L'OTAN et la Cyberdéfense[1]

Olivier Kempf

Mai 2013, article n°III.6

Cyber : le mot est dans les bouches de tous les stratégistes car chacun observe que notre monde est de plus en plus dépendant non seulement des technologies de l'information et de la communication, mais surtout de leur réticulation généralisée. Il paraît logique, dès lors, de s'interroger sur les conséquences de ce nouvel environnement dans la conduite de la guerre, celle-ci étant considérée à la fois comme un art et une science.
L'Alliance Atlantique n'est pas la dernière à se poser ces questions, ce qu'illustre le concept qu'elle a adopté lors du sommet tenu à Lisbonne en novembre 2010. Un des grands messages fut l'importance donnée à la lutte contre les nouvelles menaces, et dans des nouveaux milieux. Ainsi, le milieu cyber fut régulièrement cité à l'appui de cette novation. Il paraît opportun de faire le point à la fois du dispositif mis en place, mais aussi de sa pertinence et sa portée.

1 - L'alliance s'intéresse au milieu cyber depuis les années 2000

Le concept précédent de 1999 ne mentionnait nulle part le cyberespace ou la sécurité des systèmes d'information. La première apparition dans un document d'importance se trouve dans la déclaration donnée par les dirigeants de l'alliance à l'issue du sommet de Prague, en 2002, où ceux-ci affirment avoir décidé de « *renforcer nos capacités de défense contre les cyberattaques* ». Cela fait suite aux premières cyberattaques d'activistes serbes, au moment du conflit du Kosovo. « *Le site web sur la guerre du Kosovo conçu par les Affaires publiques et qui devait, à l'aide de présentations et de dépêches, permettre à l'Alliance de présenter sa vision du conflit, fit l'objet d'attaques DDoS*[2] *qui le rendirent « pratiquement inutilisable pendant plusieurs jours ». Dans le même temps, le serveur de l'OTAN affecté au courrier électronique était submergé par un afflux de courriels*[3] ». En conséquence, un programme NCIRC (*NATO Computer Incident Response Capability* - la Capacité OTAN de réaction aux incidents informatiques) fut établi à Bruxelles et à Mons[4]. Bien que l'attaque informatique en elle-même n'eut alors aucun retentissement opérationnel (il s'agissait d'un « simple » site web), il n'était pas acceptable qu'une telle organisation fût handicapée dans sa capacité de communication. La NCIRC s'est donc occupée de la protection des propres systèmes d'information et de communication de l'OTAN. Elle « *joue un rôle clé, qui consiste à réagir à toute cyberattaque qui*

[1] Ce texte reprend et actualise un article éponyme, publié avec Arnaud Garrigues et paru au printemps 2012 dans Sécurité globale n° 19.
2 Déni de service distribué : attaque informatique impliquant de nombreuses machines perpétrée afin de rendre inaccessible une ressource.
3 SVERRE MYRLI, « L'OTAN et la cyberdéfense », Rapport de l'assemblée parlementaire de l'OTAN n° 173 DSCFC 09 F bis, 2009.
[4] Elle dépend de l'Agence OTAN d'information et de communication (NCIA) qui a succédé à l'Agence OTAN de services de systèmes d'information et de communication (NCSA). Voir son site web : http://www.ncirc.nato.int/index.htm .

pourrait être menée contre l'Alliance. Elle offre un moyen de traiter et de signaler les incidents et de communiquer les informations cruciales sur ceux-ci aux responsables de la gestion des systèmes et de la sécurité et aux utilisateurs. Par ailleurs, elle centralise et coordonne le traitement des incidents en un point unique, éliminant de ce fait toute répétition de tâches[5] ».

