Quels enjeux politiques en matière de cyberdéfense?

Autor(en): **Dupuy, Emmanuel**

Objekttyp: **Article**

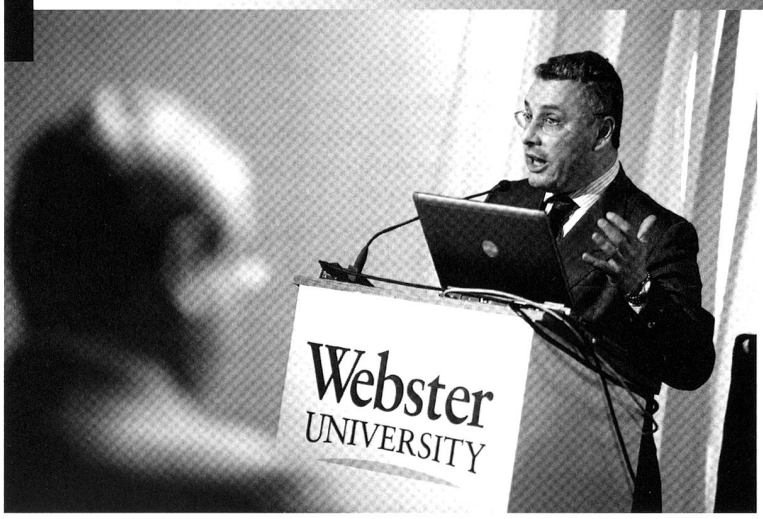
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2013)**

Heft 1

PDF erstellt am: **09.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-514769



L'auteur, au SECURITY FORUM 2013 organisé par l'Université Webster de Genève. Photo © Oliver O'Hanlon.

Cyber défense

Quels enjeux politiques en matière de cyberdéfense ?

Emmanuel Dupuy

Président de l'Institut Prospective et Sécurité en Europe (IPSE), chercheur associé au CEREM (Centre d'Etude et de Recherche de l'Ecole militaire)

Le concept de cyber-défense peut être perçu comme étant celui de la politique mise en place par l'Etat pour protéger les réseaux et systèmes d'information essentiels pour garantir la souveraineté nationale est plus large que celui de cyber-sécurité.

Ce dernier concept concerne plutôt la protection des réseaux des informations, celle des sites sensibles - dont ceux de la défense -, des infrastructures vitales (transports, énergie, hôpitaux) ou des systèmes bancaires.
Le chercheur français Daniel Ventre, Titulaire de la Chaire de Cyber-sécurité de l'Ecole militaire de Saint-Cyr, parle lui plus volontiers d'un « espace informationnel », mettant en exergue le fait qu'il ne s'agit que d'un des aspects dans lequel le numérique duplique voire remplace le scriptural (en terme de transmission des données, influence des idées et des sociétés).
Nombre d'analystes s'interrogent néanmoins afin de savoir s'il s'agit d'un nouvel espace à part, à côté de ce qu'il est convenu d'appeler les « *Global commons* » tel que mentionnés dans le concept stratégique de l'Alliance (mer, terre, air auquel il convient d'ajouter l'espace) ou, est-ce un espace « transversal » perméable aux trois précités ?
Dès lors, une attaque via l'informatique venant ou non d'un pays unique visant des objectifs privés (serveurs, sites d'entreprises, aéroports, banques...) constitue t'elle pour autant une attaque prouvée et délibérée d'un Etat contre un autre Etat ? Si avérée, cela appelle-t-il pour autant une réponse proportionnelle (comme l'Estonie l'avait sollicité alors qu'elle s'estimait attaquée par la Russie en 2007 en faisant explicitement référence à l'article 5 du Traité de Washington) ? Les mesures de rétorsion doivent-elles se limiter à des moyens cybernétiques, ou bien peut-on également envisager des frappes militaires conventionnelles ?
Questions pertinentes quand on sait qu'il s'agit de savoir qui est la tête pensante derrière les attaques portant la signature d'Hackers de nationalité chinoise ou russe ou encore ceux issus du réseau libertaire *Anonymous*.

