Cyber : dilution des frontières territoriales et souveraineté

Les grands acteurs privés du cyberespace transforment l'exercice de la souveraineté des Etats, qui doivent coopérer entre eux, pour limiter leur dépendance à leur égard, et tenter de répondre aux cyberattaques anonymes.

Ce thème a été abordé lors d'un colloque organisé, le 13 mars 2018 à Paris, par l'Institut des hautes études de défense nationale et la Chaire Castex de cyberstratégie (CCC). Y sont notamment intervenus : la professeure Frédérick Douzet, Université de Paris 8 et titulaire de la CCC ; le général de division Olivier Bonnet de Paillerets, « Comcyber » (*voir encadré)* ; David Martinon, ambassadeur pour le numérique au ministère des Affaires étrangères ; Pavel Karasev, chercheur à l'Université de Moscou.

Mouvement permanent. Le cyberespace constitue une communauté avec des interactions entre les sociétés humaines, connectées et évolutives, et les infrastructures géo-localisables qui les mettent en relation, explique Frédérick Douzet. Sa cartographie, interdisciplinaire, intègre la géographie, l'économie et les réseaux sociaux. Un dialogue approfondi entre eux permet de faire émerger un photomontage informatique à partir de données géopolitiques. Il est ainsi

possible d'identifier les points de vulnérabilité d'un territoire donné. La cartographie du cyberespace permet aussi de replacer les conflits dans leur contexte avec une approche régionale et de comprendre les stratégies d'influence. L'OTAN et les Livres blancs de la défense et de la sécurité nationale 2008 et 2013 ont identifié le cyberespace comme champ de bataille à part entière. Son réseau planétaire en fait, pour chaque pays, un enjeu de puissance, un territoire à défendre et une menace stratégique.

Espace de conflictualité. Les crises dans le monde prennent aussi une dimension cyber, impliquant technique et approche opérationnelle, estime le général Bonnet de Paillerets. Il y distingue trois couches en interaction : les infrastructures, à savoir les télécommunications et les serveurs ; les applications, construites sur les algorithmes ; l'espace cognitif, à savoir le contenu de l'information et les données. Leurs impacts sur la territorialité et la souveraineté relèvent de la responsabilité de l'Etat. La Grande-Bretagne et l'Allemagne dès 2016, puis la France en 2017 se sont dotées d'une capacité de cyberdéfense. Celle-ci comprend la détection d'une attaque, sa caractérisation, son attribution (origine) et la réponse si elle dépasse le seuil acceptable. Le champ de souveraineté s'exerce sur la maîtrise de l'équipement de détection par la technologie du code, l'intelligence artificielle et le chiffrement. La sécurité collective entre dans une logique de partenariats reposant sur le partage et la confiance. En cas d'escalade, faute de régulation contre la montée en force des attaques, il convient de réfléchir sur les équipements critiques concernés. La numérisation du champ de bataille constitue une opportunité pour le cyber, qui devient une arme d'emploi. Les experts participent à l'engagement opérationnel cyber, en intégrant l'innovation dans le champ de bataille. Enfin, l'espionnage des administrations et des entreprises, en vue d'en tirer des avantages opérationnels et économiques, préoccupe le ministère des Armées, souligne le Comcyber.

Combat au quotidien. Menaces et influence visent l'Etat et aussi les acteurs privés. Les lois de la République doivent s'appliquer sur le territoire français, notamment contre les contenus de messages haineux, antisémites, islamistes ou terroristes, rappelle l'ambassadeur Martinon. La manipulation de l'information en période électorale fait l'objet d'un projet de loi. Les règles du droit international s'appliquent au cyberespace, même en période de non guerre. L'absence de coopération conduit à la confrontation, où prime le rapport de force dans le contexte de « nouvelle guerre froide » (entre la Russie et l'Occident). L'évaluation

de l'échelle de sévérité des attaques, considérées comme acceptables avec des réponses appropriées ou qualifiés d'agressions débordant le droit international, relève du secret défense, souligne l'ambassadeur. Il s'agit d'éviter l'escalade et d'accélérer la désescalade, quand la situation devient paroxystique. Un renseignement efficace permet d'identifier l'attaquant. Certaines entreprises privées d'une portée mondiale défendent leurs intérêts et disposent d'atouts qui dépassent les moyens des Etats. Les frontières, plus diffuses aujourd'hui, peuvent être contournées sur des principes moraux, politiques ou juridiques, même entre pays alliés. Ainsi, des organisations américaines non gouvernementales estiment abusives les lois françaises sur la liberté d'expression. Des diffamations condamnées en France peuvent continuer à s'exercer ailleurs dans le monde. Quoique les intérêts américains soient plus ou moins bien définis, les « géants du numérique » (Google, Apple, Facebook, Microsoft, Twitter, Yahoo et Amazon) concourent à la politique extérieure des Etats-Unis. En outre, la Maison-Blanche soutiendra coûte que coûte les entreprises américaines, en raison de leur patriotisme.

Absence de réglementation. Depuis 2001, la Russie travaille sur la couche du cyberespace relative au contenu, pour mieux la comprendre et élaborer des normes nationales et internationales, indique Pavel Karasev. Les efforts portent sur la prévention des incidents technologiques, la recherche de leurs causes et la nécessité d'un accord international sur la définition de la cybercriminalité. Par ailleurs une soixantaine de pays dans le monde disposent de la capacité de cyberattaques. Celles-ci ne sont pas des attaques militaires, car les technologies d'information et de communication ne sont pas considérées comme des armes sur le plan international, estime Pavel Karasev. Le droit à l'auto-défense ne s'y applique donc pas, faute de preuves réelles. Selon lui, le droit international devrait s'engager sur la sécurité nationale et la création d'un espace d'information mondial sécurisé, pour éviter une « guerre froide numérique ».

Loïc Salmon

Cyber : au cœur des enjeux de défense et de sécurité

Cyber : le combat numérique, nouvelle dimension militaire

Cyberdéfense : entraînement complet au sein des armées.

En France, le Commandement de la cyberdéfense (Comcyber), assuré par un

officier général, s'occupe de la protection et de la défense des systèmes d'information du ministère des Armées et de la conduite des opérations numériques. Il compte une soixantaine de personnels et dispose du « Centre des opérations de cyberdéfense ». En 2017, il a été confronté à plus de 700 incidents ou attaques. Au sein de l'armée de Terre, la cyberdéfense comporte la cyberprotection et la lutte informatique défensive. L'armée de Terre inclut la cybersécurité dans les programmes d'armement en cours de développement : nouveau système d'information des armées et programme « « Scorpion ». La Marine nationale s'entraîne régulièrement à prévenir et déjouer les cyberattaques dans les systèmes navals embarqués ou les équipements des ports. Elle dispose du « Centre support cyberdéfense » et de groupes d'intervention rapides, projetables partout dans le monde. L'armée de l'Air a affecté la cyberdéfense au Commandement de la défense aérienne et des opérations aériennes. Elle dispose du « Centre air de conduite cyberdéfense » et du « Centre air d'expertise cyber ».