre des événements et des circonstances auxquels les pays ne sont pas en mesure de faire face isolément ;

Ils devraient notamment s'engager résolument dans une coopération bilatérale et multilatérale aux niveaux régional et mondial en vue de :

- Partager leurs connaissances et leur expérience en ce qui concerne l'élaboration de politiques et pratiques au plan intérieur et les modèles de coordination avec les propriétaires et opérateurs privés d'infrastructures d'information critiques ;
 - Élaborer une compréhension commune :
- ii. De la gestion des risques applicable aux dépendances et interdépendances transfrontières ;

- iii. Des vulnérabilités, menaces et incidences génériques concernant les IIC, afin de faciliter une action concertée contre celles qui ont un caractère généralisé, comme les failles de sécurité et le maliciel, ainsi que pour améliorer les stratégies et politiques de gestion des risques ;
- Rendre disponible l'information sur les agences nationales intervenant dans la protection des IIC et sur leurs rôles et responsabilités, afin de faciliter l'identification des homologues et améliorer la réactivité de l'action transfrontière ;
- Reconnaître la valeur de la participation aux réseaux internationaux et régionaux de veille, d'alerte et d'intervention sur incident, pour un échange d'information et une coordination robustes au niveau opérationnel, ainsi que pour une meilleure gestion de crise en cas d'incident s'inscrivant dans un contexte transfrontière ;
- Soutenir la collaboration transfrontière pour, et l'échange d'information sur, la recherche et de développement public-privé pour la protection des IIC ;

INVITE :

Les pays Membres à diffuser la présente Recommandation dans l'ensemble des secteurs public et privé, notamment auprès des autorités publiques, des entreprises et des autres organisations internationales afin d'encourager tous les participants concernés à prendre les mesures nécessaires pour la protection des IIC ;

Les économies non membres à prendre en considération la présente Recommandation et à collaborer avec les pays Membres dans sa mise en oeuvre ;

CHARGE le Comité de la politique de l'information, de l'informatique et des communications de l'OCDE de :

Promouvoir la mise en œuvre de la présente Recommandation et de la réexaminer tous les cinq ans afin d'encourager la coopération internationale sur les questions liées à la protection des IIC.