SYNTHÈSE DES CONCLUSIONS ET RECOMMANDATIONS

La Norvège est dotée d'un ensemble bien développé de politiques, d'institutions et de lois pour préserver et améliorer la sécurité des systèmes d'information et des réseaux. De plus, depuis la fin des années 90, la Norvège a pris plusieurs mesures importantes en la matière, aboutissant à une architecture législative et institutionnelle modernisée. L'essentiel des outils existants pour protéger la sécurité de l'information est spécifique aux différents secteurs : communications, banque et finance, énergie, etc. L'examen par l'OCDE des politiques de la Norvège en matière de sécurité de l'information fait ressortir la nécessité de définir un « minimum vital » de sécurité pour ces approches sectorielles et pointe quelques problèmes de coordination. L'objectif de cette synthèse est de présenter les principales constatations de l'étude, les actions possibles d'intervention et les recommandations qui ressortent de l'examen, en prêtant une attention particulière aux lacunes qui subsistent et aux points qui restent à améliorer.

Chapitre 1. Stratégie de la Norvège en matière de sécurité de l'information

Constatations

L'examen de la stratégie nationale en matière de sécurité de l'information et de sa mise en œuvre fait apparaître un certain nombre de points forts, mais aussi quelques éléments qui peuvent être améliorés. Si l'on regarde son champ d'application et de ses objectifs, la stratégie semble répondre à tous les problèmes de gestion de la sécurité de l'information ; il est précisé en particulier que « les infrastructures critiques de TI doivent être protégées sous leurs divers aspects : disponibilité, d'intégrité et de confidentialité ». Toutefois, s'agissant des outils eux-mêmes de cette politique de sécurité, l'attention portée à la disponibilité et à l'intégrité de l'information est très selon les différentes approches sectorielles. Au niveau trans-sectoriel, l'approche semble centrée sur la protection de la confidentialité des informations classifiées, mais l'importance de la définition d'un minimum vital s'agissant de la disponibilité et de l'intégrité n'est pas suffisamment reconnue. Ce reproche vaut aussi pour les mécanismes de coordination et de contrôle en place : les entités chargées de coordonner les mesures de sécurité pour les informations non classifiées ne semblent pas avoir les pouvoirs nécessaires pour s'acquitter de la totalité de leurs responsabilités formelles. Enfin, si la Stratégie fonctionne suivant un mode d'apprentissage, bien adapté aux réalités de la gestion de la sécurité de l'information, il serait possible à plusieurs niveaux de renforcer la surveillance, le feedback et l'évaluation des mesures d'application.

Actions possibles

Pour donner davantage de poids aux aspects de disponibilité et d'intégrité des systèmes, il serait souhaitable, à travers la nouvelle législation actuellement en discussion, de rectifier le déséquilibre entre sécurité, disponibilité et intégrité qui existe dans la loi relative aux services de protection de la sécurité. Il faudrait pour cela élargir le champ d'application de la loi au delà des informations et des systèmes classifiés, et y inclure les informations et systèmes revêtant de l'importance pour la sécurité de la nation et le bien-être de la société (à savoir les infrastructures critiques).

S'agissant de la gestion des informations non classifiées, la répartition des responsabilités pourrait être améliorée, en particulier au niveau la coordination des initiatives ministérielles, et de la création de normes et d'orientations sur la tolérance aux pannes des systèmes et les procédures de sauvegarde et de

reprise après des sinistres informatiques. Elles pourraient s'appliquer à l'ensemble des secteurs dans le cadre de l'application du concept de niveau national de préparation minimum (cet aspect est traité plus en détail dans la recommandation 5).

Le rôle de la société civile dans l'élaboration des politiques de sécurité de l'information pourrait être renforcé. Le savoir et l'expertise d'une large gamme d'acteurs – armée, police, société civile – sont nécessaires pour définir clairement des concepts tels que « infrastructures critiques », « sécurité de la société » et « continuité d'approvisionnement » et pour organiser la gestion du risque en conséquence (voir aussi la recommandation 6).

L'approche par apprentissage de la mise en œuvre ou de l'amélioration de la stratégie pourrait être renforcée en fixant des objectifs détaillés pour chaque ministère, en mesurant les progrès accomplis vers ces objectifs, et en évaluant régulièrement la performance globale du système de gestion de la sécurité de l'information au regard de la configuration de risque effective.

Recommandation 1 : Mettre au point les outils nécessaires et améliorer le partage des responsabilités pour la politique de la sécurité de l'information afin de mieux répondre aux exigences de disponibilité et d'intégrité.

Recommandation 2 : Élaborer un processus d'évaluation de la performance afin de mesurer l'efficacité des processus en place de contrôle de la sécurité de l'information au regard des menaces existantes.

