Fiche de lecture: "Crisis and Escalation in Cyberspace" (Martin Libicki. RAND Corp., 2012)

Vincent Joubert

Mai 2013, Article n°III.7

Objectif de l'étude

L'objectif général de l'étude était d'étudier les manières dont l'US Air Force pouvait intégrer les opérations cinétiques et non-cinétiques (c'est-à-dire cyber) dans ses missions. L'étude s'est concentrée sur la gestion de l'escalade de la violence dans le cyberespace, notamment sur les options possibles et leurs risques ; l'étude se divise en 6 chapitres :

- Le premier introduit la notion de crise dans le cyberespace, identifie les problématiques en émanant (par exemple, déterminer ce qui constitue une crise dans le cyberespace ou en identifier les prémices, déterminer l'influence de la perception des acteurs dans l'escalade de la violence dans une cybercrise, etc.), ainsi que la méthodologie de l'étude.
- Le deuxième chapitre traite de la possibilité d'introduire des normes internationales de « bonne conduite » dans le cyberespace, normes qui se concentreraient sur une gestion au jour le jour des attaques sur les systèmes d'information (SI) et promouvraient la confiance mutuelle à l'international comme base de stabilité.
- Le troisième chapitre s'intéresse à la « narration », aux dialogues, et aux signaux d'une crise dans le cyberespace. L'auteur développe ici une méthode semblable au « storytelling[1] », utile voire impérative selon lui pour désengrener une crise.
- Le quatrième chapitre analyse la gestion de l'escalade de la violence dans le cyberespace à proprement parler ; l'auteur montre qu'il sera quasiment toujours question d'éviter un conflit dans les domaines physiques (puisque les conséquences restent pour l'instant encore plus importantes que celles d'un cyber-conflit), mais que la gestion de crise d'un cyber-conflit devient logiquement prioritaire si les affrontements ne sortent pas du cyberespace.
- Le cinquième chapitre utilise les observations du chapitre 4 pour évoquer la stabilité stratégique dans le cyberespace. L'étude arrive à la conclusion qu'une cyber-crise a plus de chances d'éclater à cause de la peur exagérée des États de ne pas pouvoir faire face aux conséquences de cyberattaques lancées contre leurs réseaux et SI, plutôt qu'en raison des spécificités techniques intrinsèques au cyberespace.
- Le sixième et dernier chapitre pose des questions et apporte des réponses concernant la possibilité de gérer une crise dans le cyberespace pour l'US Air Force.

[1] Voir l'ouvrage de C. Salmon, « Storytelling, la machine à fabriquer des histoires et à formater les esprits », Ed. La Découverte, 2007.

Chapitre 1 : Introduction

Une crise dans le cyberespace peut provenir de la perception d'un État A vis-à-vis des activités d'un autre État B : si A décide que B doit changer son comportement, faire face aux conséquences de ses actes, ou que les normes actuelles ne sont plus tolérables, A peut déclencher une crise impliquant B.
Une crise dans le cyberespace a le plus de chance d'être le résultat d'une méfiance mutuelle ou manque de confiance réciproque (*mutual mistrust*) entre États. L'opacité entourant les opérations dans le cyberespace renforce largement ce sentiment. Aussi, l'absence de précédent de crises ou de conflits dans le cyberespace ne permet pas d'anticiper les réactions de l'adversaire et pousse les États à envisager les pires scénarios, ce qui en retour constitue un terreau favorable à l'éclosion d'une crise (l'auteur appuie son argument sur la base d'exemples historiques).

Chapitre 2 : les normes

L'étude propose quelques normes pouvant aider à prévenir ou limiter le développement de crises dans le cyberespace (sanctions juridiques des activités de *hacking*, se désolidariser des *hackers*, ou décourager le cyber-espionnage à but commercial). Pointant le problème de l'application de ces normes, l'auteur évoque alors l'instauration de mesures de confiance mutuelle ainsi que de normes de procédures à suivre pour les victimes des cyberattaques.
Les premières poussent à la coopération et la collaboration (pour le cas de démarches judiciaires), et les secondes incitent à adopter une posture mesurée et ne pas tirer de conclusions hâtives (pour ne pas déclencher de crise inutile).
Enfin, le chapitre se termine sur une étude des normes en cas de guerre ; reprenant les travaux de M. Schmitt sur l'applicabilité du droit de la guerre dans le cyberespace, M. Libicki dénonce le manque d'options que ces normes impliquent (ce n'est plus de la gestion de crise mais un affrontement militaire).
Pour l'auteur, des normes établies en temps de paix visant à renforcer la confiance mutuelle entre les États peuvent permettre de réduire le risque de crise dans le cyberespace. Cependant, elles ne sont en rien une panacée et n'empêcheront pas les crises d'éventuellement éclater.

