EUROPE

« Lutter contre des attaques hybrides est très compliqué »

La Russie et d'autres Etats hostiles se montrent de plus en plus audacieux avec des attaques hybrides un peu partout en Europe : piratages informatiques, drones, colis explosifs, sabotages, désinformation, etc. Pas évident de trouver la parade.

PHILIPPE DE BOECK

Les attaques hybrides ne sont pas nouvelles, mais elles se sont intensifiées depuis l'invasion de l'Ukraine par la Russie en février 2022. Les spécialistes parlent plutôt d'opérations en zone grise, parce qu'elles sont en dessous du seuil de conflictualité. Les commanditaires qui se cachent derrière ces attaques exploitent la division et l'hésitation des démocraties occidentales. « Pour y faire face, une réponse unifiée et des mesures renforcées sont nécessaires, faute de quoi la Russie et d'autres acteurs continueront à en tirer profit », résume un article publié le 4 janvier dans le *New York Times*.

« Le contexte est en effet celui de l'érosion de l'ordre international fondé sur des règles et d'attaques hybrides visant la démocratie et la sécurité européennes », observe de son côté la présidence polonaise du Conseil de l'UE. La désinformation, le sabotage, le piratage informatique et les assassinats ciblés font partie de l'attirail de la guerre hybride.

Plus de 35 attaques en 2024

D'après l'expert militaire belge et ancien colonel Roger Housen, au moins 35 opérations ou attaques hybrides (sabotages et attentats) ont été recensées en Europe dans le courant de l'année 2024. L'une d'elles a paralysé un hôpital près de Munich pendant une semaine, nécessitant le transfert de patients vers d'autres établissements de soins.

D'autres opérations ont endommagé des câbles de télécommunications sous-marins entre la Suède et la Finlande, et entre la Finlande et l'Estonie en mer Baltique.

L'une des attaques les plus visibles s'est produite en juillet dernier avec l'explosion de plusieurs colis de courrier express. Envoyés depuis la Lituanie, ils contenaient des appareils de massage électrique renfermant une substance hautement inflammable à base de magnésium. Deux colis ont explosé dans des installations de DHL en Grande-Bretagne et en Allemagne, et un troisième dans une société de messagerie polonaise.

Le mystérieux crash en phase d'atterrissage d'un avion-cargo DHL à Vilnius le 24 novembre dernier pourrait également être dû à l'explosion d'un colis.

D'après des experts cités par le *New York Times*, des enquêteurs polonais ont estimé que ces colis étaient des tests effectués par l'agence de renseignement militaire russe GRU. « Nous disons à nos alliés que ce n'est pas aléatoire, cela fait partie des opérations militaires », a déclaré Kestutis Budrys, ministre des Affaires étrangères de la Lituanie à propos des colis piégés. « Nous devons neutraliser cela à la source, et la source, c'est le renseignement militaire russe. »

La Russie nie évidemment être à l'origine de ces actes de sabotage.

Vols de drones

Autre menace potentielle : les vols de drones au-dessus de sites sensibles. Il y a trois ans, de mystérieux drones ont commencé à survoler des plateformes pétrolières et des parcs éoliens au large des côtes de la Norvège. « Leur origine n'est pas certaine, mais nous savons ce qu'ils faisaient », a déclaré Stale Ulriksen, chercheur à l'Académie royale navale norvégienne. « Une partie était de l'espionnage où ils cartographiaient beaucoup de choses. Une autre partie consistait à se positionner en cas de guerre ou de crise majeure. »

Ces drones sont soupçonnés d'avoir été lancés à partir de navires russes en mer du Nord, a précisé M. Ulriksen, y compris des navires proches de pipelines énergétiques sous-marins. « La Norvège ne pouvait pas faire grand-chose pour les arrêter car ils survolaient les eaux internationales », a-t-il ajouté.

Des drones ont également été repérés fin novembre et début décembre au-dessus de bases militaires en Angleterre et en Allemagne où sont stationnées des forces américaines.

Des analystes militaires estiment que ces engins volants pourraient être en mission de surveillance pour le compte d'un Etat mais sans préciser lequel. Ils expliquent que la présence de ces drones illustre une attaque hybride contre l'Occident, où diverses tactiques (militaires, cybernétiques, économiques et psychologiques) sont utilisées pour attaquer ou déstabiliser un « ennemi » de manière discrète. L'ennemi étant dans ces cas-ci les pays qui soutiennent l'Ukraine dans leur effort de guerre contre la Russie.

