Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: 150 (2005)
Heft: 6-7

Artikel: Le terrorisme islamiste et l'arme "Technologie de l'information" : des défis en matière de politique de sécurité
Autor: Regli, Peter
DOI: https://doi.org/10.5169/seals-346501

Le terrorisme islamiste et l'arme «Technologie de l'information»

Des défis en matière de politique de sécurité

L'état actuel du monde lance de sérieux défis en matière de politique de sécurité. Parmi ceux-ci, on relèvera entre autres la problématique posée par les flux migratoires, le crime organisé, la corruption, le terrorisme, le fondamentalisme islamiste, les armes de destruction massive de type nucléaire, chimique ou biologique ainsi que, dans une mesure grandissante, la propagation de maladies infectieuses, par exemple le virus de la grippe aviaire H5N1 qui constitue une menace émergente pour les sociétés occidentales.

Div Peter Regli[1]

Dans ce contexte, la recherche et le traitement de l'information, bien qu'encore sous-estimés, n'en revêtent pas moins une importance croissante. Il convient de distinguer l'information utilisée comme moyen de pression par les médias et celle façonnée grâce à la plus moderne des technologies, à savoir le «Technologie de l'information» *(IT)*, qui nous fait entrer de plein pied dans l'ère de la *cyberguerre* et de la *netwar*. Les milieux concernés ont néanmoins pris conscience de la vulnérabilité de l'*IT* dès le milieu des années 1990. Elle est d'ailleurs qualifiée d'«infrastructure nationale critique» par les organes étatiques.

De la vulnérabilité de l'«IT»

La technologie de l'information est très vulnérable. Elle est exposée aux abus et aux manipulations. Dans un Etat de droit, les rouages, en principe bien huilés, des infrastructures peuvent être facilement endommagés. L'administration publique et l'économie privée sont en train de prendre des mesures plus ou moins ciblées, afin de se prémunir contre toutes sortes d'intrusions clandestines, en particulier celles commises par les *hackers* et les *crackers*. Il faut malheureusement constater que la Suisse n'a pas encore accompli de progrès significatifs sur le plan de la coordination en vue d'identifier et d'écarter de telles menaces. On a trop souvent tendance à oublier ou à négliger le fait que l'homme, en sa qualité de point de jonction d'un réseau, constitue encore et toujours le maillon faible d'une organisation.

Des offensives déclenchées au niveau de l'information sont susceptibles de causer des dommages importants et irréparables, tant aux privés qu'à l'appareil étatique ainsi qu'à l'économie. Dans l'éventualité d'une combinaison de scénarios-catastrophe, par exemple une attaque terroriste qui exige la mobilisation simultanée de plusieurs entités (dont les corps sanitaires, la police et les sapeurs-pompiers), la mise hors service des systèmes *IT* de ces organisations entraînerait des conséquences inimaginables.

De l'«IT» comme arme du terrorisme

Un autre danger, qui se précise chaque jour davantage pour une nation occidentale et judéo-chrétienne comme la nôtre, réside dans le fondamentalisme islamiste. Ce nouveau type de totalitarisme, qu'on peut qualifier de «tumeur cancéreuse», a déjà essaimé dans plus de soixante pays, dont l'Europe de l'Ouest et la Suisse. Les observateurs attentifs constatent que les militants islamistes engagent de façon ciblée et professionnelle l'arme moderne que constitue l'*IT* dans la planification et la mise en œuvre de leurs attentats.

Les terroristes ont besoin des médias. Leurs actes criminels

[1] *Ingénieur EPFZ, ancien chef du Service de renseignement suisse (1990-1999). Cet article a été rédigé pour la* Newsletter *d'avril 2005 du site www.security-zone.info ainsi que pour l'ASMZ 6/05. Il a été traduit de l'allemand en français par le maj Raphaël Schaer, EM br inf 2, officier de milice et avocat.*

doivent être communiqués sans tarder à l'échelle planétaire pour en garantir le meilleur impact psychologique. A cette fin, ils utilisent des caméras digitales, le réseau Internet et des chaînes de télévision telles qu'Al Jazeera et Al Arabia. Leurs sites Internet contiennent entre autres des appels religieux, des données chiffrées relatives aux attentats en cours de planification, des vidéos de prises d'otages, de chantages et d'exécutions sanglantes, voire des instructions pour construire des bombes artisanales ou des armes de destruction massive. Des téléphones portables, autres produits emblématiques de l'*IT*, sont transformés en détonateurs à distance de charges explosives. Des groupes islamistes se servent du réseau Internet pour endoctriner et manipuler leurs communautés religieuses. Les Etats démocratiques sont ainsi confrontés à une nouvelle menace complexe et très difficile à maîtriser.