L'émergence, par ailleurs, des réseaux sociaux dans les relations internationales est une réalité indéniable. L'on a pu ainsi parler « d'E-Democratie » (avec le phénomène de la diffusion savamment ciblée de plus de 250'000 télégrammes diplomatiques, en novembre 2010) ou encore de « Révolution 2.0 » à l'occasion du « Printemps arabe » : on a volontiers fait référence à l'occasion des révoltes en Tunisie ou en Egypte, de « révolution Facebook » ou de « diplomatie Twitter ». C'est indéniablement à cause d'internet, associé à d'autres moyens, comme les téléphones portables ou la télévision, qu'a été rendu possible cette résistance collective face aux régimes autoritaires dans la région.
On s'est aussi beaucoup interrogé sur la vulnérabilité des infrastructures critiques. En principe, tout est fait pour maintenir des cloisons étanches entre les systèmes les plus sensibles de ces installations et les réseaux ouverts sur l'extérieur.
Des attaques de ce type relèvent soit de groupes de *hackers* très professionnels au service de certains Etats, soit des Etats eux-mêmes, avec leurs propres capacités offensives. Dans le même temps, rien ne permet d'identifier l'origine de l'attaque, même s'il y a des soupçons. Car, c'est bien une des caractéristiques de ces cyber-menaces : l'impossibilité de remonter à la source et d'attribuer les attaques à un adversaire identifié !
Une attaque informatique ignore par nature les frontières. L'ancien ministre de la défense britannique, Pat Cox rappelait, à cet effet, qu'il n'y avait pas de « Ligne Maginot » dans le cyber-espace. Au-delà, face à la volatilité des risques et menaces, les réponses graduées nationales mettent en exergue le manque de coopération internationale. La France devrait ainsi développer ses propres capacités à lutter contre les attaques informatiques et renforcer sa coopération dans ce domaine, notamment avec d'autres pays européens et au sein de l'Otan, tout en veillant à garder sur ces questions des éléments de souveraineté, qui ne peuvent être totalement délégués.
Jusqu'à présent, les cyber-attaques n'ont généré que des nuisances assez limitées. Les vulnérabilités sont

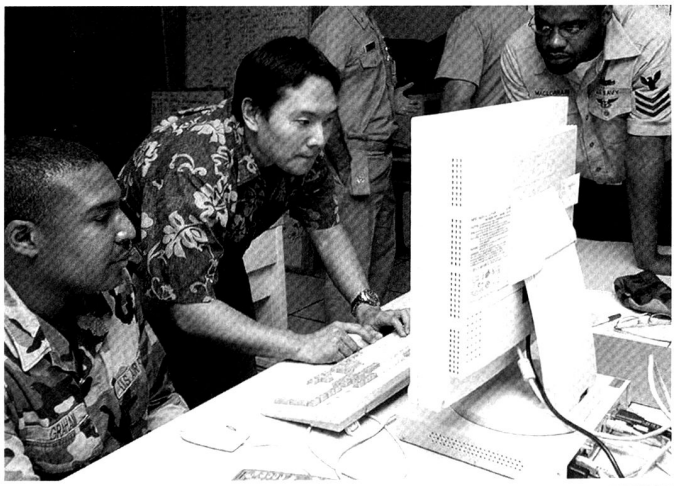
réelles et les savoir-faire se développent. On ne peut pas éviter de telles attaques, mais on peut certainement en limiter les effets en renforçant les mesures de protection et en prévoyant comment gérer la crise le temps du rétablissement des systèmes.

Les réponses varient cependant trop d'un Etat à l'autre :

En France, l'Agence nationale de sécurité des systèmes d'information (ANSSI) a été créée en juillet 2009. Son budget - de l'ordre de 90 millions d'euros pour 2012 - et ses personnels (250 agents aujourd'hui, 360 en 2013) restent à l'échelle européenne et mondiale nettement insuffisants ;

Aux Etats-Unis, le Président Barack Obama s'est fortement engagé sur le sujet et a qualifié la cyber-sécurité de priorité stratégique en nommant à la Maison blanche un conseiller spécial chargé de ce dossier. Il existe plusieurs organismes, au sein du département d'Etat de la défense et du département d'Etat chargé de la sécurité nationale, qui interviennent dans ce domaine, comme l'Agence de sécurité nationale ou encore le Cybercommand, inauguré en 2010 et qui est chargé, fort plus particulièrement de protéger les réseaux militaires américains. De 2010 à 2015, le gouvernement américain devrait consacrer 50 milliards de dollars à la cyber-défense ;

Au niveau de l'OTAN, le Centre d'Excellence de l'OTAN de Tallin (CCD-COE) existe depuis le Sommet de Riga (2004). Son renforcement a été à l'ordre du jour lors du Sommet de Lisbonne de novembre 2010, avec la perspective de doter l'Alliance d'une pleine capacité opérationnelle en matière cybernétique d'ici fin 2012 à travers l'élaboration d'une « politique de cyber-défense en profondeur ». Composé de 10 pays et de 30 personnes seulement (sans officier français jusqu'ici !) l'objectif est loin d'être atteint et ne le sera très certainement pas à temps...



