COMITÉ PERMANENT DE CONTRÔLE DES
SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ

Enquête de contrôle 2007.181

Conclusions et recommandations de l'enquête sur la manière dont les services belges de renseignement envisagent la nécessité de protéger les systèmes d'information contre des interceptions et cyberattaques d'origine étrangère

La protection des systèmes d'information et de leurs interconnexions, gérés au moyen des nouvelles technologies informatiques, est une préoccupation régulièrement évoquée au Parlement fédéral. La sécurité des réseaux de communications électroniques est un des éléments essentiels au développement de la société de l'information. Les moyens techniques actuels d'interception et d'interférence sur les systèmes d'information et de télécommunication font assurément peser des menaces, non seulement sur la sécurité et sur les intérêts militaires, stratégiques et économiques du pays, mais aussi sur les droits et les libertés fondamentales des citoyens.

Le Comité permanent R l'a souligné plusieurs fois dans ses rapports. Les commissions parlementaires chargées du suivi du Comité permanent R ont partagé et relayé ces inquiétudes auprès du gouvernement. Dès 1994, le Comité a attiré l'attention du Parlement sur l'importance de la sécurité des systèmes d'information officiel : il avait recommandé qu'un organisme officiel soit chargé de concevoir et d'appliquer une politique globale de sécurité des systèmes d'information pour l'ensemble de la fonction publique.

Depuis lors, la Loi du 10 juin 1998 modifiant la Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise connaissance et l'enregistrement de communications et de télécommunications privées, est entrée en vigueur le 2 octobre 1998.

Dans son rapport d'activités 2006, le Comité permanent R a encore rappelé qu'il était opportun d'appliquer le principe général de précaution en vue d'élaborer cette politique globale de sécurité. Il a aussi fait remarquer que la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité conférait au SGRS la mission de protéger les systèmes d'information et de communications

militaires. A cette fin, le Comité permanent R avait recommandé que la Défense établisse les règles complémentaires d'exécution des normes de l'OTAN et de l'UE afin de pouvoir identifier et neutraliser toute tentative de pénétration dans ses systèmes informatiques.

Le Comité n'a donc jamais relâché son attention sur la manière dont les services de renseignement belges abordaient les menaces sur la sécurité des systèmes de télécommunications, y compris celles pouvant émaner de pays alliés de la Belgique.[1]

Il convient aussi d'observer la tendance actuelle de nombreux gouvernements étrangers de renforcer les prérogatives et les moyens d'action de leurs services de renseignement, notamment en renforçant leurs capacités d'écoutes et d'interception des télécommunications et messages électroniques, ceci tant à l'intérieur qu'à l'extérieur de leurs frontières.[2]

Les technologies permettant l'interception de communications satellitaires ou sur Internet devenant de plus en plus performantes et accessibles, des sociétés commerciales s'activent aussi sur ce marché de l'interception et de la sécurité, qui intéresse particulièrement les services de renseignement.[3]

La Belgique ne fait pas exception à la tendance de renforcer ses moyens d'écoute. En témoignent notamment certaines dispositions de la nouvelle Loi du 4 février 2010 relative aux méthodes de recueil des données des services de renseignement et de sécurité.[4]

Le Comité permanent R rappelle à cet égard que le contrôle de la manière dont le SGRS pratique les interceptions de communications à l'étranger entre déjà dans le cadre de ses missions légales. Le Comité veille ainsi à ce que les capacités d'interception accordées à ce service soient exclusivement utilisées conformément à leur finalité légale, qui est d'assurer la sécurité extérieure et militaire du pays ainsi que celle des ressortissants belges à l'étranger.

---

1 COMITE PERMANENT R, *Rapport d'activités 2000*, 29, « Rapport de synthèse sur la manière dont les services de renseignement réagissent face à l'éventualité d'un réseau Echelon d'interception des communications en Belgique », 64, « Rapport de l'enquête sur la manière dont les services de renseignement ont réagi à propos d'éventuels faits d'espionnage ou de tentative d'intrusion dans le système informatique d'un centre de recherche belge » et *Rapport d'activités 2004*, 43, « Rapport relatif aux constatations faites dans le cadre de l'enquête sur une éventuelle mise sous écoute téléphoniques de magistrats par les services de renseignement ».