Chapitre 2. Évaluer les risques pesant sur la sécurité de l'information

2.1. Évaluation des risques au sein de l'administration

Constatations

L'évaluation des risques pesant sur les systèmes administratifs n'est pas complète. Une norme globale pour l'administration a été adoptée mais elle n'est pas appliquée comme minimum vital de sécurité, et ne peut donc pas contribuer à simplifier la tâche délicate de l'évaluation des risques pour les systèmes administratifs.

En l'absence d'une évaluation complète et cohérente des risques, il est difficile d'attribuer la totalité des responsabilités de gestion de la sécurité et d'établir des priorités pour l'action des pouvoirs publics.

Actions possibles

La Norvège pourrait lancer un projet de création d'une norme en matière de gestion de la sécurité, par exemple en retenant la norme ISO 17799 comme minimum vital dans toute l'informatique de l'administration. En s'appuyant sur l'expérience des administrations d'autres pays et de grandes organisations, un processus de mise en œuvre progressive pourrait être défini : les ministères norvégiens pourraient par exemple viser l'auto-déclaration de conformité à la norme dans les cinq ans : ensuite, une certification officielle dans le cadre d'un dispositif national d'accréditation serait requise dans les dix ans. Cette approche systématique aurait l'avantage de donner l'exemple pour le secteur privé.

En outre, les contrats internes à l'administration et avec les entreprises sous-traitantes pourraient contenir une clause exigeant que soit démontrée la conformité avec les normes et les principes directeurs pertinents en matière de sécurité de l'information. En matière de liaisons réseau, accords internes à l'administration et avec des entreprises sous-traitantes pourraient également contenir un impératif de

démonstration de conformité avec les normes et principes directeurs pertinents en matière de sécurité de l'information.

Le NSM pourrait définir des Profils de protection avec des Critères communs pour les produits et systèmes certifiés qui soient aussi conformes aux règles de gestion de la sécurité définies dans la norme ISO 17799 pour répondre aux impératifs de la loi relative aux services de protection de la sécurité.

Une évaluation du risque au niveau ministériel pourrait établir en détail les impératifs de sécurité et clarifier les « règles du jeu » pour la mise en œuvre d'une norme de gestion de la sécurité en tant que minimum vital. Une partie de ces impératifs pourraient être définis par la conformité avec les lois générales de sécurité s'appliquant dans l'administration, les lois de protection des données, etc. D'autres pourraient avoir pour objectif d'assurer la continuité de fourniture des services essentiels dans le secteur du ministère.

Recommandation 3 : définir et mettre en œuvre un système reposant sur un minimum vital pour la gestion de la sécurité dans les systèmes de l'administration, complété par des évaluations ciblées du risque

2.2. Évaluation du risque dans les infrastructures critiques

Constatations

L'évaluation du risque pesant sur les infrastructures de l'information critiques n'est pas complète, mais le projet BA25, avec en particulier les travaux de la commission gouvernementale sur les infrastructures critiques, pourrait constituer une base solide pour ce travail.

Actions possibles

Dans le prolongement des travaux de la Commission gouvernementale sur les infrastructures critiques, un processus de dialogue entre les utilisateurs, les fournisseurs et les régulateurs des infrastructures critiques pourrait être mis au point pour l'ensemble des secteurs, afin de clarifier les aspects de gestion du risque, en particulier concernant la sécurité de l'information (voir aussi la recommandation 6).

Les utilisateurs et fournisseurs des infrastructures critiques pourraient aussi être invités à participer à l'élaboration du projet BAS5 (voir aussi recommandation 13).

Recommandation 4 : Mettre en place une procédure systématique d'évaluation des risques pour les infrastructures critiques

Chapitre 3. Protéger les systèmes d'information

Section 3.1 Protection des systèmes administratifs

Constatations

Les responsabilités relatives à la politique de sécurité de l'information sont dispersées entre un trop grand nombre d'acteurs ministériels pour être assumées de manière cohérente.

Actions possibles

La Norvège pourrait envisager d'autres solutions pour mieux coordonner sa politique nationale de sécurité de l'information. Par exemple, il serait possible d'attribuer clairement un rôle d'orientation à un ministère donné sur tous les aspects de la sécurité de l'information au-delà du champ d'application actuel de la Loi relative aux services de protection de la sécurité, avec pour mandat de développer la sécurité de l'information comme faisant partie intégrante de l'administration en ligne et de l'électronique d'entreprise. Cela permettrait de réduire le risque de mesures redondantes entre différents ministères et de cibler les efforts sur les aspects prioritaires.

Il serait aussi possible de coordonner les politiques relatives à la sécurité de l'information au niveau du Cabinet (à l'image de la solution proposée dans la recommandation 10 pour la gestion des urgences). Dans ce modèle, les différents ministères pourraient ensuite assumer la responsabilité d'exécution des tâches prioritaires et de production effective des améliorations.