De la nécessité d'agir

Les organisations terroristes exploitent et engagent toujours plus fréquemment les moyens offerts par l'*IT*. Les Etats démocratiques sont contraints à réagir. Pour cela, ils doivent pouvoir se façonner une vision claire et globale de la situation. Cette vue d'ensemble, seuls des services de renseignements efficaces sont susceptibles de la leur procurer. Les instruments conventionnels et largement éprouvés du renseignement ne suffisent cependant plus à remplir une telle mission. La situation exige le recrutement de nouveaux moyens tels que celui d'*IT freaks* intuitifs, perspicaces et expérimentés. Ces derniers devront être capables d'explorer le réseau Internet en suivant des critères précis et de trouver, selon l'expression consacrée, «une aiguille dans une meule de foin». Leur tâche consistera à détecter les activités illégales, comme les appels à la haine ou à des actes terroristes, ainsi qu'à rassembler les indices des diverses conspirations en cours. Ceci requiert des aptitudes particulières. Des connaissances élémentaires en matière d'*IT* n'y suffisent pas. La maîtrise de langues spécifiques se révèle également indispensable. Les sites visés sont en effet habituellement rédigés en arabe, farsi, pashtu, tadjik ou en toute autre langue fort exotique sous nos latitudes.

De la responsabilité des politiques

Compte tenu des dangers esquissés, gouverner est devenu chose plus complexe et plus périlleuse. L'incertitude ambiante influence largement notre manière d'appréhender et de gérer le quotidien. Nos politiciens devraient se poser sans relâche les questions suivantes: «Savons-nous vraiment ce que nous savons?» et, a contrario, «Savons-nous vraiment ce que nous ignorons?». Cogiter sur de telles questions leur permettrait d'assigner à leurs services de renseignement des missions concrètes et ciblées. Au sein de ces derniers, la branche de l'IT est venue se greffer depuis quelque temps sur les traditionnels domaines de la recherche et de l'analyse. Les services se sont vus forcés de créer de nouveaux centres de compétences chargés, d'une part de prendre des mesures destinées à protéger leurs propres systèmes informatiques, d'autre part d'infiltrer les systèmes d'ennemis potentiels. Ce mode opératoire particulier impose des aménagements, tant au niveau des bases légales, que dans la manière de travailler. Il faut en effet garder à l'esprit que, tandis que l'ennemi asymétrique ne reconnaît ni règles ni conventions, l'Etat de droit ne peut agir que dans un cadre légal. Cette asymétrie est largement profitable et du reste exploitée sans vergogne par l'adversaire.

Bilan

L'*IT* occupe une place toujours plus importante dans les thèmes relevant actuellement de la politique de sécurité. La mission des services de renseignement est d'assurer la protection de l'Etat et de sa population. Les responsables politiques devraient donc veiller à fournir à ces derniers les moyens légaux et logistiques ainsi que les compétences indispensables à l'accomplissement de leur travail. Négliger la sécurité au profit des finances, comme on le fait en Suisse aujourd'hui, est tout à fait irresponsable. La sécurité doit s'adapter à la situation, ce qui implique forcément que des moyens financiers correspondants lui soient octroyés. C'est notre seule chance d'identifier, d'évaluer et d'écarter, efficacement et à temps, des menaces comme celles que font planer les opérations menées par les cellules terroristes islamistes. Compte tenu du péril que représente l'alliance de l'*IT* avec le terrorisme, les succès enregistrés dans la lutte contre la pornographie sur Internet apparaissent quelque peu dérisoires.

P. R.