Chapitre 3 : l'utilité du storytelling, du dialogue, et des signaux

Plus que pour toute autre forme d'affrontement, les conflits dans le cyberespace ont besoin de communication. Cela s'explique par l'invisibilité des attaques et de leurs conséquences. Pour l'auteur, l'objectif d'une cyberattaque n'étant pas de désarmer l'adversaire mais de lui envoyer un message, il faut donc que ce message soit parfaitement compris. Ainsi, selon lui, le storytelling aide à dissiper toute mauvaise interprétation ; il permet de connaître la représentation que se font les décideurs de la crise (avec notamment la définition du cadre narratif pour expliquer une crise dans le cyberespace). Il offre la possibilité de façonner sa position dans une cyber-crise (comme victime d'une agression, comme accusateur d'un adversaire, comme moyen de justifier ses représailles, ou comme agresseur), et surtout de justifier celle-ci.
Le storytelling est souvent initiateur d'un dialogue entre protagonistes, dialogue qui reposera sur la narration de l'autre ; le dialogue peut permettre de désamorcer une crise en expliquant son innocence/sa bonne foi (« nous n'avons rien fait », « ce n'étaient pas sous nos ordres », « c'est un accident », « tout le monde le fait », « au moins, ça ne présage rien d'inquiétant »). Développant chaque position possible, l'auteur examine dans les détails leurs avantages/risques/limites respectifs.
Les signaux ont une utilité très limitée dans la gestion d'une cyber-crise ; en effet, la marge d'erreur d'interprétation du signal est bien plus grande que dans un dialogue/la narration, et cette ambigüité est accrue par la complexité du cyberespace.

Chapitre 4 : gérer l'escalade de la violence

Pour M. Libicki, l'escalade de la violence est très périlleuse dans le cyberespace. Si elle est généralement utilisée pour tenter de gagner un avantage stratégique sur son adversaire ou tester sa réaction, l'absence de « lignes-rouges » ou seuils identifiés et identifiables dans le cyberespace peut très vite faire perdre le contrôle de la situation aux protagonistes.
Les principaux risques conduisant à une escalade de la violence lors d'une cyber-crise sont les suivants : (1) la différence entre les effets initialement recherchés (l'intention initiale) et les effets réels d'une action ; (2) la différence entre les effets réels et leur interprétation par l'État ciblé, qui deviennent alors les « effets perçus » ; (3) la différence entre les effets initialement recherchés de la réponse de l'État ciblé et leurs effets réels ; (4) la différence entre les effets réels de la réponse et la perception de ces effets par l'État ciblé. Pour l'auteur, le problème central réside donc dans l'écart existant entre les intentions initiales, les effets produits, et l'interprétation par la cible. Identifiant des situations illustrant son propos (dans le cas d'un conflit imminent entre deux États, d'un conflit local ou celui d'un conflit étendu par exemple), l'auteur explique comment ces deux problèmes (absences de lignes-rouges et imprévisibilité des conséquences) peuvent mener à une escalade de la violence.
L'auteur se penche ensuite sur le rôle d'un État tiers dans le déclenchement de l'escalade de la violence, et analyse les possibilités de gestion d'une telle situation.

Il explique ensuite l'inapplicabilité d'une stratégie « *tit-for-tat*[2] » dans le cyberespace, en soulevant d'abord ce qu'elle implique : la planification (reconnaissance des réseaux adverses et de leurs vulnérabilités exploitables), le problème de l'écart entre intentions/effets/interprétations qui empêche le succès d'une telle stratégie, ou encore l'escalade involontaire due à l'absence de lignes-rouges. Il entreprend alors d'envisager le débordement d'une cyber-crise en guerre cinétique ou en conflit économique, analysant les implications, les conséquences de chaque situation possible.
L'étude revient après cela à l'analyse de stratégies d'escalade de la violence permettant d'éviter une surenchère. La « *sub-rosa escalation*[3] », bien qu'attrayante, ne paraît pas si simple à mettre en place ; l' « *intrawar deterrence*[4] », elle, se heurte au problème de l'interprétation, limitant aussi son succès éventuel.
Enfin, il est rappelé la condition primordiale pour éviter une escalade involontaire de la violence : la maîtrise par les décideurs politiques et les commandeurs de leurs C2 (dans leur rôle, leurs pouvoirs, et leurs devoirs).

