Conflit russo-géorgien et guerre de l'information

Autor(en): **Ventre, Daniel**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **174 (2008)**

Heft 12

PDF erstellt am: **27.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-71514

Conflit russo-géorgien et guerre de l'information

La Russie et la Géorgie se sont affrontées au cours d'une guerre éclair qui éclata le 8 août 2008. Comme dans toute guerre, l'information a joué un rôle central: déclarations, propagande, utilisation des médias visant l'opinion nationale et internationale.

Daniel Ventre

Mais il semblerait que le conflit ait également gagné l'espace informationnel, se propageant dans le cyberespace. Qui a pu organiser de telles opérations? L'impact sur le conflit a-t-il pu être significatif?

Opérations dans les cyberespaces russe et géorgien

A compter du 8 août 2008, date que par simplification nous retiendrons comme celle du début des hostilités militaires, de nombreux sites internet géorgiens ont été paralysés, leurs serveurs soumis à des attaques de type DDoS (Distributed Denial of Service), ou bien défigurés, leurs pages modifiées par des hackers.

Parmi les sites géorgiens touchés on compte ainsi celui du Président Mikhail Saakashvili[1], celui du ministère des Affaires étrangères[2], du Parlement[3], du Ministère de la Défense[4], de la banque nationale de Géorgie[5], du site rustavi2.com, de sosgeorgia.org (qui fait depuis défiler sur son site un bandeau pour informer les internautes qu'il fait l'objet d'attaques massives de la part des hackers russes), etc.

Les défigurations ont essentiellement consisté à remplacer les pages officielles par des photomontages associant l'image du président géorgien à celles de Hitler.

La Géorgie ne fut cependant pas seule touchée par ces opérations de hacking de sites: ont ainsi été piratés le site d'information skandaly.ru, le site de l'agence de presse russe RIA-Novosti[6], le site stopgeorgia.ru[7] dénonçant les opérations de guerre de l'information menées par la Géorgie et qui fut paralysé entre le 14 et le 18 août, des sites d'information d'Ossétie du Sud (osinform.ru et osradio.ru) dont les pages furent remplacées le 12 août par celles de l'agence d'information géorgienne Alania TV[8], le site du gouvernement d'Abkhazie[9], etc. Les ISPs géorgiens auraient également procédé au filtrage de l'internet pour bloquer les sites russes, en guise de mesure défensive, dans la logique de l'Etat d'urgence décrété par le gouvernement.

Le Ministère des Affaires étrangères géorgien affirme sur son blog de substitution[10] qu'«une campagne de cyber-guerre organisée par la Russie perturbe sérieusement de nombreux sites géorgiens, dont celui du Ministère des Affaires étrangères». Le site du président polonais indique également que «parallèlement à l'agression militaire, la Fédération de Russie bloque les portails internet géorgiens».

C'est sur la base de ces quelques informations et déclarations qu'aussitôt partout dans le monde, la presse, les sites internet, forums, blogs, croyant voir là les prémisses d'un conflit révolutionnaire dans sa forme, ont repris et développé à satiété cette idée de cyber-guerre, de guerre de l'information livrée sans merci entre les belligérants.

Tableau chronologique: quelques attaques recensées

Date	Victime	Fait marquant
20 juillet	Géorgie	Attaque DDoS du serveur hébergeant le site du président géorgien
8 août	Abkhazie	Hacking du site du gouvernement d'Abkhazie en exil
9 août	Géorgie	Défiguration du site du ministère des affaires étrangères géorgien
10 août	Russie	Hacking du site skandaly.ru
11 août	Russie	Serveur de l'agence russe RIA Novosti attaqué
12 août	Ossétie du Sud	Hacking des sites ossètes osinform.ru et osradio.ru. Les pages sont remplacées par celles de l'agence géorgienne Alania TV.
14 au 18 août	Russie	Attaque du site stopgeorgia.ru (qui avait été créé le 9 août)