L'Union européenne a aussi un grand rôle à jouer, car une grande partie des règles qui régissent les réseaux de communications électroniques relèvent de sa compétence. Elle peut donc agir pour l'harmonisation de certaines dispositions techniques au niveau européen qui sont importantes du point de vue de la cyber-défense.

Le propre des attaques informatiques est d'exploiter des failles, de se porter là où les parades n'ont pas encore été mises en place ; mais l'on peut renforcer la sécurité des réseaux et des infrastructures les plus sensibles, et améliorer leur résilience.

On peut aussi s'interroger sur la gouvernance de l'internet, ce réseau par lequel transitent ces attaques. Internet est un espace non régulé, dépourvu d'autorité centrale.

Peut-on ainsi imaginer, par exemple, de renforcer la traçabilité sur internet, et donc de restreindre l'anonymat derrière lequel s'abritent les agresseurs, en conciliant transparence et traçabilité ?

Enfin, beaucoup reste à faire pour sensibiliser le monde de l'entreprise. Faut-il aller plus loin et passer par la loi pour fixer un certain nombre de règles ou de principes ? Faut-il défnir une cyber-stratégie à la hauteur des menaces qui pèsent sur nos démocraties ?

Alors que le rapport parlementaire du Sénateur du Haut-Rhin, Jean-Marie Bockel, venait rappeler que la France demeurait potentiellement sous la menace d'une cyber attaque d'ampleur, le Président de la République, François Hollande, confirmait, le 14 juillet dernier, la mise en place effective de la Commission chargée de rédiger un nouveau Livre blanc sur la Défense et la sécurité nationale, quatre ans seulement après celui de 2008.

Il confirmait dans le même élan la « sanctuarisation » de la dissuasion nucléaire, transformant ainsi une promesse de campagne en décision essentielle afin de garantir notre sécurité et assurer le rang de la France dans le concert des Nations.

Sans remettre nullement en cause le coût de la dissuasion nucléaire - relativement raisonnable, eu égard aux 0,76 du PIB qu'elle consomme, il est désormais temps de considérer la protection des systèmes informatiques comme aussi vitale pour la sécurité des Français.

Comme les capacités militaires balistiques, savamment mis en place depuis les premiers essais au milieu des années 60, répondent au principe du « *Faible au Fou* » - confirmant son caractère défensif et le principe de sa stricte suffisance -, une cyber-dissuasion française impliquerait de renforcer les moyens techniques, humains, financiers - trop faible en comparaison avec les dispositifs et la sensibilité de nos alliés à cet enjeu majeur pour leur sécurité nationale : 90 millions d'euros mis à profit par l'Agence nationale des systèmes d'informations (ANSSI) alors qu'aux Etats Unis, la cyber sécurité est un objectif stratégique et que le CyberCommand dispose d'un budget de 50 milliards de dollars !

Une fois consolidée, cette stratégie défensive réglerait *de facto* les réflexions autour des capacités offensives. Là encore, la comparaison avec la dissuasion est pertinente :