Le communiqué d'Istanbul en 2004 n'évoqua pas la question, mais celui de Riga en 2006 fut plus prolixe, puisque les Alliés affirment alors leur intention de « *s'employer à développer une capacité en réseau de l'OTAN pour partager les informations, les données et les éléments du renseignement d'une façon fiable et sûre, qui ne retarde pas les opérations de l'Alliance, tout en améliorant la protection de nos systèmes informatiques clés contre les cyberattaques* ». En fait, c'est l'attaque contre l'Estonie, en 2007, qui éveilla l'attention des dirigeants, d'autant que la république balte était désormais pleinement alliée. Jusqu'alors, l'OTAN pensait surtout à se protéger, en tant qu'organisation, et non à aider les Alliés quand ceux-ci faisaient eux-mêmes l'objet d'agression. Ainsi, le changement consistait à passer d'une problématique somme toute classique de sécurité des systèmes d'information (adaptée à un contexte militaire et allié) à une vision plus globale de « cyberdéfense ». La question posée est celle des aspects militaires et violents de telles pratiques, susceptibles ou non d'être qualifiés d'agression au sens du droit international et de la convention de l'ONU.

A la suite de l'expérience estonienne, les ministres de la défense réunis à Noordwijk en octobre 2007 favorisèrent l'adoption d'une « *politique de l'OTAN en matière de cyberdéfense* » (classifiée), qui fut approuvée quelques mois plus tard au sommet de Bucarest en avril 2008[6].

Dans leur déclaration du sommet de Bucarest, en 2008, les dirigeants montrent leur intérêt plus soutenu, puisque la menace cyber fait l'objet d'un article autonome, où le préfixe « cyber » est utilisé cinq fois : « *L'OTAN reste déterminée à renforcer la protection de ses systèmes informatiques clés contre les cyberattaques. Nous avons récemment adopté une politique sur la cyberdéfense, et nous définissons les structures et les autorités pour son application. Notre politique sur la cyberdéfense souligne la nécessité pour l'OTAN et pour les pays de protéger les systèmes d'information clés conformément à leurs responsabilités respectives, de mettre en commun les meilleures pratiques, et de mettre en place une capacité visant à aider, sur demande, les pays de l'Alliance à contrer les cyberattaques. Nous comptons bien poursuivre le développement des capacités de l'OTAN en matière de cyberdéfense et renforcer les liaisons entre l'OTAN et les autorités nationales* ».

De même, l'OTAN annonçait la mise en place d'une autorité de gestion de la cyberdéfense (la CDMA – *Cyber Defense Management Authority*)[7]. « *Cette autorité servirait de commandement central pour les activités techniques, politiques et de partage de l'information menées par les membres de l'Alliance, ainsi que diriger et gérer les entités de cyberdéfense de l'OTAN existantes. La CDMA devrait aussi, sur demande, être prête et apte à fournir ou à coordonner l'aide en réponse à d'éventuelles cyberattaques dirigées contre un ou plusieurs Alliés*[8] ». Parfois oublié, le Bureau des C3 (C3B) de l'ex-agence NC3A[9] (NATO Consultation, Command and Control Agency) fournit également une expertise technique dans les domaines des technologies de l'information et de la communication et a vu le volume de ses activités en matière de sécurité augmenter.

---

5 Site web de l'Alliance, http://www.nato.int/cps/fr/natolive/topics_49193.htm, accédé le 9 avril 2013.

6 « *La France a largement participé au processus de définition de la politique de cyberdéfense de l'OTAN* », in « Cyberdéfense : un nouvel enjeu de sécurité nationale », Rapport d'information n° 449 (2007-2008) de M. Roger ROMANI, fait au nom de la commission des affaires étrangères, déposé le 8 juillet 2008.

7 Nato sets up cyber defense management authority in Brussels, Computer weekly, 4 avril 2008 : http://www.computerweekly.com/Articles/2008/04/04/230143/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels.htm. "*The CDMA will co-ordinate responses to attacks if invited by national cyberdefence authorities. It will also develop and propose standards and procedures for national and Nato cyberdefence organisations to prevent, detect and deter attacks*"

8 Sverre Myrli, op. Cit.

9 La NC3A a été intégrée à la NCIA. http://www.ncia.nato.int/Pages/default.aspx

Le sommet de Strasbourg-Kehl est encore plus détaillé, puisque le préfixe cyber est utilisé huit fois dans la déclaration finale[10]. Chacun a bien vu que lors du conflit en Géorgie, à l'été 2008, des attaques contre Tbilissi avaient été lancées, et même si la Géorgie n'était qu'un partenaire, de plus faiblement informatisée à la différence de l'Estonie, cela confirmait l'importance de ces attaques en appui des conflits plus classiques[11].

