La dimension cybernétique de la crise ukrainienne

24/03/2014 à 07h00 Mis à jour le 24/03/2014 à 09h37

Le conflit ukrainien a aussi lieu dans le cyberespace, et les cyberattaques peuvent donner des indications sur les prochaines manœuvres ayant lieu sur le terrain. Difficile cependant de savoir à qui profitent ces opérations.

Les acteurs militaires ou civils des conflits armés s'efforcent d'exploiter le cyberespace au mieux de leurs intérêts. Traitant des évènements en Ukraine, les médias internationaux se sont fait l'écho ces derniers jours d'informations qui tendraient à démontrer, une nouvelle fois, que les réseaux se trouvent au cœur de l'action : défigurations de sites internet (d'institution, entreprises, ministères), attaques par déni de service, intrusion dans des serveurs et vols de données sensibles, propagation de malwares (le virus Snake, actif depuis plusieurs années, aurait infecté des réseaux gouvernementaux ukrainiens), attaques contre les portables des parlementaires ukrainiens (via des équipements qui auraient été installés sur les systèmes de télécommunication en Crimée), utilisation des réseaux sociaux, constituent l'essentiel des formes d'utilisation par les divers protagonistes. Ces derniers sont nombreux : hackers/hacktivistes nationalistes/patriotes, pro-Russie, pro-Ukraine, pro-Europe, d'autres refusant pour l'Ukraine la seule alternative Russie/Europe ; cyberactivistes ; cybercriminels pouvant être mobilisés par des Etats ; acteurs étatiques (renseignements, armées)... Mais les identités réelles peuvent se perdre dans les méandres du net et le cyberespace, univers du virtuel, permet toutes les constructions. Le risque de manipulation, de désinformation est grand.

Difficile de mesurer l'impact des cyberattaques sur le conflit

À LIRE AUSS

Nexans va di
mensuelle à s
crise durera
(http://bfmbus
va-distribuer-
ses-salaries-t
1890454.htm

Droit de retra
il faut que « l'
prévient Cédr
(http://bfmbus
de-retrait-dan
que-l-arriere-
1878329.htm

Il est également difficile de faire la part entre les actions devant être associées spécifiquement au contexte, et celles qui constituent le lot quotidien du cyberespace (les défigurations de sites ne sont ainsi pas propres à un contexte de crise internationale ou de conflit). Difficile également de peser l'efficacité réelle des actions menées (en quoi par exemple la défiguration d'un site internet ou de quelques centaines même, étatiques ou non, oriente-t-elle le cours de l'histoire ou remet-elle en question la sécurité d'un Etat ?).

Nombre d'opérations peuvent également se tramer dans l'ombre, à l'initiative des Etats, en vue d'un éventuel affrontement armé : opérations dans le cyberespace visant à préparer la maîtrise informationnelle sur un théâtre d'opération, cyberattaques visant à affaiblir des adversaires (attaques contre des systèmes d'information, de télécommunication, de commandement ; opérations de sabotage par le biais de cyberattaques).

La problématique est celle de la place du cyber dans les relations internationales, et plus particulièrement dans les crises et les conflits armés, intra et interétatiques. Elle peut être déclinée en un ensemble d'interrogations : les forces armées ukrainiennes ont-elles tiré profit des échanges entamés avec l'OTAN sur les questions de cyberdéfense ces dernières années ? Les cyberdéfense ukrainienne est-elle opérationnelle ou dépendra-t-elle de l'aide indispensable de pays alliés? Les Etats ont-ils tiré toutes les leçons de la dimension cybernétique du conflit russo-géorgien de 2008 ? Les cyberattaques sont-elles un facteur de désescalade de la violence (selon qu'elles peuvent faire office de moyen de contrainte et de dissuasion, ou qu'elles sont utilisées comme substituts à certaines formes de violence cinétique), ou bien au contraire sont-elles des pratiques à haut risque, pouvant entraîner des répliques - recours à la force armée - voire une extension géographique du conflit (du fait de l'absence de maitrise totale de la propagation d'une attaque virale, ou de maîtrise de la complexité des réseaux rendant les acteurs interdépendants les uns des autres) ?

Des manœuvres dans le cyberespace qui préfigurent des actions sur le terrain ?

Pour les principaux protagonistes, l'utilisation défensive/offensive du cyberespace constitue donc un véritable défi : parce que les intentions des adversaires sont toujours difficiles à anticiper ; parce que le réel niveau capacitaire des Etats en matière de cyberdéfense est assez mal connu ; parce qu'un cadre juridique international fait encore défaut. Comment russes et américains vont-ils décider d'utiliser leurs importantes capacités de cyberdéfense dans ce contexte ? Les limites sont, outre la technique, celles que se posent les Etats, en termes de droit, d'éthique, d'évaluation du risque et des effets attendus.

Quoi qu'il en soit, la situation en Ukraine doit être observée au prisme de ce qui se passe dans le cyberespace, dont certains événements pourraient être les signes avant-coureurs de nouvelles manœuvres sur le terrain.

Daniel Ventre

Daniel Ventre est ingénieur au CNRS (Centre de recherches sociologiques sur le droit et les institutions pénales - CESDIP), titulaire de la Chaire Cybersécurité & Cyberdéfense (Ecoles de Saint-Cyr Coëtquidan - Sogeti - Thales), chargé de cours à Télécom ParisTech. Ses travaux et publications traitent des conflits dans le cyberespace (guerre de l'information, cyberguerre). Il est également directeur de la collection Cyberconflits et cybercriminalité, aux éditions Hermès-Lavoisier.