viendrait-il, en effet, à l'esprit de quiconque de douter de la capacité potentiellement offensive de cette dernière, compte-tenu des vecteurs qui en assurent sa crédibilité ?
Disposer d'une stratégie interarmées, d'une mobilisation interministérielle, associant les opérateurs d'importance vitale et renforcée par la garantie de la résilience des usagers, de plus en plus conscients des enjeux dans ce secteur, reviendrait à confirmer - à qui en douterait - que la France dispose des moyens technologiques de répondre à toute attaque dans l'espace cybernétique d'où qu'elle vienne.
Gradualité et proportionnalité d'une éventuelle réponse et infaillibilité quant à la traçabilité des attaques sont ainsi les deux axes d'efforts en direction desquels il convient de s'engager.
Au-delà de la technologie, c'est aussi d'intelligence, dont la France et l'Europe ont aussi besoin, afin que le principe de dissuasion comprenne un nouveau pilier, cybernétique, qui loin de concurrencer la filière nucléaire pourrait suivre les mêmes voies qui en ont fait « l'assurance vie » de notre pays depuis le milieu des années 60.
Se joue aussi, par ailleurs, l'avenir de la dimension prospective que doit se donner l'UE vis-à-vis des nouveaux enjeux dans l'espace cybernétique. Ainsi, ce sont d'âpres discussions qui, actuellement en cours à Dubaï, où se tient du 3 au 14 décembre 2012, la Conférence mondiale des Télécommunications Internationales, mettent en exergue l'enjeu consistant à procéder à la modification du traité de l'Union Internationale des Télécommunications (UIT), en veillant au savant dosage entre régulation et liberté au sein du réseau internet.
L'Union européenne et ses 27 Etats membres semblent néanmoins jouer enfin de pair afin de ne pas sombrer aux sirènes des lobbies, qui cherchent à profiter de la manne financière des connexions à internet, notamment en cherchant à imposer le prélèvement de droits sur les bénéficiaires de ces connexions.
La cohérence de l'UE se mesure ainsi aussi à l'aune de cette position unitaire et commerciale juste et équitable.
En tout état de cause, assurer la sécurité des systèmes d'information des entreprises n'est pas seulement un enjeu technique, mais est aussi un enjeu économique, puisqu'il s'agit de protéger la chaîne de valeur, notre savoir-faire technologique dans la guerre économique que nous connaissons aujourd'hui, voire un enjeu politique, lorsque les intérêts de la nation sont en jeu.

E. D.

Compte rendu

Géopolitique du Mali

Aymeric Chauprade, géopolitologue français et ancien professeur au Collège interarmées de défense (CID), à l'invitation de la SMG, a présenté à Genève le jeudi 7 février, le Mali dans un contexte historique et géopolitique.
L'origine du Mali n'est pas un Etat-nation, mais une construction caractérisée par un lien national faible, marqué par la division entre une population noire et sédentaire, au Sud, et une population majoritairement nomade et arabe, notamment touareg, au Nord. L'histoire de ces peuples est marquée par la traite des esclaves, par lesquels les nordistes ont pris l'ascendant sur les Africains du sud, avant la période coloniale où l'influence occidentale s'est appuyée sur les anciens oprimés du Sud.

La situation actuelle du Mali s'explique par plusieurs séries de facteurs :
- la guerre en Lybie, qui a vu de nombreux combattants touaregs regagner le Mali, en armes, autour d'un mouvement nationaliste et indépendantiste, le MNLA ;
- les organisations islamistes, dont Ansar Dine et Al Qaeda au Maghreb islamique (AQMI) – à l'origine formés en Algérie à la suite des Groupes islamistes armés (GIA) et du Groupe salafiste pour la prédication et le combat (GSPC) ;
- les organisations criminelles, qui bénéficient de nombreux trafics, notamment les enlèvements : on estime que chaque enlèvement d'Européen rapporte en moyenne trois millions d'euro ;
- enfin, le gouvernement du Mali, faible comme nous l'avons vu plus haut, renversé par un coup d'Etat militaire au printemps 2012, suite à sa défaite face aux Touaregs ; et le régime putchiste lui-même a connu également l'humiliation face aux « djihadistes » passés à l'offensive ce printemps.

Alors que les Touaregs sont parvenus, courant 2010, à prendre l'ascendant et gagner leur autonomie face au gouvernement de Bamako, proclamant de fait la création d'un Etat baptisé l'Azawad, ceux-ci ont été bousculés par les groupes islamiques. L'intervention de la France s'explique donc par la volonté de protéger l'Etat malien contre un assaut et la prise du pouvoir par des groupes minoritaires - islamistes et djihadistes internationaux. N'oublions pas cependant que même si le nord du Mali représente la moitié de la superficie du pays, la population locale représente moins de 10% de la population totale.

L'intervenant a présenté ensuite la politique et l'intervention française, possible grâce au maintien de bases africaines – le porte-avions Charles de Gaulle étant en maintenance pour une période de six mois. Il conclut que les questions d'intérêts économiques sont clairement secondaires, en face des intérêts politiques en jeu au Sahel.

A+V