

De l'importance stratégique du cyberspace

VINCENT JOUBERT

Chercheur à l'Observatoire de géopolitique

Chaire Raoul-Dandurand en études stratégiques et diplomatiques

Au mois d'octobre, déclaré « National Cyber Security Awareness Month » par la Maison-Blanche depuis l'année dernière, le domaine du cyberspace a bénéficié d'une attention accrue ; les États-Unis ont mené un exercice de simulation d'attaque de grande envergure de leurs réseaux en collaboration avec douze pays alliés¹, le Canada vient de rendre publique sa stratégie nationale de cybersécurité², l'Inde, à l'instar de la Russie, de la Chine ou de la Corée du nord, a récemment décidé de publier son propre système d'exploitation pour garantir une plus grande sécurité et une plus grande souveraineté sur ses réseaux, et le Royaume-Uni a réduit son budget de la défense... sauf pour la cybersécurité³! Cet enthousiasme général révèle l'importance que les gouvernements et les États accordent à ce domaine et soulève plusieurs questions ; s'agit-il là d'une simple vogue ou le cyberspace représente-t-il un domaine stratégique majeur ? Allons-nous assister à une cyberguerre, un cyberArmageddon comme l'ont avancé certains experts ?

Une brève analyse des applications du cyberspace dans la sphère du militaire comme du civil permettra de distinguer les véritables enjeux inhérents à ce domaine des mythes et fantasmes scénaristiques.

1. La perspective militaire

Les nouvelles technologies ont été au cœur de l'évolution des armées modernes, et leur rôle a été accentué par le concept de « Revolution in Military Affairs » mis en place par l'armée américaine (1991-2001). Depuis lors, les champs de bataille se sont vus découpés et analysés comme autant de systèmes dans lesquels les points faibles de l'ennemi étaient détruits par des armes de haute technologie. Les technologies de l'information (TI) ont permis aux armées de penser la guerre d'une manière nouvelle, en agissant rapidement, à distance, avec une précision « chirurgicale », et en limitant au maximum le nombre de victimes dans leurs rangs. Les concepts de guerre réseau-centrée (Network Centric Warfare, 1991) et de « guerre de l'information » (Information Warfare, 1991) ont alors pris l'ascendant sur les stratégies plus classiques. En effet, les TI ont permis aux états-majors de disposer de manière quasi instantanée des informations nécessaires à la décision opérationnelle et de diffuser leurs

¹ L'exercice « Cyber Storm III », dirigé par le Department of Homeland Security, a eu lieu au cours du mois de septembre dernier ; voir sa description sur <http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf>

² Pour une description complète, voir : <http://www.securitepublique.gc.ca/prg/em/cbr/ccss-scc-fra.aspx>

³ <http://www.telegraph.co.uk/news/newstoppers/politics/defence/8074574/Defence-review-security-services-to-receive-extra-funds-for-terror-attacks.html>

ordres tout aussi instantanément au sein des différentes unités sur le terrain. La disponibilité de l'information a profondément changé la vision militaire au point que les réseaux des TI sont aujourd'hui une composante majeure des arsenaux militaires.

L'ensemble des nouveaux concepts stratégiques et opérationnels élaborés à partir des technologies de l'information sont applicables grâce au cyberspace. L'information devient l'élément clé et son acheminement se révèle décisif dans les conflits. Les armées modernes l'ont bien compris et cherchent à développer leurs capacités dans le domaine, notamment par l'élaboration de véhicules automatisés. Toutefois, la volonté de régler les conflits par la technologie a montré ses limites. Bien que l'opération « Tempête du Désert » (Irak, 1991), la première du genre réseau-centrée, fut un succès pour l'armée américaine, le conflit des Balkans a vite révélé les lacunes des technologies de pointes⁴ et la nécessité d'avoir des troupes sur le terrain pour mettre fin aux attaques. Les guerres d'Irak et d'Afghanistan ont renforcé le scepticisme lorsque l'armée américaine est revenue à des stratégies de contre-insurrection traditionnelles pour enrayer la violence au sein de ces pays. Ces différents échecs de la guerre réseau-centrée ont rappelé aux nations que l'Homme est une composante essentielle de la guerre ; la volonté de déshumaniser les combats pour limiter au maximum les pertes militaires s'est heurtée à la réalité des conflits. Même si les TI et la guerre réseau-centrée se révèlent inefficaces dans certains cas de figure, on ne peut cependant nier le rôle majeur qu'elles ont eu sur le développement des arsenaux et sur les possibilités qu'elles ont créées pour les armées. De plus, le cyberspace est indispensable aux stratégies d'infoguerre ou de guerres psychologiques qui sont des éléments centraux des guerres modernes et des stratégies diplomatiques de type « *soft power* »⁵.

