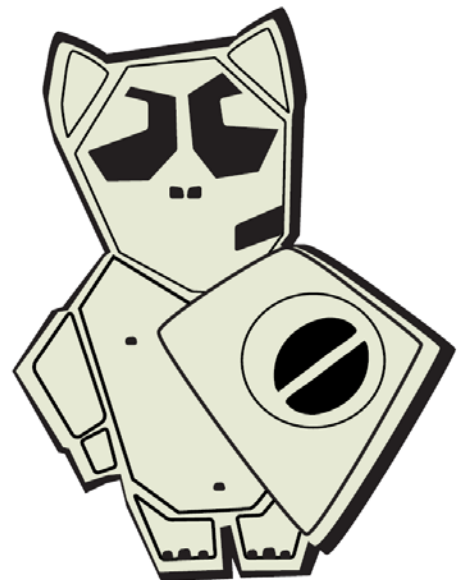


Protection contre la cyberguerre



Adopté par la Présidence le 12 novembre 2010

L'art de la guerre a subi des transformations énormes depuis la fin de la guerre froide. L'époque où les guerres n'opposaient que des États est révolue. Très récemment, la «guerre contre le terrorisme» a montré que des groupes de privés et des États se font également la guerre. Bien qu'il existe aujourd'hui d'énormes différences de ressources entre les États et à plus forte raison entre les privés, ceux-ci peuvent néanmoins se livrer des guerres (asymétriques). Les opérations militaires ne se déroulent plus nécessairement sur le champ de bataille ou dans le cadre d'une action de guérilla. Les réseaux informatiques jouent en l'espèce un rôle important. Pour la Suisse, les menaces les plus imminentes ne sont plus les traditionnelles divisions blindées ou attaques aériennes, mais les offensives contre l'infrastructure digitale de notre pays. Nos réseaux digitaux sont notre talon d'Achille. Une cyberattaque est à même de causer des dégâts considérables à l'économie, aux infrastructures, voire à l'espace vital suisses. Nos transports, l'alimentation en courant, le système des assurances sociales, les banques: tout dépend du Net et est potentiellement manipulable. D'un jour à l'autre, notre pays pourrait être littéralement replongé dans le Moyen Âge. Nous exigeons par conséquent:

- **Protection des réseaux de communication et des données comme tâche de l'État:** chaque jour, les réseaux de communication et les données de la Suisse font l'objet de milliers d'attaques à visées criminelles. Notre économie et nos autorités étatiques en subissent des dommages considérables. Des connaissances sont dérobées (piraterie commerciale), des machinations frauduleuses sont permises, et le travail d'innombrables employés est ralenti, voire interrompu pendant des heures. La protection des réseaux de communication et des données de la Suisse et de son économie doit par conséquent être érigée en tâche de l'État au plan constitutionnel.
- **Chapitre concernant la cyberguerre dans le rapport sur la politique de sécurité:** en premier lieu, il convient de rattraper ce que le Conseil fédéral a omis dans le rapport sur la politique de sécurité. En effet, le thème de la cyberguerre doit être analysé à fond, y compris les transitions fluides du cybercrime et de la cyberguerre. Il sied également de formuler des mesures pour la prévention et la lutte contre les menaces existantes et futures d'organisations cyberterroristes, un plan concret devant être présenté pour leur mise en œuvre.
- **Concept pour la protection de l'infrastructure digitale de la Suisse:** il faut présenter un concept permettant aux forces de sécurité réunies de notre pays – y compris l'armée – d'atteindre, en association avec l'économie et la recherche, la capacité de protéger l'infrastructure digitale de la Suisse dans son ensemble. La lutte incessante sur Internet constituera une tâche centrale des forces de sécurité au XXI^e siècle. Le concept doit montrer quelles tâches l'armée assumera au sein de

l'association, et sous quelle forme d'organisation. Cela étant, la mission «l'armée se protège elle-même» est certainement insuffisante également en ce qui concerne la cyberguerre.

Définitions

Afin de permettre une meilleure compréhension de la thématique, voici quelques définitions de base:

Cyberattaque, cyberoffensive: de nombreuses formes de telles attaques sont possibles; l'éventail va de simples efforts de mettre des ordinateurs hors d'état de fonctionner à l'objectif de l'espionnage.

Cybercrime, criminalité en réseau, criminalité Internet, machinations criminelles sur Internet: différents termes utilisés pour les actes criminels commis exclusivement ou partiellement avec l'aide de la technologie d'information et de communication. Actes criminels perpétrés dans le – ou autour du – cybermonde de privés avec des moyens informatiques et revêtant une dimension pénale.

Cybermonde / monde virtuel: on désigne comme «virtuel(le)» une entité (quelque chose) qui n'existe pas physiquement, mais déploie néanmoins des effets. Ce monde virtuel s'appelle également *cybermonde*. Les ordinateurs relient des êtres humains, des machines, etc. sous des formes très rapides et surtout invisibles.

Cyberguerre: la cyberguerre est la guerre menée dans l'espace virtuel, que l'on peut se représenter en soi comme une concentration d'actions offensives menées par ordinateur sur différentes infrastructures cruciales de la Suisse, ou comme partie d'un concept d'attaque plus complet comprenant par exemple des sanctions et manœuvres dilatoires juridiques et économiques, voire classiquement militaires. Toutes les activités dirigées contre l'État, ses institutions ou son intégrité, contre la population ou des parties de celle-ci et en mesure de menacer leur existence sont concernées. Les cyberguerres sont menées par des États ainsi que des organisations paraétatiques ou terroristes.