Bernard Barbier, Jean-Louis Gergorin et Edouard Guillaud : « La France doit engager le nécessaire sursaut stratégique sur le cyber et la lutte Informationnelle »

Collectif

Le cyberparapluie américain protégeant les infrastructures européennes n'est pas éternel. Trois spécialistes en défense soulignent, dans une tribune au « Monde », que la France a les moyens techniques et humains pour affirmer un leadership dans ce domaine essentiel en matière de sécurité.

Après cent vingt jours de guerre de la Russie contre l'Ukraine, le bilan des opérations cyber-offensives russe est très contrasté. Des cyberattaques contre des ports pétroliers en Allemagne, en Belgique et aux Pays Bas ont été détectées à partir du 29 janvier. L'objectif de ces attaques attribuées par les Etats-Unis, le Royaume-Uni et l'UE à des groupes criminels russes connus était de perturber l'approvisionnement énergétique de l'Europe.

Le 24 février, le service de communication par satellite de l'opérateur américain VIASAT a été bloqué par une cyber-attaque attribuée aussi à la Russie par les Européens et les Américains. Elle a fortement perturbé les communications militaires ukrainiennes en ce début du conflit jusqu'à ce qu'Elon Musk propose et mette rapidement en œuvre une solution de remplacement grâce à sa constellation satellitaire Starlink.

L'Ukraine a subi de très nombreuses cyberattaques avant et depuis le 24 février. Cependant, ses infrastructures critiques semblent avoir plutôt résisté. Les Américains ont confirmé publiquement qu'ils avaient aidé les Ukrainiens à durcir le système d'information de leurs opérateurs critiques et aussi à supprimer les implants que les Russes avaient déposés avant leur invasion.

Pas d'infrastructures touchées par une cyber attaque

De son côté, la Russie a subi de nombreuses cyberattaques provoquées par des groupes activistes tel « Anonymous », qui a réussi des opérations symboliques comme la perturbation de la retransmission télévisée du discours de Vladimir Poutine le 9 mai. Depuis février 2014, la Russie est en guerre hybride permanente avec l'Ukraine, soutenue, depuis lors, par des experts du cyber officiels et privés occidentaux, notamment américains.

A la suite de la mise en œuvre de sanctions occidentales contre la Russie, Vladimir Poutine a évoqué des ripostes « militaro-techniques » (comprendre cyber). En dépit des inquiétudes du Président Biden, aucune cyberattaque visible ne s'est produite contre des infrastructures critiques américaines et européennes. L'explication se trouve dans un discours prononcé le 1er juin par le général Nakasone, chef de l'US CyberCommand et directeur de la NSA, au Centre d'expertise du cyber de l'OTAN à Tallinn, en Estonie. Dans ce discours, puis dans une interview à Sky News, Nakasone révèle que son commandement conduit des

opérations cyber défensives et offensives, et de lutte informationnelle, en soutien de l'Ukraine comme des alliés atlantiques.

Un catalogue d'intentions louables

A partir de renseignements sur des cyberattaques en préparation, le CyberCommand lance des opérations de neutralisation des outils de ces attaques qui ont évidemment aussi un effet dissuasif. Il serait erroné de conclure comme le font certains de nos partenaires de l'UE, qu'il existe un cyber-parapluie américain durable protégeant les infrastructures européennes.

Il apparaît en effet de plus en plus probable que les Républicains, avec une majorité de candidats peu europhiles influencés par Donald Trump, reprendront au minimum un contrôle fort de la Chambre des Représentants lors des midterms (élections de mi-mandat) en novembre, et auront de bonnes chances de remporter la présidentielle de 2024 avec Trump ou un trumpiste.

Or, le grand écart que nous avons mentionné, en janvier, entre les doctrines et capacités américaines et britanniques d'une part, et une politique cyber européenne d'autre part, essentiellement fondée sur la résilience, n'a pas changé. La « boussole stratégique » adoptée en mars par le Conseil Européen reste d'abord à ce stade un catalogue d'intentions louables.

Les trois initiatives importantes

Dans ce contexte, seule la France possède en Europe continentale à la fois des capacités techniques suffisantes et les ressources humaines associées dans le cyberespace. Elle seule est ainsi en mesure, et peut avoir la volonté de prendre le leadership d'un sursaut européen qui associerait le discours et les actes.

Alors qu'elle subit depuis cinq ans en Afrique francophone, notamment au Sahel, une offensive informationnelle russe majeure à l'impact évident, elle a défini en octobre 2021 une doctrine de lutte informatique d'influence confiée au Commandement de Cyberdéfense.

Trois initiatives pourraient être lancées :

- d'abord, énoncer clairement et publiquement que toute cyberattaque immédiate ou « à retardement » (pose d'implants) contre des infrastructures critiques civiles ou militaires entraînera une riposte appropriée. Il est inutile d'être plus précis, pour cultiver une nécessaire ambiguïté dialectique ;
- ensuite, augmenter encore plus significativement et optimiser les moyens du cyberrenseignement aux fins d'attribution des cyberattaques et des manipulations informationnelles étrangères, toutes activités qui sont menées par les mêmes services au sein des pays autoritaires. Les efforts récemment annoncés au plus haut niveau sont les bienvenus, il apparaît primordial de les amplifier ;
- enfin, développer des coopérations bilatérales complémentaires avec des partenaires européens choisis d'abord pour leurs compétences, cyber et informationnelles, mais aussi pour leur attitude dynamique et leur refus de se contenter d'une simple résilience. En la matière, la passivité ne peut être de mise. Ces coopérations n'empêcheront ni celles avec nos alliés anglo-saxons ni les souhaitables et lucides dialogues avec la Russie et la Chine.

Des moyens trop dispersés

Comme seul pays de l'Europe continentale membre permanent du Conseil de sécurité de l'ONU, la France peut et doit engager un sursaut stratégique essentiel pour sa sécurité et son statut ; elle a su le faire en son temps et avec succès dans les domaines nucléaire et spatial. Nous investissons dans la cybersécurité deux à trois fois moins que les Britanniques, en termes de moyens humains comme financiers ; nos deux pays sont pourtant de taille et de puissance équivalentes.

Alors que notre expertise technique est reconnue par nos alliés, nos moyens sont encore trop dispersés au sein de plusieurs entités : il est temps de réfléchir à un socle technique commun et mutualisé à l'instar de nos alliés britanniques.

Surtout, comme les autres membres du Conseil de sécurité, il est nécessaire de compléter l'excellente coordination opérationnelle par un pilotage stratégique, cyber et informationnel unique au plus haut niveau de l'État, intégrant non seulement les volets défense et sécurité, mais aussi les relations diplomatiques et l'interaction avec les grands acteurs privés numériques dont le rôle ne peut être ignoré.

Les signataires : Bernard Barbier, ancien directeur technique de la DGSE, ancien directeur du Laboratoire d'électronique de technologiques de l'information (LETI) et membre de l'Académie des technologies ; **Jean Louis Gergorin**, chargé de cours à Sciences Po, ancien chef du Centre d'analyse et de prévision du Quai d'Orsay ; **Edouard Guillaud**, amiral et ancien chef d'état-major des armées.