Chapitre 5 : Implications pour la stabilité stratégique

Après avoir expliqué le concept et ses origines (Guerre Froide), l'auteur envisage les possibles perturbations par une cyber-crise. Il affirme que tant que les armes nucléaires existent, elles resteront le gage ultime de cette stabilité et que le cyberespace vient après.
Il examine alors les possibilités offertes par le cyberespace pour contrebalancer cet avantage stratégique : levier pour une application de la force coercitive d'un État, empêcher l'utilisation des capacités nucléaires, désarmer entièrement les capacités cyber d'un adversaire. Il explique ensuite que l'application de concepts développés pour les conflits nucléaires dans le cyberespace (le « alert-reactions cycle ») est inutile puisqu'inefficace ; l'auteur insiste alors sur les conséquences d'une course à l'armement dans le cyberespace et de ses effets plus que limités sur la stabilité stratégique de l'environnement international. Il en conclut que la course aux cyber-armements n'est pas facteur de

[2] Une stratégie « tit-for-tat » signifie une rétorsion ou des représailles équivalentes ; on pourrait ainsi la traduire par une stratégie « œil-pour-œil ».
[3] Traduction littérale « escalade de la violence secrète ou confidentielle » ; une telle stratégie implique que l'escalade n'est visible que pour certains protagonistes choisis, mais n'est pas publique. On envoie alors un message ciblé.
[4] Traduction littérale « dissuasion à l'intérieur du conflit » ; une telle stratégie cherche à limiter l'étendue, l'intensité, et la fréquence des représailles d'un adversaire déjà engagé dans un processus d'escalade de la violence. En d'autres termes, il s'agit de dissuader un adversaire de franchir un palier qui n'aurait pas encore été franchi.

déstabilisation et que même un traité international limitant l'acquisition de « cyber-armes » ne serait pas un facteur ni un gage de stabilité.
L'auteur conclut ce chapitre en démontrant que l'utilisation de cyberattaques en soutien d'une attaque physique a de fortes chances d'être facteur de déstabilisation stratégique, et que les facteurs principaux de déstabilisation sont les facteurs subjectifs : « *Les incertitudes quant au comportement permis, la mauvaise interprétation de la préparation de mesures défensives, les erreurs d'attribution, la croyance infondée que l'adversaire ne peut pas attribuer des attaques, ou encore une mauvaise interprétation des normes de neutralité sont autant de sources potentielles d'instabilité qui peuvent conduire à une crise dans le cyberespace.*[5] »

Chapitre 6 : Les crises dans le cyberespace peuvent-elle être gérées ?

L'auteur s'adresse ici directement à l'USAF, mais son propos général est parfaitement résumé dans ce court paragraphe (placé en introduction de l'étude) :
« *Le message en substance est simple : l'escalade de la violence et les crises dans le cyberespace peuvent être maîtrisées si les décideurs politiques comprennent les différences majeures qui existent entre les affrontements dans/par le cyberespace et les affrontements dans les domaines physiques. Parmi ces différences, on retrouve les nombreuses possibilités stratégiques et politiques offertes par le champ de la cyberdéfense ; la quasi impossibilité et donc l'inutilité d'essayer de désarmer un adversaire dans le cyberespace ; l'ambigüité des opérations dans le cyberespace, notamment l'écart important pouvant exister entre l'intention initiale de l'attaquant, les effets réels de son action, et la perception des effets de l'action par la cible. Ainsi, les stratégies étatiques devraient se concentrer sur (1) la reconnaissance que l'instabilité d'une crise dans le cyberspace provient largement d'erreurs de perceptions, (2) la promulgation de normes qui permettraient de modérer les réactions des protagonistes lors de crises, (3) le désamorçage politique de crises involontaires résultant d'incidents, (4) l'emploi de la narration plutôt que de signaux pour expliquer les actions, (5) la mise en place d'un niveau de défense tel qu'un attaquant potentiel serait convaincu qu'une attaque (hors cyberespionnage) ne modifierait pas la balance des forces en présence, et (6) une utilisation rationnelle d'opérations offensive dans le cyberespace en fonction de leur potentiel d'escalade de la violence.*[6] »

Observations générales

Les concepts clés de cette etude sont donc:

- L'instabilité née de l'absence de lignes-rouges identifiées et identifiables.
- L'écart existant entre l'intention initiale, les effets réels, et l'interprétation d'une action dans le cyberespace par l'adversaire.
- L'utilité de la narration pour faciliter l'interprétation des messages et/ou actions.
- La connaissance préalable du fonctionnement des systèmes d'informations et de l'architecture des réseaux est nécessaire pour ne pas se hâter dans les représailles disproportionnées et mieux concentrer ses efforts de cyberdéfense.
- L'utilité limitée de normes pour diminuer la crainte mutuelle et réduire le risque de crise dans le cyberespace.

