Table ronde

Guerre froide sur le net

Jeudi 25 novembre 2010 – Amphithéâtre Des Vallières

Cybercapacités, cyberrésilience, cyberwarfare : quelles réalités ?

Guillaume TISSER
Directeur du Pôle « Risques opérationnels », CEIS

Avant d'entrer dans l'analyse des menaces proprement dites, il me semblait intéressant de commencer en soulignant que le contexte cyber avait profondément changé ces dernières années et qu'on était entré, qu'on le veuille ou non, dans une période d'instabilité croissante pour plusieurs raisons :

- La première c'est qu'internet a changé de dimension, on l'oublie un peu souvent : il y a aujourd'hui 1,7 milliard d'internautes, avec un périmètre géographique qui change considérablement (l'essor du 3G, le fait que des pays qui n'avaient pas jusqu'à présent les infrastructures physiques nécessaires commencent à accéder à internet, modifient la donne)
- La deuxième chose, et c'est une résultante, c'est que le centre de gravité d'internet a changé : 15% des internautes sont américains aujourd'hui, 50% en 1998, donc on voit que le centre de gravité s'est déplacé, notamment vers la Chine qui compte aujourd'hui plus d'internautes que les USA. En terme de trafic c'est la même chose, on a aujourd'hui simplement 25% du trafic mondial qui passe par les USA, c'était 70% il y a dix ans ;
- Troisième facteur d'instabilité, c'est le fait que le la prédominance américaine s'érode, on le voit bien à travers ces chiffre, mais elle s'érode aussi en termes de gouvernance, en termes d'infrastructures ;
- Et quatrième facteur enfin, à la fois d'ailleurs cause et conséquence de cette instabilité, c'est le fait qu'internet, qui était depuis sa création essentiellement un espace marchand géré par des techniciens, fait l'objet d'une sorte de réappropriation progressive par le politique et par les Etats. Avec d'une part, le fait que chaque affrontement politique ou militaire a un prolongement ou se transpose dans le cyberespace, ce qui participe évidemment à cette instabilité et induit du même coup un risque de militarisation du cyberespace, risque qui est souvent relevé, et de l'autre évidemment pour faire face à cette menace, les Etats entendent réaffirmer

leur souveraineté dans cet espace et mettre en place une nouvelle régulation, une nouvelle gouvernance.

Je ne vais pas revenir sur les différents niveaux d'affrontement que l'on a dans le cyberespace (cybercriminalité, cyber-hacktivisme, cyber-espionnage, cyber-terrorisme ou guerre informatique), mon propos sera juste de souligner que le terme « guerre » est souvent utilisé de façon impropre, parce que le terme « guerre », au sens juridique du terme, induit évidemment l'existence d'un conflit armé. Or même si les attaques informatiques actuelles peuvent mettre en cause la souveraineté d'un Etat, on n'est pas dans le cadre d'un conflit armé tant que le seuil qui caractérise l'usage de la force n'est pas atteint.
Or en droit international, le franchissement de ce seuil suppose des attaques répétées, un niveau de sophistication relativement élevé, des destructions de biens matériels et des pertes en vie humaines, et l'attribution de l'attaque à un Etat ou à une organisation agissant sous contrôle. Donc aucune des attaques constatées n'a réuni pour le moment ces conditions. On est donc dans une sorte d'affrontement de basse intensité qui reste en dessous du seuil d'usage de la force en droit international.
Ceci étant posé, il ne faut pas cependant complètement écarter l'hypothèse d'une guerre informatique, ne serait-ce que parce que ces différents types de menaces ne sont pas étanches : le cybercriminel peut être recruté, au plan technique ce sont souvent les mêmes outils qui sont utilisés pour des attaques avec un objectif cupide et pour des attaques qui ont un objectif plus politique et par ailleurs, des attaques en apparence bénignes peuvent avoir des effets très graves et surtout irréversibles au plans matériel et humain.