Autre possibilité, qui serait compatible avec une architecture décentralisée, la fixation de normes définissant l'approche minimale à un niveau central, le suivi et l'application étant effectués au moyen d'évaluations de la gestion et de la performance dans le cadre des procédures d'audits de l'administration.

Recommandation 5 : Répartir les responsabilités entre un plus petit nombre d'acteurs au sein de l'administration

Section 3.2. Protection des systèmes d'infrastructure critiques

Constatations

Deux grands problèmes ont été mis en évidence en matière de protection des infrastructures critiques ; d'abord, il y a un manque de clarté dans la division des responsabilités de protection des infrastructures critiques entre l'administration et les opérateurs, notamment au niveau du traitement des interdépendances entre infrastructures ; ensuite, il faudrait instaurer une communication et une coopération systématique entre les propriétaires et les opérateurs de toutes les infrastructures critiques.

Actions possibles

Pour faciliter une communication et une coopération régulières, les pouvoirs publics pourraient commencer par dresser un tableau général de tous les acteurs des infrastructures critiques, quelle que soit leur taille, avec leur situation en matière de sécurité (par exemple en relation avec le projet BAS5).

Un dialogue systématique et plurisectoriel entre l'administration, les opérateurs et les utilisateurs des infrastructures critiques (comme décrit dans la recommandation 4) pourrait répondre aux questions sur le niveau de risque acceptable dans les infrastructures critiques, et du niveau de sécurité que doivent assurer les opérateurs dans le cadre de leur fonctionnement normal. Ce dialogue pourrait déboucher sur une répartition claire des responsabilités entre opérateurs, autorités de régulation et organes de supervision en matière de protection des infrastructures critiques, établi dans un contexte plus large que celui de la surveillance réglementaire des marchés.

Différents mécanismes pourraient être mis en place pour assurer le respect de la règle de droit en matière d'infrastructures critiques : lois en matière de responsabilité, incitations économiques benchmarking.

Les responsabilités et les compétences pourraient de plus être établies pour les problèmes de gestion des interdépendances et de continuité de fourniture qui sortent du champ de compétence des régulateurs sectoriels, en coopération avec ceux-ci.

Recommandation 6 : Déterminer le niveau de risque acceptable et le partage des responsabilités dans la gestion des risques de chaque infrastructure critique.

Recommandation 7 : Renforcer l'implication des opérateurs dans les activités de gestion des risques

Chapitre 4. Alerte et sauvetage

Section 4.1 gestion des incidents

Constatations

Une crise majeure de sécurité de l'information aurait sans doute un impact considérable sur les PME et sur la société dans son ensemble ; il existe pourtant peu de mesures pour inciter le secteur privé à mettre en place une fonction de réponse aux incidents.

Actions possibles

Pour combler ce déficit de capacité, il est suggéré que le gouvernement norvégien crée un CERT spécifiquement axé sur les besoins du secteur privé, et en particulier sur ceux des PME, en relation avec le SIS et le NSO (voir recommandation 11).

Recommandation 8 : Favoriser l'élaboration d'un système de soutien à la gestion des incidents pour les PME

Section 4.2. Planification des urgences et préparation

Constatations

Il existe un vide de responsabilité au niveau du conseil et de l'audit de la planification d'urgence pour les infrastructures critiques privées et les services publics qui n'ont pas à traiter d'informations classifiées.

Deux organismes, le NSM et le DSB, pourraient dispenser des avis sur le niveau de préparation en matière de sécurité, la planification des urgences et les scénarios de menace. Ils sont aussi chargés des audits.

Actions possibles

Les pouvoirs publics pourraient développer une capacité de conseil pour les utilisateurs des secteurs public et privé afin d'encourager à la création de plans d'urgence.

Une fonction administrative d'audit pourrait être étendue à toutes les infrastructures critiques que leurs propriétaires ou leurs exploitants soient publics ou privés, et qu'elles aient à traiter des informations classifiées ou non. Les audits pourraient aussi être confiés au secteur privé.

Parallèlement, les pouvoirs publics pourraient aussi envisager d'appliquer le principe de séparation des fonctions d'audit et de conseil, qui est devenu très courant, voire obligatoire pour le secteur privé.

Recommandation 9 : Renforcer les services publics de conseil et d'audit afin d'améliorer le niveau de préparation et la planification d'urgence.

Section 4.3 Gestion des urgences et gestion de crise

Constatations

Un centre national de gestion de crise peut jouer un rôle vital dans le suivi d'une crise de TI à mesure qu'elle se développe, et atténuer ses effets si elle dépasse le stade de l'incident ou de l'urgence.