Quelques commentaires sur ces «cyber-attaques»

Les atteintes aux systèmes (systèmes de télécommunication, réseaux, internet …) qui permettent de délivrer de l'information officielle sont intervenues au plus mauvais moment pour la Géorgie, au plus fort de l'engagement. Elles ont d'autre part touché les sites les plus symboliques: on touche au pouvoir quand on attaque le site d'un Président, d'un Parlement, d'un Ministère, d'une Banque nationale, et on touche à la liberté d'expression, voire aux relais du pouvoir, quand on attaque les sites de certains medias. Priver un Etat de ces ressources, c'est limiter ses capacités de communication, l'isoler, lui interdire de voir et d'être vu. Mais tel ne fut pas tout à fait le cas. La Géorgie a trouvé des relais, des alliés, des solutions, son internet n'a pas été coupé du reste du monde.

Des solutions de remplacement ont rapidement été trouvées: pour faire face à ces agressions, le gouvernement géorgien a déplacé ses pages d'information sur un blog aux Etats-Unis. Le site du ministère des affaires étrangères est temporairement

hébergé sur un blog de Google[11]. L'hébergeur américain Tulip System, petite entreprise dont la PDG, Nino Doijashvili, est une géorgienne expatriée, déclara: «nous avons accepté d'héberger le site du Président parce que des hackers russes ont paralysé tout l'internet géorgien»[12].

Le Président polonais, Lech Kaczynski[13] a également accepté de mettre à disposition son propre site internet pour la dissémination de l'information du gouvernement géorgien. Rappelons que le président Kaczynski avait été l'un des acteurs de la libération de la Pologne du joug soviétique: cet hébergement doit être perçu comme une expression, parmi d'autres, de la solidarité de la Pologne à l'égard de la Géorgie. Leur combat est similaire: celui de la liberté, de la démocratie, mais aussi celui de David contre Goliath.

Ce ne sont toutefois pas quelques paralysies de serveurs et de sites, pour officiels qu'ils soient, qui décident d'une victoire ou d'une défaite. Ces atteintes auraient toutefois plutôt joué en faveur de la Géorgie sur la scène internationale, y renforçant son image de victime, contribuant à faire passer son message: celui d'une petite démocratie menacée, attaquée, qui en appelle à l'aide du monde libre.

Les atteintes aux systèmes d'information ont probablement eu un impact très limité sur les capacités de la Géorgie. Pour que de tels actes puissent avoir un impact sur un acteur quelconque, il faut que celui-ci soit très fortement dépendant de ses systèmes d'information. Or les infrastructures réseaux-télécommunications de la Géorgie ne sont pas parmi les plus développées, les infrastructures nationales ne sont pas encore aussi connectées qu'elles le sont dans les pays industrialisés les plus avancés, la population est peu connectée. Tous les indices et classements internationaux mesurant le degré de développement des nations en matière de réseaux, télécommunications, internet, placent la Géorgie parmi les plus mauvais élèves du monde. L'impact d'une atteinte aux systèmes d'information sur le fonctionnement de la Géorgie est donc moins immédiat et profond qu'il ne le serait dans le cas d'une attaque contre un pays très connecté.

Précisons également que les atteintes aux systèmes d'information géorgiens et russes, ne se sont pas concentrées sur la seule période du conflit. Les affrontements dans l'espace informationnel, au-delà du seul cyberespace, ne sont pas

Capture d'écran publiée sur le site Zataz le 12 août 2008, http://www.zataz.com.