Dans ces conditions, le cyberspace s'impose comme une composante incontournable des arsenaux et des États-majors qui a considérablement bouleversé la sphère militaire au cours des cinquante dernières années.

2. L'appropriation par le civil

Les TI, développés à leur début pour un usage militaire, ont rapidement trouvé une utilisation commerciale très lucrative. Aussi, la société actuelle est entièrement dépendante de ces technologies car elles composent et commandent les secteurs vitaux des États : économie, commerce, santé, communication, industrie, énergie, et nous l'avons vu, la défense. Les réseaux et les technologies de communication et d'information se sont développées de manière considérable et permettent l'échange de quantité astronomique de données. Ces données sont autant d'informations capitales pour les institutions publiques, les entreprises et les particuliers. Elles sont stockées dans des serveurs qui ne disposent pas toujours des meilleurs systèmes de protection et deviennent alors des cibles faciles pour des personnes ou des groupes malintentionnés. En effet, toutes les données qui transitent via le cyberspace ont une valeur pécuniaire plus ou moins importante, et leur protection devient alors un enjeu stratégique pour les États.

Le constat est là ; les intrusions malveillantes dans les systèmes d'exploitation connaissent la même croissance que le développement du cyberspace. Au fur et à mesure que le domaine se développe, sa sécurité décroît, et ceci pour des raisons très simples : la complexité intrinsèque

⁴ Barthélémy Courmont et Darko Ribnikar, *Les guerres asymétriques ; Conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces*, 2^e éd., 2009, pp.131-162.

⁵ Sur le rôle du cyberspace dans la stratégie de *soft power*, voir : Joseph S. Nye, *Cyber power*, Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

du cyberspace fait qu'aucune autorité ne peut le contrôler ni le maîtriser, l'identification des auteurs d'intrusions est extrêmement difficile, il n'existe aucun moyen de sanctions face à ces attaques dû au vide juridique dans le domaine, et enfin les principaux acteurs du cyberspace sont majoritairement étrangers aux règles les plus basiques de sécurité dans le domaine. Ces attaques mettent en péril l'activité de nombreuses entreprises et le bon fonctionnement d'institutions publiques. Conscients de cette situation, les gouvernements et les professionnels de la sécurité informatique commencent à mettre en place des politiques d'éducation aux principes de bases de sécurité dans le cyberspace pour créer un domaine plus sûr. Ces politiques sont longues à mettre en place car elles nécessitent d'expliquer les enjeux économiques et juridiques qui découlent d'une conduite prudente dans le cyberspace.

A l'instar de la sphère militaire, la sphère civile a été profondément bouleversée par le TI et le cyberspace. Totalement dépendante des réseaux d'information et de communication, les sociétés sont vulnérables aux attaques perpétrées dans le cyberspace et perdent des sommes colossales en information chaque jour. C'est cette réalité que les États tentent aujourd'hui de faire comprendre et de combattre.

3. Réalité stratégique

La valeur stratégique du cyberspace est une réalité incontestable ; il est indispensable au fonctionnement des États développés mais le manque de protection des réseaux est une menace directe pour l'économie et la sécurité des États. Si la cybersécurité doit être une préoccupation majeure des États, la perspective d'une cyberguerre se heurte à trop de facteurs aléatoires pour devenir le conflit type de demain⁶. Ainsi, les prédictions apocalyptiques de certains journalistes ou professionnels de la sécurité informatique se heurtent aux faits. Les excès sémantiques peuvent s'expliquer par les intérêts commerciaux qu'ils pourraient avoir à créer un climat de peur et d'insécurité dans le cyberspace, mais sont dangereux ; ils créent la confusion, la panique, et détournent les autorités publiques des vrais enjeux stratégiques qui existent dans le cyberspace. La protection des réseaux des secteurs vitaux d'une société et des données échangées constitue la priorité stratégique ; elle passera par des solutions juridiques, diplomatiques et technologiques qui établiront les règles à respecter dans ce domaine.



Chaire Raoul-Dandurand
en études stratégiques et diplomatiques
Raoul Dandurand Chair
of Strategic and Diplomatic Studies

⁶ La difficulté de définir avec certitude la source d'une attaque ; les attaques peuvent venir d'éléments isolés qui agissent seuls ; le vide juridique qui permet une large interprétation de la proportion d'une réponse face à une cyberattaque ; les pertes humaines directement causées par une cyberattaque sont pour l'instant inexistantes, donc peu intéressantes pour un conflit ouvert.