Actions possibles

Pour plus d'efficacité, il faut que les membres clés d'un centre national de gestion de crise aient une compétence collective de direction et de gestion des ressources une fois qu'une situation de crise est déclarée. Il peut être nécessaire de que cette compétence et la déclaration de cette crise nécessite s'appuient sur le Parlement et sur une législation en matière de gestion des crises. Ce centre pourrait être une composante du Conseil d'urgence du Cabinet, nouvellement créé (voir aussi recommandation 5).

Recommandation 10 : Créer une fonction nationale de gestion des crises de TI

Chapitre 5 : Renforcer les fondements de la sécurité

Section 5.1. Sensibilisation

Constatations

Les actions de sensibilisation ne sont utiles que si elles sont accompagnées d'un soutien en cas d'incidents et si des solutions sont proposées. A cet égard, le lancement de NettVett et la décision de faire de SIS une organisation permanente essentiellement tournée vers les PME sont deux mesures positives prises depuis quelques mois.

Actions possibles

Pour soutenir les progrès récents accomplis en direction des petites entreprises et du grand public, les autorités pourraient assurer la viabilité de SIS et de NettVett en pérennisant leur financement.

Des partenariats pourraient être développés avec SIS pour renforcer les actions en direction des entreprises et de la société civile.

Enfin, la création d'une structure de type CERT dédiée aux PME pourrait contribuer à promouvoir des solutions tout en développant la sensibilisation à l'égard des risques (voir recommandation 8).

Recommandation 11 : Améliorer et rationaliser les actions de sensibilisation en direction des PME et du grand public

Section 5.2 Partage des informations

Constatations

Il existe au sein des différents ministères et agences un savoir et une expérience considérables en matière de sécurité de l'information, mais les occasions de partager ces connaissances sont limitées dans

certains cas en raison de « silos » sectoriels existant au sein des ministères. Il serait souhaitable de stimuler les échanges d'informations et de bonnes pratiques entre utilisateurs sur les moyens de sécuriser les réseaux et systèmes d'informations, en fonction de leur niveau individuel de maturité en matière de sécurité de l'information.

Actions possibles

Une option économique pour fournir des plates-formes de soutien aux PME consisterait à parrainer, à encourager et à promouvoir de petits groupes locaux d'entraide, avec le soutien et les conseils d'experts extérieurs issus de l'administration et des universités.

Le fonctionnement et les rôles des forums ouverts et fermés pourraient être plus clairement différenciés en fonction du niveau de sensibilité des informations échangées.

SIS et NorCERT pourraient être utilisés pour offrir des plates-formes plus actives et plus larges de partage de l'information pour tous types d'utilisateurs, avec des outils spécifiques pour les différents groupes cibles : particuliers, PME, administrations publiques, etc. (voir aussi recommandation 11) ;

Recommandation 12 : Stimuler les échanges d'information et de bonnes pratiques entre utilisateurs

Section 5.3 Enseignement et R&D

Constatations

Les liens entre la recherche et la stratégie nationale norvégienne en matière de sécurité de l'information sont particulièrement ténus ; les bénéficiaires de la recherche en bout de course semblent avoir peu de moyens pour influencer le contenu des programmes de recherche.

Lorsque les programmes de recherche sont orientés vers une question ou une solution particulières, leur surveillance pourrait être facilitée si un plan d'exploitation des programmes était établi dès leur conception. Cela permettrait de définir plus clairement les bienfaits escomptés et les bénéficiaires des recherches. C'est cette démarche qui semble faire défaut à un projet comme le BAS5, ce qui pourrait expliquer le glissement graduel de son contenu, de ses objectifs et de ses ressources.

Actions possibles

Le partage d'information avec les départements ministériels et les agences concernées devrait être une condition obligatoire à tout accord de parrainage de recherches dans ce domaine. De telles relations n'ont pas été observées dans les initiatives de recherche examinées.

Une stratégie nationale pour la recherche en matière la sécurité de l'information permettrait d'identifier les lacunes, de définir les priorités pour l'attribution des ressources, d'orienter les programmes de recherche et de mettre en évidence les domaines où la coopération avec des équipes étrangères pourrait être la plus fructueuse.

Les utilisateurs et les bénéficiaires potentiels de la recherche pourraient avoir davantage de poids dans la définition et l'orientation des programmes de recherche. Le KIS est un cadre possible pour ce type de rencontre, à condition que le secteur privé soit associé plus spécifiquement. Le KIS pourrait aussi avoir la possibilité de commanditer, de financer et d'évaluer des recherches, afin de donner plus d'importance à la demande dans l'orientation des programmes de recherche.

Recommandation 13 : Définir une stratégie nationale de recherche sur la sécurité de l'information et renforcer l'influence de la demande dans l'orientation des projets de recherche.