ponctuels, limités au seul temps de guerre. Les attaques dans le domaine de l'information, au sens de «news», font l'objet de querelles depuis plusieurs années entre l'Ossétie du Sud et la Géorgie. Un article publié sur le site www.Civil.ge le 14 janvier 2006 titrait «S. Ossetia calls Tbilisi to Stop 'Information War'»[14], dénonçant les campagnes d'information visant à dénigrer le président de l'Ossétie du Sud. Au cours des semaines précédant le conflit, le site du président géorgien avait déjà été pris pour cible. Le fait n'est pas nouveau: on recense des actions similaires (attaques DDoS, défigurations) depuis plusieurs années, dans tous les pays de la région comme partout dans le monde, là où se développent les crises et les conflits: entre la Chine et les Etats-Unis, le Japon et la Chine, la Russie et la Tchétchénie, la Malaisie et l'Indonésie, Israël et la Palestine, etc. Récemment 300 sites ont été défigurés en Lithuanie (1° juillet 2008) suite à l'adoption d'une loi interdisant l'affichage public de symboles datant de l'ère soviétique et de jouer l'hymne national soviétique. En avril 2008 des groupes diffusant de la propagande pro-Kosovo ont défiguré des sites albanais, et diffusé des listes de sites internet albanais à prendre pour cibles. En 2007 ce sont les systèmes d'information estoniens qui ont été pris pour cibles, sur fond de crise entre les communautés russes et estoniennes du pays, puis de crise entre l'Estonie et la Russie, manifestant les tensions entre la Russie et l'OTAN. L'affaire estonienne est devenue une affaire politique internationale. Un an après les faits cependant le seul «coupable» qui soit réellement identifié est un hacker, géorgien d'origine russe. L'affaire estonienne appelle donc à la prudence: les accusations portées contre le gouvernement russe ont été levées par l'Estonie. Ainsi, bien que les atteintes aux systèmes d'information géorgiens et russes s'inscrivent dans le cadre d'un conflit, l'identité des auteurs (coupables) des actes reste toujours difficile à avancer avec certitude. Les serveurs impliqués se trouvent en Russie, mais aussi en Turquie, aux Etats-Unis. Outre les militaires, les gouvernements, les services de renseignement, on peut raisonnablement penser que des hackers mus par un sentiment patriotique (hacktivistes) se soient impliqués. Qui est le fameux «South Ossetia Hack Crew» qui revendique la défiguration du site du Parlement géorgien mais dont personne n'a jamais entendu parler? Doit-on parler d'actions russes ou pro-russes? Les actions sont-elles l'œuvre de groupes organisés, manipulés, ou de quelques individus isolés? Le crime organisé est-il impliqué – certains avancent que le réseau cybercriminel RBN serait un acteur du cyberconflit?

Le conflit a-t-il été le théâtre d'une guerre de l'information?

Né aux Etats-Unis à la fin des années 1980 le concept a fait son apparition sur la scène internationale avec la première guerre du Golfe, démontrant alors l'importance de la maîtrise de l'espace informationnel dans un conflit moderne dominé par les nouvelles technologies.

La guerre de l'information est définie comme l'utilisation agressive/défensive des composantes de l'espace informationnel (information, systèmes d'information), pour atteindre/protéger les intérêts souverains d'un Etat en temps de paix, de crise ou de conflit. Ce concept englobe ainsi toutes les formes d'utilisation, à des fins agressives et défensives, des technologies de l'information et de la communication, qui peuvent être à la fois les armes et les cibles des agressions: guerre de commandement et de contrôle, ISR, guerre électronique, Psyops, attaques par réseaux d'ordinateurs.

Les opérations de guerre de l'information peuvent être réalisées, selon qu'elles sont menées par des acteurs militaires ou civils, par un éventail impressionnant d'acteurs aux potentiels les plus disparates: Etats, militaires, groupes structurés

(terrorisme, dissidence, activisme…), individus isolés, simples «pirates» informatiques. Leurs motivations peuvent être multiples: politiques, économiques, idéologiques…

Le conflit russo-géorgien a très probablement offert aux belligérants un champ d'utilisation de leurs capacités de guerre de l'information. Mais l'absence d'information en provenance des opérations militaires russes et géorgiennes interdit toute conclusion définitive et toute analyse plus méthodique. Rien ne permet d'affirmer que les attaques contre les systèmes d'information géorgiens ont été une action coordonnée par les militaires russes en vue de couper les systèmes de communication du pays et faciliter la progression des opérations militaires. Ces quelques temporaires défigurations de sites et saturations de serveurs, auxquelles des solutions de remplacement rapides ont été trouvées (sites miroirs, hébergements des pages dans des pays alliés…) ne résument quoi qu'il en soit pas à elles seules le concept de guerre de l'information.