2 Par exemple, la Loi « *Protect America Act* » de 2007 étend les capacités d'interception des communications internationales déjà accordées aux services de renseignement américains par la Loi « *Foreign Intelligence Surveillance Act* » (FISA).

3 *Intelligence Online*, (IOL) n° 572 du 15 juin 2008 énumère une dizaine de firmes américaines, françaises et européennes fournisseuses de logiciels d'interceptions, de sécurité et de protection de données.

4 *M.B*, 10 mars 2010.

Depuis quelques années, l'actualité est riche en informations faisant état d'écoutes téléphoniques, d'interceptions abusives de télécommunications, de fuites d'informations sensibles, d'intrusions malveillantes dans des systèmes informatiques d'entreprises ou d'autorités publiques, aussi bien en Belgique qu'à l'étranger.[5]

Selon Luc Beirens, chef de la « *Federal Computer Crime Unit* », (FCCU) l'unité de la Police judiciaire fédérale chargée de la lutte contre la cybercriminalité, les menaces intentionnelles contre les systèmes d'information peuvent émaner de plusieurs sources. Il y a les pirates informatiques agissant individuellement ou en réseau, les organisations criminelles, les mouvements terroristes ainsi que certains Etats (Inde, Chine, Corée du Nord, Russie, etc.) qui développent des systèmes destinés à attaquer les infrastructures qui revêtent une importance critique pour les autorités et les entreprises privées d'autres pays.[6]

La question de départ de la présente enquête porte sur la manière dont les services belges de renseignement envisagent la nécessité de protéger les systèmes d'information contre des interceptions d'origine étrangère. A cette question, la réponse est claire : tant la Sûreté de l'État que le SGRS ont conscience de la gravité des menaces que représentent les attaques informatiques, d'origine étatique ou non, dirigées contre les systèmes d'informations vitaux (civils et militaires) du pays.

Les deux services ont dès lors pris des initiatives en vue de sensibiliser leurs « clients » à la problématique générale des attaques informatiques, aux vulnérabilités de leurs systèmes d'information et à la nécessité de prendre des mesures de protection. Le travail accompli en ce sens est remarquable.

Dans la mesure des moyens limités mis à leur disposition, les services de renseignement belges enquêtent aussi sur les attaques détectées sur les systèmes d'information des autorités tant civiles que militaires. Mais il s'agit encore d'une approche essentiellement défensive de détection, d'évaluation et de réaction.

Force est cependant de constater que l'absence d'une politique fédérale globale en matière de sécurité de l'information (et de réelle autorité en la matière) entraîne une très grande vulnérabilité du pays en cas d'agression sur ses systèmes et réseaux vitaux d'information.

Les menaces qui pèsent sur ces systèmes d'information sont susceptibles de porter atteinte à la sécurité et aux intérêts fondamentaux de l'Etat tels que définis par les

---

5 L'actualité de cette fin d'année 2010 avec les fuites révélées par l'affaire « *Wikileaks* » en est un flagrant exemple.

6 *Doc.Parl.*, Chambre, 2007-2008, 0898/001, Rapport fait au nom de la Commission de l'infrastructure, des communications et des entreprises publiques par Roel Deseyn « Sécurité TIC ».

articles 7 et 11 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

Plusieurs institutions fédérales s'occupent à présent des questions de sécurité des systèmes d'information : l'Autorité Nationale de Sécurité (ANS), FEDICT, BELNET et l'IBPT. Aucune d'elles ne semble pourtant avoir une vue d'ensemble sur l'infrastructure critique des systèmes d'information.[7] Les moyens techniques mis à la disposition de l'ANS sont nettement insuffisants.