L'affrontement de communautés hacktivistes est, depuis plusieurs années, un moyen quasi-classique de l'expression des revendications, notamment dans les zones de tension ou en conflits. Sur ce point précis, les attaques informatiques en Géorgie ne changent pas radicalement la donne, ne serait-ce que parce que la « cible » Internet ou les réseaux géorgiens ne représentent pas une cible stratégique cruciale. Toutefois, le cas géorgien semble montrer une réelle capacité de préparation puis de corrélation avec les actions militaires. Malgré le manque de preuve, commun dans le cas des attaques informatiques, il n'en demeure pas moins que ce sentiment d'une organisation poussée invite à analyser en profondeur les événements et à développer des scénarios d'actions et de réactions.
L'Alliance annonçait ainsi la constitution d'équipes de réaction rapides susceptibles d'être mises à la disposition des États-membres en cas d'attaque. Une demande d'envoi de ces équipes par des pays non membres devrait recevoir l'aval du Conseil de l'Atlantique Nord.

2 - Le sommet de Lisbonne et le cyberespace.

L'année 2010 a confirmé ces orientations. Tout d'abord, le commandement allié pour la transformation a évoqué le sujet dans le cadre de son étude « futurs multiples » (avril 2009) destinée à préparer la rédaction du nouveau concept stratégique. Il recommandait d'écrire un concept stratégique pour la cyberdéfense, d'améliorer les capacités techniques pour détecter, identifier, localiser et engager les origines des attaques cyber, de développer des capacités cyber offensives. Toujours en vue de préparer le concept, une conférence de haut niveau se tint à Tallinn en juin 2009. Enfin, le groupe d'expert, dirigé par Mme Albright, rendit un rapport préparatoire au concept qui appelait à se protéger contre les menaces non-conventionnelles[12.]

Le concept stratégique marqua l'importance qu'il accordait désormais au domaine, élevé au rang des premières priorités de l'alliance, en lui dédiant deux articles[13]. L'innovation tient au recours « *à la*

[10] Art. 49 : *Nous restons déterminés à renforcer la protection des systèmes d'information et de communication qui sont d'une importance essentielle pour l'Alliance contre les cyberattaques, car des acteurs étatiques et non étatiques pourraient tenter d'exploiter la dépendance croissante de l'Alliance et des Alliés à l'égard de ces systèmes. Afin de prévenir de telles attaques, et d'y répondre, nous avons établi une Autorité OTAN de gestion de la cyberdéfense, amélioré la capacité existante de réaction aux incidents informatiques et ouvert, en Estonie, le Centre d'excellence pour la cyberdéfense en coopération, conformément à la politique sur la cyberdéfense que nous avons adoptée. Nous entendons accélérer la mise en place de nos capacités de cyberdéfense pour parvenir à un état de préparation maximal. Il est prévu que la cyberdéfense soit pleinement prise en compte dans les exercices de l'OTAN. Nous poursuivons le renforcement des liaisons entre l'OTAN et les pays partenaires concernant la protection contre les cyberattaques. Dans cet esprit, nous avons établi un cadre de coopération en matière de cyberdéfense entre l'OTAN et les pays partenaires, et nous reconnaissons la nécessité de coopérer avec les organisations internationales, lorsqu'il y a lieu*.

[11] Voir Arnaud Garrigues, « Géorgie 2008 : le vrai visage de la cyberguerre ? » in St. Dossé et O. Kempf,Stratégies du cyberespace, Cahier AGS/ l'esprit du livre, juin 2011.