Je vous propose maintenant de regarder rapidement quelles sont les postures adoptées par certains Etats, à commencer par les USA.
On le dit souvent, la cybersécurité est devenue aux USA une priorité nationale. On parle maintenant d'arme de perturbation massive, après les armes de destruction massive. Cette posture américaine peut se résumer en trois principes clés :

- La résilience, le fait que les attaques constituent la situation normale, qu'il faut donc que les systèmes et les réseaux encaissent en permanence les attaques. C'est quand même une évolution considérable par rapport aux postures précédentes où on cherchait plutôt à empêcher les attaques grâce à une sécurité péri-métrique et à une capacité de détection et de protection
- L'attribution, la possibilité de tracer l'origine d'une attaque
- Le développement d'une capacité informatique offensive officielle avec un objectif très clair, qui est d'assurer la suprématie américaine dans le domaine du cyber espace, considéré aujourd'hui comme le cinquième espace de bataille. Avec une caractéristique, c'est qu'il est transverse à l'ensemble des espaces, d'où d'ailleurs les nombreuses luttes de pouvoirs que le *Cyber Command* a pu générer.

Sur ces derniers points, on voit très bien que la vision américaine de la guerre informatique est quelque peu fantasmée, vision qui est d'ailleurs sans doute un peu entretenue par les grands industriels américains dans le domaine de la défense et de la sécurité. L'affrontement informatique est finalement perçu comme un conflit ouvert, assez comparable à un conflit classique, avec des règles assez similaires, mettant en prise des

forces constituées, avec tous les problèmes éthiques, juridiques, organisationnels ou opérationnels que cela pose.
On est également dans une perspective d'affrontement relativement symétrique, notamment avec la Chine et la Russie alors que des conflits asymétriques paraissent souvent plus probables, d'où d'ailleurs l'importance des moyens qui sont alloués à l'ensemble des programmes aux USA qui portent le vocable cyber.
Troisième point important également, c'est le fait que la doctrine aujourd'hui reste largement basé sur le principe de dissuasion, principe dont on sait qu'il ne fonctionne pas, ou peu, ou différemment en tout cas, en matière informatique. Tout simplement parce que dans le cadre d'une perspective asymétrique l'attaquant ne possède pas ou peu de vulnérabilités, donc on ne peut pas le menacer de quelque chose qu'il ne craint pas, et deuxièmement, pour qu'il craigne quelque chose, il faut encore qu'il soit sûr d'être identifié, or on connaît les difficultés d'attribution dans cet espace.
Evidement cette posture, cette vision quelques peu fantasmée a ses limites, qui sont d'ailleurs de plus en plus critiquées en interne. Elle a néanmoins le mérite de poser un certains nombre de questions, et souvent les bonnes questions ; peut être pas, au début en tout cas, d'apporter les bonnes réponses mais en tout cas de lancer le débat.

Quelques mots sur la vision russe, qui tranche singulièrement avec cette vision américaine puisqu'on a aujourd'hui une absence de doctrine officielle coté russe, mais une vision beaucoup plus pragmatique.
Une vision qui est basée d'une part sur le fait qu'on considère l'affrontement informatique comme un conflit de basse intensité, permettant d'intervenir de façon relativement *soft* dans sa zone d'intervention traditionnelle, on l'a vu en Géorgie et en Estonie, sans que sa responsabilité ne puisse être directement mise en cause.
Deuxièmement, avant d'être une guerre informatique, le conflit informatique est d'abord un conflit informationnel. D'où, par exemple, le fait que le pays cherche à protéger un écosystème cybercriminel ou hacktiviste qui s'est manifesté dans un certain nombre d'attaques. Il est évidemment toujours difficile de parler du lien qui unit ces mouvements hacktivistes et les officiels russes, néanmoins le rôle des organisations de jeunesse patriotique peuvent être pointées du doigt, ce sont des gens qui souvent contribuent à fédérer en quelque sorte la jeunesse russe.
Cette position reflète en fait la prise de conscience de la Russie de son retard au plan numérique par rapport aux USA et à la Chine et l'affaiblissement évidemment de son potentiel militaire en matière d'information et de communication.
A cet égard il est très intéressant d'observer qu'il y a un affrontement qui oppose les russes et les américains sur le sujet de la gouvernance internet. Vous avez d'un coté les russes qui réclament aujourd'hui un traité de désarmement sur le cyberespace, or il est toujours délicat de distinguer l'offensif d'un coté et le défensif de l'autre, alors qu'on a souvent des technologies et des outils duaux. Evidemment, derrière cette demande, ce sont les américains et leur *Cyber Command* qui sont visés. Des discussions ont été ouvertes, mais bien sûr les Etats-Unis refusent et réclament de leur coté l'extension de la coopération internationale sur le sujet, ce que refusent évidemment les russes qui souhaitent protéger leur écosystème cybercriminel.