Cette étude de M. Libicki vient ainsi compléter son monographe « Cyberdeterrence and Cyberwar » publié en 2009 par la RAND Corp., en ce sens que l'auteur analyse ici les limites d'une autre analogie

[5] « *Uncertainties about allowable behavior, misunderstanding defensive preparations, errors in attribution, unwarranted confidence in the other side's inability to attribute, and misunderstanding the norms of neutrality are all potentially sources of instability leading to crisis.* », p. 135.
[6] Notre traduction, p. iii.

appliquée au cyberespace, à savoir l'escalade de la violence dans une crise ou un conflit dans/par le cyberespace.

Si l'ensemble peut sembler parfois un peu confus tant M. Libicki passe d'une hypothèse à une autre, d'un scénario à un autre, tout en faisant des renvois historiques, il faut reconnaître que l'auteur couvre ainsi une très grande majorité des scénarios possibles et de leurs conséquences.

L'étude étant volontairement axée sur des enjeux et des problématiques politiques et stratégiques[7], les questions techniques sous-jacentes sont vulgarisées et rapidement expliquées ; on peut par exemple regretter que l'auteur n'ait pas approfondi la question de l'intégration de solutions de réponses automatisées dans la gestion de l'escalade de la violence dans le cyberespace, question qui cristallise aujourd'hui beaucoup d'intérêt aux États-Unis et qui pourrait avoir des conséquences politiques et stratégiques importantes.

Outre ce bémol, on retrouve dans cette étude des éléments de discours qui sont révélateurs du débat stratégique qui a lieu en ce moment aux États-Unis concernant la militarisation du cyberespace. La militarisation est entendue comme l'excès d'une approche militaire à des fins de sécurité dans le cyberespace. En substance, les chercheurs dénonçant la militarisation du cyberespace postulent que cette approche n'est pas la solution la plus adaptée ni la plus efficace pour la majorité des risques et menaces dans le cyberespace, et que cette approche militaro-centrée empêche les décideurs politique d'envisager d'autres solutions, non-militaires, qui seraient plus adaptées. Cette position peut sembler étonnante étant donnés les commanditaires et bénéficiaires de cette étude (l'US Air Force), mais n'est pas incohérente avec le cœur du message de l'auteur : une approche trop militaro-centrée peut être un facteur supplémentaire de risque d'escalade de la violence involontaire dans une cyber-crise.

L'intérêt de cette étude réside ainsi dans l'analyse prospective de la gestion des conséquences politiques et stratégiques d'une escalade de la violence dans une cyber-crise. L'auteur ne tombant pas dans l'utilisation de scénarios catastrophe comme le font beaucoup d'experts américains ces derniers temps, l'étude garde un certain intérêt, mais reste toutefois lésée par l'absence d'approfondissements techniques.

Quelques lectures de référence :

- Libicki M., *Cyberdeterrence and cyberwar*, RAND Corp., 2009.
- Libicki M., *Chinese Use of Cyberwar as an Anti-access Strategy: Two Scenarios*, RAND Corp., 2011.
- Libicki M., *Cyberspace Is Not a Warfighting Domain*, RAND Corp., 2012.
- Lin Herbert, *Escalation Dynamics and Conflict Termination in Cyberspace*, SSQ 2012 (automne).
- Manzo V., *Deterrence and Escalation in Cross-Domain Operations:Where do Space and Cyberspace Fit?*, Strategic Forum (NDU), December 2011.
- Lewis J., "Ready Player One", in *Foreign Policy*, 12 oct. 2012.
- Dunn Cavelty M., *The Militarisation of Cyberspace: Why Less May Be Better?*, 2012 International Conference on Cyber Conflict Proceedings, CCD CoE, 2012.

[7] L'étude rentre en effet dans le cadre du programme RAND Project Air Force, dont le but est de fournir aux dirigeants de l'Air Force des analyses indépendantes sur des politiques alternatives pouvant avoir un impact (positif ou négatif) sur les capacités de combat de l'Air Force.

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

La chaire remercie ses partenaires