[12] « *L'OTAN doit accélérer ses efforts face au danger de cyberattaques, en protégeant ses propres systèmes de communication et de commandement, en aidant les Alliés à mieux pouvoir prévenir et se relever de telles attaques, et en mettant au point toute une gamme de moyens de cyberdéfense pour une détection et une dissuasion efficaces.* »

[13] Art 12 : *Les cyberattaques augmentent en fréquence, sont mieux organisées et causent des dommages plus coûteux aux administrations, aux entreprises, aux économies, voire aux réseaux de transport et d'approvisionnement ou autres infrastructures critiques ; elles risquent d'atteindre un seuil pouvant menacer la prospérité, la sécurité et la stabilité des États et de la zone euro atlantique. Des forces armées et services de renseignement étrangers, la criminalité organisée, des groupes terroristes et/ou extrémistes sont autant de sources d'attaque possibles.*

planification OTAN pour renforcer et coordonner les capacités nationales de cyberdéfense » qui suggère que la cyberdéfense relève de la planification de défense et éventuellement, des plans de défense [14].

Cette vision est somme toute logique puisque la « cyberdéfense » comprend un volet de protection ou de sécurité des systèmes d'information, démarche de long-terme et complexe mais ne relevant pas, de prime abord, d'une vision militaire des choses. Elle recouvre également un aspect très opérationnel, de réaction à des crises informatiques qui se poseraient à l'OTAN en tant qu'organisation : il convient donc d'avoir développé une capacité et préparé des plans et des scénarios de réaction. Enfin, elle inclut une dimension plus militaire correspondant aux missions de l'OTAN et qui pourrait être décrite comme la réaction aux attaques informatiques dont un membre allié est victime dans le cadre d'une agression.

De façon plus concrète, la déclaration des dirigeants[15], publiée à la fin du sommet, énonce les objectifs de court terme : accélérer l'évolution de la NCIRC, mettre en place une capacité centralisée de cyberprotection, rénover la politique de cyberdéfense.

Le sommet de Chicago confirmait cette attention donnée au cyber. Ainsi, l'article 49 de la déclaration des chefs d'Etat et de gouvernement, publiée le 20 mai 2012, affirmait : « *Le nombre de cyberattaques continue de s'accroître de manière significative et leur niveau de sophistication et de complexité ne cesse d'évoluer. Nous réaffirmons les engagements pris au sommet de Lisbonne en matière de cyberdéfense. Suite à ce sommet, nous avons adopté l'an dernier un concept, une politique et un plan d'action pour la cyberdéfense, dont la mise en œuvre est en cours. Sur la base des capacités existantes de l'OTAN, les éléments critiques de la capacité opérationnelle totale (FOC) de la capacité OTAN de réaction aux incidents informatiques (NCIRC), y compris la protection de la plupart des sites et des utilisateurs, seront en place d'ici la fin 2012. Nous nous sommes engagés à fournir les ressources et à mener à bien les réformes nécessaires pour mettre en place une capacité centralisée de cyberprotection pour tous les organismes de l'OTAN, de manière à garantir que les moyens que nous investissons collectivement dans l'OTAN sont protégés par des capacités de cyberdéfense renforcées. Nous allons continuer d'intégrer des mesures de cyberdéfense dans les structures et les procédures de l'Alliance et, à titre individuel, nous restons attachés à recenser et à mettre en place des capacités*

Art 19 : (…) *nous continuerons de développer notre capacité à prévenir et à détecter les cyberattaques, à nous en défendre et à nous en relever, y compris en recourant à la planification OTAN pour renforcer et coordonner les capacités nationales de cyberdéfense, en plaçant tous les organismes de l'OTAN sous une protection centralisée et en intégrant mieux les fonctions de veille, d'alerte et de réponse de l'OTAN avec celles des pays membres* ; (…)

[14] Voir le site de l'OTAN http://www.nato.int/cps/fr/natolive/topics_49193.htm : *L'OTAN utilisera aussi ses processus de planification de défense pour promouvoir le développement des capacités de cyberdéfense des Alliés, aider les Alliés qui en feraient la demande, et optimiser le partage de l'information, la collaboration et l'interopérabilité. Les Alliés s'emploieront aussi à soutenir l'élaboration de normes internationales de conduite dans le cyberespace.*

