Cyber : instrument de la puissance russe en Baltique

Dans le cadre de sa stratégie de guerre hybride et d'action diplomatique, la Russie procède à des actions offensives dans le cyberespace, notamment dans son environnement proche. En conséquence, les Etats ciblés renforcent leurs normes de sécurité informatique.

Ce thème a fait l'objet d'un colloque organisé, le 25 mai 2018 à Paris, par l'Institut de recherche stratégique de l'Ecole militaire (IRSEM). Y sont notamment intervenus : Rémi Géraud, chercheur à l'Ecole normale supérieure ; François-Bernard Huyghe, chercheur à l'Institut de recherches internationales et stratégiques ; François Delerue, chercheur à l'IRSEM.

L'info-sphère russophone. Héritière des canaux développés pendant l'ère soviétique, la Russie a fondé son propre réseau internet dénommé Runet, régi par le droit russe et sur lequel se sont greffés les journaux publiés à l'étranger (135 langues), explique Rémi Géraud. A partir de 2011, leur nombre a été réduit pour donner naissance notamment à *Rossija Segodnia*, organisme officiel de communication à l'international (2013), et *Sputnik*, agence de presse multimédia internationale (2014). Cette dernière se présente comme « alternative » et « *dévoile ce dont les autres ne parlent pas* ». Les moteurs de recherche Yandex, équivalent de Google, et VKontakte, équivalent de Facebook, diffusent en russe pour contrer l'hégémonie de l'anglais. Ensuite, des voix bénévoles, mais politiquement engagées dans la ligne officielle, en reprennent les éléments de langage, qui seront présentés comme des faits légitimes provenant d'une source non-russe. En outre, il s'agit de maintenir un climat de doute, d'incertitude ou de conspiration en discréditant, de façon répétée, les experts occidentaux par des parodies, scandales ou débats et de souligner la « russophobie » des médias occidentaux. L'appel au sentiment d'humiliation identitaire, culturelle, historique ou morale, surtout dans la zone baltique, se combine à l'image d'une Russie forte. Divers médias destinés aux pays baltes, comme *Baltic Media Alliance, Sputnik* en version locale, *Vesti. Iv* et *Rubaltic.ru* se reprennent mutuellement et diffusent, en langue locale, des contenus issus des médias russes. Il s'agit de légitimer les populations russophones baltes et un retour des pays baltes dans le giron de la

Russie. Des sondages réalisés en Lettonie en 2015 montrent l'efficacité de cette propagande. Pour en maintenir l'effet, trois axes se dégagent : montrer une image frappante plutôt qu'un débat ou alors le discréditer pour délégitimer l'adversaire ; développer méthodes (équipes) et moyens technologiques (logiciels dédiés) pour élaborer et diffuser du contenu rapidement et à grande échelle ; s'appuyer sur des slogans, « hashtags », citations et interviews pour en rendre les origines floues, en faciliter la reprise et donner l'illusion d'une omniprésence. Ce mode de communication privilégie les réponses des médias et des « cibles » par rapport à la véracité ou la fausseté des faits. Il commence par choisir ses thèmes : menaces militaire, politique, morale et économique de l'OTAN et de l'Union européenne ; imminence d'un conflit militaire proche ; hausse du nazisme à cause des politiques libérales ; « menace » russe présentée comme une propagande ; force et exemplarité de la Russie ; persécution de la Russie et des minorités russes. Ensuite, il construit une image par : des stocks de photos ou vidéos existantes, copies d'écran ou création, rares, de documents ; récoltes d'avis de personnes présentées comme des « experts » ou « l'opinion publique ».

L'attribution et la preuve. En droit, la preuve, matérielle ou établie par un expert qui sait l'interpréter, permet de démontrer l'existence d'un fait, à savoir identifier une cyber opération et ses conséquences puis l'attribuer, explique François Delerue. En 2007, l'Estonie a été paralysée par des cyber attaques par déni de service à des institutions gouvernementales, médias et banques. Membre de l'OTAN, elle a tenté, sans succès, de la faire intervenir, faute de pouvoir les attribuer avec certitude à la Russie car le « reroutage » des données a utilisé 180 pays. En 2009, l'origine du virus Stuxnet, utilisé contre les centrifugeuses du programme nucléaire iranien, a été identifiée par des indices relatifs à Israël et une « fuite » venue des Etats-Unis. Pendant longtemps, Téhéran a cru à une malfaçon des centrifugeuses avant de considérer une cyberattaque. En 2010, l'Iran est parvenu à modifier le plan d'autoplanage d'un drone américain RQ170 pour le forcer à atterrir sur son sol. Il a revendiqué cette action pour une raison politique et a vendu les plans du drone à la Chine et à la Russie. Théoriquement, l'attribution implique une machine, une personne et un Etat, mais pas dans une suite logique. Un ordinateur peut être détourné sans identification de son utilisateur et l'effacement de certains éléments altère l'intégralité de la preuve. Le mode opératoire, complémentaire des informations techniques, identifie la personne à l'origine d'une cyber opération. En 2015, les Etats-Unis ont attribué à la Corée du Nord celle contre Sony Picture Entertainment, grâce à des écoutes de

ses télécommunications, moyen inacceptable pour un tribunal international. La découverte de lettres cyrilliques lors du piratage de la convention du parti Démocrate aux Etats-Unis en 2016 n'a pas suffi à établir, de façon légale, un lien de causalité, que la Russie a démenti. Les cyber opérations, conduites ou commanditées par des Etats, émanent d'organes officiels ou mis à la disposition d'un Etat par un autre Etat, de personnes ou d'entités exerçant des prérogatives de puissance, même si celles-ci outrepassent leurs compétences ou contreviennent aux instructions reçues. En fait, 90 % des cyber opérations sont conduites par les Etats-Unis, la Russie et la Chine, qui opposeraient leur veto de membres permanents du Conseil de sécurité si le sujet était abordé à l'ONU. Ces trois pays exercent aussi une grande influence au sein de la Cour internationale de justice de La Haye.

Loïc Salmon

Depuis l'antiquité, le stratagème consiste à amener l'adversaire à prendre la mauvaise décision sous l'effet d'apparences fausses pour le déstabiliser, rappelle François-Bernard Huyghe. La propagande « noire » des deux guerres mondiales recherche l'adhésion des masses en attribuant les pires horreurs à l'ennemi. Dès 1953, l'URSS pratique la désinformation, en distillant de fausses nouvelles dans les mass médias des pays occidentaux pour créer le chaos parmi leurs dirigeants. Dans les années 1960, les Etats-Unis répliquent par des émissions radio vers l'URSS, en vue d'exercer un effet subversif sur ses élites et médias. A l'ère d'internet et des réseaux sociaux et dans un contexte géopolitique de tensions, apparaissent les « fake news », à savoir des allégations à partir d'un fait réel pour les rendre vraisemblables. Celles-ci créent un scepticisme à l'égard des médias traditionnels parmi les masses, enclines à choisir un contenu informationnel plus conforme à ses conceptions. Les « fake news », soupçonnées d'avoir perturbé le processus démocratique lors des élections américaines de 2016, ont surtout été attribuées à la Russie. Toutefois, des études américaines ont démontré que l'effet des « fake news » est resté limité. Celles-ci n'ont représenté que 6 % du flux total d'informations diverses.

Guerre de l'information et information de guerre

Cyber : au cœur des enjeux de défense et de sécurité

Proche-Orient : retour en force de la Russie dans la région