Quelles premières conclusions tirer?

Sans doute est-il trop tôt aujourd'hui pour reconstruire le scénario de ce qui s'est réellement passé dans l'espace informationnel des belligérants et en tirer les conclusions.

Du temps sera nécessaire pour une enquête et une analyse méthodique, qui évitera de tomber dans le piège des raccourcis pris lors de l'emballement médiatique observé au mois d'août 2008, en s'attachant à répondre à quelques questions:

- Cette «guerre de l'information» s'est-elle résumée à quelques défigurations et mises hors services de sites internet officiels? Quel aura été l'impact des défigurations et mises hors services des sites officiels?
- Quelles actions dans le cyberespace ont été des actes de guerre, quelles actions relèvent uniquement des actes de délinquance?
- Les affrontements révèlent-ils l'existence d'un arsenal de cyberguerre?
- Quelles actions ont été menées sous la direction de l'armée et du gouvernement? L'armée s'est-elle réellement emparée de l'espace informationnel?
- Des citoyens (russes, pro-russes, géorgiens, pro-géorgiens) se sont-ils impliqués au cyber-conflit? Le concept de «guerre du peuple» cher à l'armée chinoise gagnerait-il le monde?
- La participation des civils aux conflits est-elle un atout ou contribue-t-elle à accroître le brouillard du champ de bataille?
- Quelles sont les relations, si elles existent, entre crime organisé et effort de guerre, dans le cyberespace? L'implication du RBN dans les cyberattaques contre la Géorgie est-elle avérée?
- L'avantage pris par l'offensive en matière de cyber-agression est-il imparable?
- Faut-il accorder une importante stratégique, politique, aux opérations non revendiquées? Doit-on leur donner une importance politique ou les laisser dans le champ de la délinquance ordinaire?
- L'objectif de maîtrise de l'espace informationnel n'est-il pas une utopie?
- La guerre de l'information confère-t-elle un avantage menant au succès?
- Une guerre moderne, éclair ou sur le long terme, peut-elle être gagnée sans recours à la guerre de l'information?
- Si l'on considère que la Russie a gagné cette guerre, le doit-elle à ses actions cinétiques létales ou bien en grande partie à son avantage sur le champ de la guerre de l'information? ■

Im Blitzkrieg zwischen Russland und Georgien vom August 2008 hat die Information eine zentrale Rolle gespielt: mit Erklärungen, Propaganda und ganz allgemein mit den Medien sollte die nationale und internationale Haltung der Mächte beeinflusst werden.
Es ist heute zu früh, abschliessend Erkenntnisse aus dem Konflikt zu ziehen. Sicher ist, dass der Internet-Krieg eine neue Dimension der Informationskriegführung darstellt und dass Russland als Sieger sich auf diesem Feld besser behauptet hat. *Be*

1 www.president.gov.ge
2 http://www.mfa.gov.ge/
3 http://www.parlament.ge/
4 http://www.mod.gov.ge
5 http://www.nbg.gov.ge
6 http://en.rian.ru/russia/20080810/115936419-print.html
7 http://stopgeorgia.ru à ne pas confondre avec le site stoprussia.org
8 Voir capture d'écran sur http://www.civil.ge/eng/article.php?id=18896&search=hack
9 http://abkhazia.gov.ge
10 11 août 2008. http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html
11 georgiamfa.blogspot.com
12 http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/
13 http://www.president.pl
14 http://www.civil.ge/eng/article.php?id=11511

Daniel Ventre
Ingénieur
Chercheur au CESDIP
Montigny le Bretonneux
France