[15] Art 40 : *Les cybermenaces se multiplient rapidement et sont de plus en plus sophistiquées. Pour que l'OTAN puisse accéder au cyberespace en permanence et sans entrave, et afin de garantir l'intégrité de ses systèmes critiques, nous tiendrons compte de la dimension informatique des conflits modernes dans la doctrine de l'OTAN, et nous renforcerons la capacité de l'Alliance à détecter et à évaluer les cyberattaques dirigées contre des systèmes revêtant pour elle une importance critique, à les prévenir, à s'en défendre et à s'en relever. Nous nous efforcerons en particulier d'accélérer l'évolution de la capacité OTAN de réaction aux incidents informatiques (NCIRC) pour qu'elle atteigne sa capacité opérationnelle totale d'ici à 2012, ainsi que la mise en place d'une capacité centralisée de cyberprotection pour tous les organismes de l'OTAN. Nous utiliserons les processus de planification de défense de l'OTAN en vue de promouvoir le développement des capacités de cyberdéfense des Alliés, d'aider les Alliés qui en feraient la demande, et d'optimiser le partage de l'information, la collaboration et l'interopérabilité. Pour faire face aux risques de sécurité émanant du cyberespace, nous travaillerons en étroite collaboration avec d'autres acteurs, tels que l'ONU et l'UE, comme convenu. Nous avons chargé le Conseil d'élaborer, en s'inspirant notamment des structures internationales existantes et sur la base d'un réexamen de notre politique actuelle, une politique OTAN de cyberdéfense en profondeur d'ici juin 2011, et de préparer un plan d'action pour sa mise en œuvre.*

nationales de cyberdéfense qui renforcent la collaboration et l'interopérabilité au sein de l'Alliance, y compris dans le cadre des processus OTAN de planification de défense. Nous continuerons de développer notre capacité à prévenir et à détecter les cyberattaques, à nous en défendre et à nous en relever. Pour faire face aux menaces qui pèsent sur la cybersécurité et pour améliorer notre sécurité commune, nous sommes déterminés à travailler avec les pays partenaires concernés, au cas par cas, et avec des organisations internationales, entre autres l'UE, comme convenu, le Conseil de l'Europe, l'ONU et l'OSCE en vue d'accroître la coopération concrète. En outre, nous tirerons pleinement parti de l'expertise offerte par le Centre d'excellence pour la cyberdéfense en coopération en Estonie. »

D'autres actions marquaient l'intérêt allié pour le cyber : le secrétariat international de l'Alliance à Bruxelles se réorganisait en créant en août 2010 une nouvelle division, « *Défis de sécurité émergents*[16] » qui incluait notamment un bureau dédié aux cyberconflits. Enfin, le 10 mars 2011, les ministres de la Défense des pays de l'OTAN approuvèrent un nouveau document conceptuel sur la cyberdéfense[17]. Ils approuvaient une nouvelle politique OTAN de cyberdéfense[18] et un plan d'action à leur réunion de juin 2011 (le plan d'action a été approuvé par les ministres en octobre 2011). Comme l'explique la page web de l'Alliance[19], « *cette nouvelle version de la politique propose une approche coordonnée de la cyberdéfense dans l'ensemble de l'OTAN et met l'accent sur la prévention des cyberattaques et sur le développement de la résilience. Toutes les structures de l'OTAN seront placées sous un dispositif de protection centralisé, et de nouvelles règles seront appliquées en matière de cyberdéfense. La politique précise les mécanismes politiques et opérationnels de la réponse de l'Organisation aux cyberattaques, et elle intègre la cyberdéfense dans le processus de planification de défense de l'OTAN. Elle définit en outre les modalités selon lesquelles l'OTAN apportera aux Alliés qui en auront fait la demande une aide dans leurs initiatives de cyberdéfense, le but étant d'optimiser l'échange d'informations et la connaissance de la situation, ainsi que la collaboration et l'interopérabilité sécurisée à partir de normes OTAN agréées. Enfin, cette politique énonce les principes de la coopération, dans le domaine de la cyberdéfense, de l'OTAN avec les pays partenaires, les organisations internationales, le secteur privé et le monde universitaire*. »