Si on regarde maintenant la Chine, là aussi on voit que l'on n'a pas de doctrine officielle, et une vision également très réaliste et pragmatique de la guerre informatique.

Le cyberespace peut clairement être utilisé dans le cadre d'une guerre hors limites, une guerre totale. On retrouve même la notion de guerre du peuple, notion chère à Mao Tse-Tung, qui trouve là une nouvelle application, via l'implication directe de citoyens dans le cadre d'un conflit, via l'implication directe de mouvements hacktivistes qui sont également très présents en Chine.
Le concept de *cyberwar* s'intègre parfaitement dans le concept chinois de guerre asymétrique et dans la notion de *soft power*. Alors toute la question au plan stratégique consiste à savoir si l'avantage stratégique qui nait de la relative dissymétrie de la Chine par rapport aux Etats-Unis au plan numérique va durer très longtemps. Aujourd'hui, compte tenu de l'essor de l'internet et des réseaux en Chine, on n'est pas encore dans une situation de symétrie parfaite, mais on y tend, et donc cet avantage va disparaitre progressivement.
Ce qui est certain, c'est que côté chinois, on voit bien que les autorités ont maintenant une approche très pratique d'internet, qui est vraiment utilisé comme un outil de contrôle de la population. Il y a eu une période de méfiance, de lutte, de censure au début. On est toujours dans une optique de contrôle des débats, mais on est aussi dans une optique d'exploitation d'internet pour maintenir le contrôle sur la population.
On est aussi sur l'idée qu'internet est indispensable au développement du pays, et on voit très bien que l'érosion de la domination américaine dont je parlais est notamment due à l'essor très important des industriels chinois en matière de télécommunications et d'informatique. On disait pendant longtemps que les industriels copiaient et se contentaient de mettre sur le marché des produits copiés. On voit aujourd'hui des industriels qui dépassent leurs concurrents américains en termes de dépôts de brevets. Cela montre bien que les industriels aujourd'hui rivalisent très nettement avec les grands équipementiers, de type SISCO par exemple.
Cette volonté d'autonomie on la retrouve aussi en matière de gouvernance internet. On se souvient notamment que la Chine a mis en place un DNS à deux niveaux, DNS qui permet en théorie à l'internet chinois de fonctionner de façon relativement autonome et qui permettra aussi sans doute à terme de limiter considérablement l'anonymat sur l'internet chinois, autre conséquence intéressante.

En conclusion, je crois qu'il est évidemment d'aborder ce sujet avec beaucoup de modestie puisque les évolutions sont très rapides et on ne sait pas de quoi demain sera fait.
Il faut bien voir qu'on est plutôt en présence d'un nouveau type d'affrontement plutôt qu'en présence d'une nouvelle arme.
Un nouveau type d'affrontement avec des caractéristiques vraiment propres :

- Le haut niveau d'anonymat qu'il permet, avec le problème d'attribution et le problème de riposte ;
- Des effets directs et indirects difficiles à évaluer ;
- Des outils et technologies qui ont un usage dual ;
- On est en présence d'une confusion des niveaux, niveaux des conflits informationnels, c'est-à-dire le niveau *pour* l'information, *par* l'information et *contre* l'information (renseignement, guerre psychologique et guerre informatique) ;
- L'arme informatique a un rayon d'effets qui est potentiellement important ;
- Le conflit informatique a une temporalité tout à fait différente, les effets peuvent se prononcer avec beaucoup de retard, plusieurs mois après ;
- C'est ensuite un univers dans lequel nous n'avons pas de domination absolue possible et qui est forcément partagé, donc conflictuel par nature ;

- C’est un monde qui est non prédictif puisque c’est une construction humaine et par conséquence une attaque qui est lancée à un moment donné à un endroit donné peut avoir une conséquence à l’autre bout du monde sans contrôle possible de la part de l’attaquant.

Merci de votre attention.