De l'impact de pratiques de cyber-surveillance sur les relations internationales

10/12/2013 à 14h46 Mis à jour le 13/12/2013 à 10h15

Les conséquences géopolitiques au niveau régional du réseau de cyber-surveillance mis en place par les Etats-Unis sont multiples : risques d'exacerbation des tensions, rupture du dialogue et des projets de coopération en cours, motivation accrue des hacktivistes. Pourtant aucune réponse collective et coordonnée des Etats victimes n'est encore apparue.

Asie du Sud-Est : Singapour agit comme tierce partie au bénéfice des 5 grands yeux du réseau de cyber-surveillance centré sur les Etats-Unis, et intercepte les communications de ses pays voisins depuis des décennies. Voilà autant de données de nature à tendre les relations avec son voisinage, notamment la Malaisie, qui fut l'une des cibles de ces activités d'espionnage (http://www.nst.com.my/latest/dpm-malaysia-takes-spying-allegations-seriously-1.412915). Le projet de cyber-surveillance planétaire déployé par les Etats-Unis et ses alliés a ainsi des implications et des conséquences à l'échelle de cette région et de bien d'autres sur la planète.

Nous pouvons formuler quelques hypothèses et constats quant aux conséquences des pratiques et révélations de cyber-surveillance.

Aucune réponse coordonnée des Etats victime de la cyber-surveillance américaine

Si de nombreux [illegible] se trouvent être la cible des opérations d'un réseau (constitué d'un [illegible]sur américano-centré étendu à quelques-uns de ses alliés), on ne voit pas pour autant se constituer une réponse coordonnée des Etats victimes. Nous constatons que les Etats touchés (France, Allemagne, Mexique, Brésil, Indonésie, Malaisie, Chine…) adoptent tous des démarches similaires : discours ferme, résolu à ne pas accepter la situation, convocation des diplomates ou entretiens avec des membres des gouvernements incriminés, demandes d'explications et d'excuses, manifestation officielle du mécontentement (http://www.huffingtonpost.com/huff-wires/20131126/as--malaysia-singapore-spying/?utm_hp_ref=green&ir=green). Les autorités sont dans l'obligation de faire passer un message : vis-à-vis de l'extérieur, mais aussi de l'intérieur (leurs citoyens, les groupes de défense des droits et des libertés individuelles (http://www.themalaymailonline.com/malaysia/article/perkasa-to-singapore-apologise-to-malaysia-over-spy-claims)…) Les réponses à l'action du réseau dit « agresseur » se font de manière individuelle et se trouvent ainsi dépourvues de force de pression réelle.

Un risque d'exacerbation des tensions à l'échelle régionale

Les relations internationales ne s'en trouvent pas encore radicalement transformées. Pourtant, nous ne saurions écarter l'éventualité de voir ces questions de cybersécurité servir de moteur à l'exacerbation de tensions et conflits sous-jacents, notamment à l'échelle régionale (Malaisie-Singapour par exemple). Si les situations ne peuvent s'envenimer en Europe au point de menacer de rompre des relations diplomatiques, économiques, culturelles, avec des nations dont elle dépend, il n'en ira peut-être pas de même sous d'autres horizons.

Coopération et dialogue régionaux remis en cause

Certains Etats remettent déjà en question des relations jusque-là dites de confiance: l'Indonésie ayant appris qu'elle était l'objet d'espionnage de la part de l'Australie, a choisi de mettre un frein à son programme de coopération militaire avec cette dernière (http://www.scmp.com/news/asia/article/1360037/indonesia-review-ties-australia-amid-row-over-wiretap-president). Des deux côtés, australien et indonésien, la perception des pratiques diffère. L'Indonésie attend bien plus que de simples explications, se sentant visiblement trahie par un partenaire privilégié ; de son côté le pouvoir australien tend à minimiser l'affaire, et ne paraît pas disposé à apporter d'explications, encore moins à s'excuser. Le dialogue est donc rompu. Certains observateurs n'hésitent pas à parler de désastre diplomatique (http://www.abc.net.au/news/2013-11-25/maccallum-a-diplomatic-disaster-from-the-spy-boffins-up/5114482).

L'accumulation de « désastres » diplomatiques pourrait altérer le projet américain dans la région, qui vise à créer un réseau d'alliés, de partenaires, dans le but de contrer la montée en puissance de la Chine.

Les hacktivistes confortés dans leurs attaques contre les Etats espions

Les Etats « agresseurs » ou « espions » se trouvent désormais dans le viseur des hacktivistes et autres hackers, leur fournissant prétexte à l'action. Des membres indonésiens d'Anonymous (http://www2.interaksyon.com/article/74103/anonymous-indonesia-hacks-

australia-sites-ov[illegible]ng) ont lancé des cyberattaques contre des centaines de sites australiens, mais aussi philippins et singapouriens (dont celui du premier ministre) (http://www.analyzednews.com/article.php?id=6571453&category=worldNews)[1], en guise de représailles.

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.

Auteurs de plusieurs ouvrages sur la question, Daniel Ventre tient également un blog (http://econflicts.blogspot.com).

Daniel Ventre