De même, « *en février 2012, un marché d'une valeur de 58 millions d'euros a été attribué en vue de l'établissement d'une capacité OTAN de réaction aux incidents informatiques (NCIRC), qui devrait être pleinement opérationnelle d'ici fin 2012. Une Cellule de veille cybernétique, dont le rôle sera de renforcer le partage du renseignement et la connaissance de la situation, est également sur le point d'être mise en place*. »

Simultanément, dans un nouveau projet conceptuel, « Global Commons[20] », ACT dénombre quatre espaces lisses qui méritent l'action future de l'Alliance : mer, air, espace et cyber espace. Le SACT explique ainsi : « *Tout d'abord, nous ne prétendons pas que les « Global commons » soient le lieu où se dérouleront obligatoirement les conflits dans le futur. Mais ce sont des espaces où toute atteinte au libre accès a un impact considérable, non seulement sur la possibilité de mise en œuvre des moyens militaires mais aussi sur nos sociétés, leur sécurité et la prospérité économique mondiale. Or, aujourd'hui, ces espaces sont de plus en plus vulnérables. Aucune nation n'est à même d'y répondre seule à des menaces. Cette étude a contribué à mieux visualiser les défis du futur. Elle devrait se traduire à terme par une réflexion plus élaborée en matière de concepts d'emploi, de doctrines et de capacités*[21] ».

---

[16] Voir la présentation officielle : http://www.nato.int/cps/en/SID-ED0F7AEC-2EF6EC44/natolive/news_65107.htm .

[17] http://www.nato.int/cps/fr/SID-CC3D342A-5F1A90A5/natolive/news_71432.htm?selectedLocale=fr

[18] Voir OTAN, « la politique de cyberdéfense en un coup d'œil », *site de l'OTAN*, septembre 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence-fr.pdf

[19] Voir http://www.nato.int/cps/fr/SID-C4621EB1-D3267419/natolive/topics_78170.htm

[20] http://www.act.nato.int/activities/seminars-symposia/the-global-commons

[21] Pour une discussion de cette notion de Global Commons, voir O. Kempf, « *Introduction à la cyberstratégie* », Economica, 2012.

3 L'action de l'Alliance

L'action de l'Alliance s'organise aujourd'hui selon quatre domaines : coordination des travaux (CDMA), aide aux alliés (équipes de réaction rapide), recherche et formation et coopération avec les partenaires

Coordination des travaux

Le Conseil de l'Atlantique nord supervise les actions de cyberdéfense au niveau politique, et ile demeure le principal niveau de décision politique en cas de crise liée à la cyberdéfense. Il est assisté par le Comité de la politique et des plans de défense. Au niveau opérationnel, le Bureau de gestion de la cyberdéfense (CDMB) est chargé de la coordination des activités de cyberdéfense dans l'ensemble des organismes civils et militaires de l'OTAN. Il est placé au sein de la division des défis de sécurité émergents, au Secrétariat International. Pour les aspects techniques, il consulte le bureau des C3 (C3B). L'expression des besoins est assurée par les autorités militaires (État-major international, SHAPE et SACT) et la NCIA.

Cette dernière, grâce au NCIRC, fournit les services techniques et opérationnels assurant la cybersécurité de l'organisation. « *Le premier niveau de la NCIRC est le Centre de coordination de la NCIRC, situé au siège de l'OTAN et composé de personnels du NHQC3S. Le Centre de coordination de la NCIRC est un élément d'état-major responsable de la coordination des activités de cyberdéfense menées au sein de l'OTAN et avec les pays, du soutien administratif du CDMB, de la planification de l'exercice annuel Cyber Coalition, et de la liaison dans le domaine de la cyberdéfense avec les organisations internationales telles que l'UE, l'OSCE et l'ONU/UIT. La Cellule d'évaluation de la cybermenace (CTAC) est également colocalisée avec le Centre de coordination de la NCIRC*[22] ».