Compte tenu de ce grand morcellement de la politique en matière de sécurité des systèmes d'information, le Comité permanent R souscrit aux conclusions du « *livre blanc pour une politique nationale de sécurité de l'information* » et il recommande l'élaboration d'une stratégie fédérale en la matière et la création rapide d'une agence chargée de coordonner les activités visant à la sécurité de l'information.[8]

Le Comité permanent R est convaincu que les services de renseignement belges disposent d'une expérience et d'un savoir-faire qui sont susceptibles d'être mis en œuvre au sein ou au profit d'une agence de sécurité de l'information à créer.

Au niveau international, le SGRS et la VSSE assurent parfois une représentation dans certains groupes de travail, mais sans réelle coordination avec les autres autorités concernées. Un effort de clarification du rôle assigné aux services de renseignement dans la protection des systèmes d'information du pays semble donc nécessaire et le Comité permanent R recommande que le Comité ministériel du Renseignement et de la Sécurité s'y attèle. Encore faudrait-il que nos services de renseignement disposent des moyens nécessaires pour accomplir cette tâche et qu'ils puissent notamment recruter (et conserver) chez eux des ressources humaines qualifiées. Les statuts administratifs et pécuniaires actuellement proposés par la Fonction publique ne sont pas de nature, en regard des salaires du secteur privé, à exercer un grand attrait pour du personnel possédant de hautes qualifications en informatique. Le Comité permanent R considère la faiblesse actuelle des moyens humains qualifiés des services de renseignement comme très problématique. Il recommande que ces services puissent enfin recruter les ressources humaines qualifiées nécessaires à l'exécution de leur mission en matière de sécurité informatique.

Le Comité permanent R considère également la faiblesse des moyens techniques de certification et d'homologation comme très problématique sur le plan de la sécurité informatique. Il recommande que les moyens nécessaires soient enfin mis

---

7 Pendant le mois de mars 2010, l'inventaire des infrastructures critiques ITC était cependant en cours de développement au sein du service FEDICT.

8 De telles agences existent dans des pays voisins tels que la France (*Agence Nationale de la Sécurité des Systèmes d'Information* » (ANSSI) dépendant du Premier ministre) l'Allemagne (« *Bundesamt für Sicherheit in der Informationstechnik* » (BSI) dépendant du ministère de l'Intérieur), le Royaume Uni («Office of Cyber Security » (OCS) dépendant du Premier ministre).

en place pour que la certification et l'homologation des systèmes utilisés pour le traitement d'informations classifiées en Belgique puissent enfin se faire sans dépendre d'autorités et de services étrangers.

Le Comité recommande aussi la plus grande prudence dans le choix des équipements techniques sécurisés nécessaires au traitement d'informations sensibles et classifiées, notamment en rapport avec l'application des méthodes de recueil des données des services de renseignement et de sécurité. Faisant siennes les recommandations du livre blanc élaboré par la plate-forme de concertation sur la sécurité de l'information, le Comité recommande que ce matériel fasse l'objet d'une évaluation, d'une certification et d'une homologation quant à sa fiabilité et à sa sécurité selon des critères et une procédure conformes aux normes de l'Union européenne.

Le Comité permanent R recommande également la plus grande prudence dans le choix des fournisseurs de ce matériel. Le Comité recommande que pour la passation de ces marchés, la possession d'une habilitation de sécurité soit imposée aux firmes adjudicataires.

Le Comité recommande que les liens éventuels de ces firmes avec certains services de renseignement étrangers fassent l'objet d'une attention toute particulière lors de l'enquête de sécurité.

La Loi du 4 février 2010 relative aux méthodes de recueil des données des services de renseignement et de sécurité a accordé au SGRS un moyen de riposte en vue de contrecarrer des cyberattaques menées contre les systèmes informatiques de la Défense nationale. Le Comité recommande toutefois qu'il soit aussi envisagé de prévoir cette faculté de neutralisation de systèmes à l'étranger en cas d'attaques menées contre les systèmes informatiques d'autres départements ministériels que la Défense (Services du Premier ministre, SPF Affaires étrangères, VSSE, etc.) ou contre ceux d'infrastructures critiques pour le fonctionnement du pays. La VSSE pourrait recevoir cette mission.