Aide aux alliés

Des mécanismes ont été mis au point : sur demande d'un pays allié, l'Otan enverra des équipes de réaction rapide (RRT). En effet, les alliés restent responsables de leur sécurité, et l'Alliance ne saurait assurer leur cyberdéfense et notamment la sécurité de leurs systèmes informatiques. Toutefois, « *l'OTAN (…) s'emploiera donc, avec le concours des autorités nationales, à définir les principes et les critères garantissant un niveau minimum de cyberdéfense aux points d'interconnexion entre les réseaux des pays et ceux de l'OTAN* ».

Recherche et formation

Pour la partie recherche, la NCIA est en charge de la maîtrise d'œuvre de projets techniques. Ses représentants proposent ainsi des projets très intéressants[23] en matière de sécurité des systèmes d'information. Ainsi, « *Le projet CIAP (Consolidated Information Assurance Picture) vise à pallier ce manque en étudiant comment toute l'information nécessaire à la cyber-défense peut être consolidée dans un système complet, reposant sur un modèle de donnée commun s'appuyant sur des standards et sur un système de stockage distribué. CIAP fournit également diverses visualisations complémentaires de toutes les données collectées, notamment des vues d'ensemble de la topologie réseau et des vues géographiques* ».

Le projet DRA (Dynamic Risk Assessment), quant à lui, est une « *étude complémentaire de CIAP qui vise à fournir une analyse de risque en temps réel, afin de déterminer automatiquement l'impact réel dû à la situation sécurité globale du système et du réseau. Pour cela une nouvelle méthodologie innovante a été développée en combinant un générateur automatique d'arbres d'attaque (attack trees/graphs) et un moteur d'analyse de risque « traditionnel » similaire à EBIOS*[24] ».

---

[22] Voir http://www.nato.int/cps/fr/SID-C4621EB1-D3267419/natolive/topics_78170.htm

23 Voir Philippe Lagadec, « Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense », in http://www.sstic.org/2010/presentation/CyberDefense/ (accédé le 28 mai 2011): Présentation des projets SSI du NC3A en matière notamment d'analyse de risque dynamique pour la cyber-défense.

[24] Ph. Lagadec, op. Cit.

Ces projets témoignent ainsi d'un certain dynamisme technique au sein de l'organisation et d'une évolution bienvenue dans le développement et l'acquisition des capacités de communication et d'information sécurisées ainsi que des capacités spécifiques en matière de sécurité des systèmes d'informations militaires.

Pour la formation, c'est le Centre d'excellence pour la cyberdéfense en coopération (CCDCOE[25]) de Tallinn (Estonie), qui est responsable de ce dernier domaine.

Si le projet date de 2004 et fut alors proposé par l'Estonie à l'Alliance (avant donc les événements de 2007), la capacité opérationnelle initiale du centre est atteinte en 2006 et il est officiellement homologué comme « centre d'excellence de l'OTAN » en 2008. Il compte un effectif de 30 personnes, composé notamment de spécialistes venant des pays contributeurs. En effet, les centres d'excellence n'appartiennent pas à la structure intégrée proprement dite, et sont financés par les seuls pays participants, même s'ils ont une homologation alliée et qu'ils remplissent une fonction partagée. Ainsi, onze pays participent aujourd'hui au Centre de Tallinn : Estonie, Lettonie, Lituanie, Allemagne, Hongrie, Italie, Slovaquie, Espagne, Pays-Bas, Pologne, Etats-Unis. La France et le Royaume-Uni ont annoncé leur participation à compter de l'été 2013.

Il organise son activité autour des quatre domaines suivants : aspects juridiques et politiques, concepts et stratégie, environnement tactique, protection des infrastructures d'information critique.
En 2010 et 2011, il a mené des activités dans les domaines suivants : exercices de cyberdéfense (série « *cybercoalition* », mais aussi « *Baltic cyber shield* » en mai 2010, en collaboration avec les Suédois, *Locked shields* en avril 2013), des cours sur les généralités juridiques et politiques, des cours techniques (solution de surveillance cyber, migration de botnet, attaque et défense des systèmes IT), et des conférences (une conférence annuelle, CyCon multidisciplinaire, réunissant professionnels et chercheurs, avec 300 participants : la prochaine conférence se tiendra en juin 2013 et examinera les conséquences techniques, tactiques et légales de l'utilisation de méthodes automatiques pour gérer des cyberconflits).

Enfin un groupe d'experts a proposé un manuel sur le droit international applicable aux conflits cyber[26], et qui a été publié au début de 2013. Il a été dirigé pendant trois ans, par le Professeur Michael Schmitt de l'US Naval War College. Il se compose de deux parties, la première concerne la sécurité du cyberespace en droit international, quand la seconde traite du droit international des conflits cybernétiques. Ainsi, l'objectif principal du Manuel est d'interpréter les normes de droit international aux conflits cyber. Les experts ont réussi à se mettre d'accord sur 95 règles de droit, assorties de commentaires détaillés. Les experts ont trouvé un consensus sur la qualification d'emploi de la force, a qualification d'agression armée, et l'attaque cyber qui est définie comme une opération cybernétique, offensive ou défensive dont on peut raisonnablement attendre qu'elle cause des pertes en vies humaines, des blessures aux personnes, des dommages ou des destructions de biens. En revanche, ils n'ont pu se mettre d'accord sur l'évaluation du seuil de l'agression armée, la notion de légitime défense et les notions de groupes armés organisés et de participation directe aux hostilités[27].
Ainsi, l'apport du centre de Tallinn ne porte pas sur la partie technique des conflits cyber, mais plutôt sur la partie juridique et politique : quels sont les critères (théoriques et pratiques) qui permettent de déterminer qu'une action cyber relève de la catégorie du conflit ?

[25] Voir http://www.ccdcoe.org/
[26] MILCW : *Manual on International Law Applicable to Armed Conflicts in Cyberspace*.
[27] Voir Oriane Barat-Ginies, « Commentaires sur le manuel de Tallinn », *Egéa*, 12 décembre 2012 (http://www.egeablog.net/dotclear/index.php?post/2012/12/11/Le-Manuel-de-Tallinn-%3A)

Aide aux partenaires

Cette dernière mission n'apparaissait pas initialement dans les objectifs de l'Alliance. Elle a été rajoutée après l'adoption de la nouvelle politique de l'Otan. Cette coopération sera menée « à la carte ». L'Otan n'hésitera pas à faire appel pour cela à des partenaires privés et à des universitaires.

Conclusion

Il reste que la guerre de Géorgie l'a, d'une certaine manière, illustré : les conflits de demain comporteront nécessairement une part « cyber » dont la forme exacte n'est pas encore certaine et qui pourrait être source d'une certaine surprise. Là est probablement la légitimité de l'OTAN, dans la gestion de cette partie d'un conflit qui engagerait le reste de l'Alliance. Mais elle ne saurait être légitime pour conduire un conflit qui se réduirait au seul milieu cyber : tout d'abord parce qu'il est extrêmement difficile, aujourd'hui, d'isoler le cyber de son environnement. En fait la guerre de demain aura des aspects cyber, mais elle ne pourra pas être une cyberguerre.

Cette distinction explique la place ambiguë de l'Alliance en ce domaine : la guerre sera moins simple au 21ème siècle qu'en 1949, lorsque l'Alliance fut fondée. Au fond, l'Alliance hésite encore sur sa position stratégique : doit-elle adopter le modèle américain de cyber-dissuasion ? Celui-ci est-il adapté au cadre atlantique ? Ou ne faut-il pas se concentrer tout d'abord sur l'élévation du niveau de protection avant de s'intéresser aux possibilités de riposte[28] ?

[28] Sur cette question, voir V. Joubert, « Five years after Estonia's cyber attacks : lessons learned for NATO ? », *NDC Research Paper*, NDC, may 2012.