Quelle réponse à ces attaques ?

Comment désigner le coupable lorsque ces opérations sont justement conçues pour éviter d'être attribuées à tel ou tel acteur ? Comment dissuader de telles opérations sans risquer de déclencher un conflit plus large ? « C'est justement ça le problème avec les opérations en zone grise. La riposte est très compliquée et il est difficile d'avoir une réponse équilibrée. Mais c'est voulu justement », résume Alain De Neve de l'Institut royal supérieur de défense (IRSD), en citant le sabotage de câbles sous-marins dans les eaux internationales. « La Suède est une habituée de ce genre de menaces, les pays baltes également mais d'autres plus au sud le sont moins parce qu'on a perdu nos réflexes de la guerre froide. Il faut aller vers une meilleure coordination des différentes agences au sein des Etats. Aujourd'hui, on en est loin », poursuit Alain De Neve.

Des opérations ont par exemple endommagé des câbles de télécommunications sous-marins entre la Suède et la Finlande, et entre la Finlande et l'Estonie en mer Baltique. © AFP.

Il faut aller vers une meilleure coordination des différentes agences au sein des Etats. Aujourd'hui, on en est loin

Alain De Neve
Chercheur au Centre d'études de sécurité et défense à l'Institut royal supérieur de défense

Pour lui, la réponse devrait d'abord se faire sous la forme d'une meilleure coordination entre Etats concernés. « L'Otan le fait sur le plan militaire mais au niveau civil et sécuritaire, il n'y a rien. C'est ça que l'UE devrait construire », estime encore Alain De Neve.

L'Otan est en train d'élaborer une nouvelle stratégie pour contrer ces attaques en remplacement de celle mise en œuvre en 2015. Et l'UE renforce ses efforts, imposant pour la première fois, en décembre, des sanctions contre seize individus et trois entités accusés de menaces hybrides pro-russes. Il s'agit entre autres de l'unité 29155 du GRU, une unité secrète au sein de l'agence de renseignement militaire russe.

« Un danger pour la démocratie »

Tout cela sans oublier des opérations plus sournoises comme la désinformation. « On peut lutter contre ça en préservant les outils d'information, le pluralisme des médias et le financement de l'audiovisuel public pour avoir la capacité à dénoncer ce type d'agissements », explique Yannick Quéau, directeur du Groupe de recherche et d'informations sur la paix et la sécurité (Grip).

« Le problème de la guerre hybride, c'est que c'est un danger pour la démocratie qui pourrait amener une réponse militarisée tout aussi orientée avec des professionnels de la guerre qui, eux, sont en mesure de nous dire ce qui doit être dit et comment pour contrer ce genre de choses. Si on ouvre cette porte-là, le problème, c'est qu'on devient un système autoritaire. Il faut lutter contre la désinformation en respectant le jeu de la démocratie. On s'en sort assez bien mais c'est plus compliqué en période électorale », conclut Yannick Quéau.

Guerre hybride ?

Ce qu'on appelle communément *guerre hybride* repose sur la combinaison d'instruments de puissance conventionnels et non conventionnels et de méthodes subversives. L'objectif est d'exploiter les vulnérabilités de l'adversaire et de réaliser des synergies en employant ces outils de façon coordonnée (sabotages, piratages, désinformation, etc.).

La guerre hybride présente deux particularités. La première est qu'elle brouille les lignes entre temps de guerre et temps de paix. D'où le fait que les spécialistes préfèrent parler d'« opérations en zone grise ». En d'autres termes, il devient difficile de discerner le seuil à partir duquel on peut parler de « guerre ». La notion même de « guerre » devient floue car on en distingue moins les manifestations concrètes et les contours.

La deuxième particularité de la guerre hybride tient à son caractère ambigu et est liée à la question de l'attribution. En général, un grand flou entoure les attaques hybrides parce que leurs auteurs cultivent l'ambiguïté afin de compliquer l'attribution des actes perpétrés ainsi que la réponse à ceux-ci. Avec une attaque informatique, par exemple.

L'idée est que le pays visé soit dans l'incapacité de déceler l'attaque hybride ou d'en attribuer la responsabilité à l'Etat ou le commanditaire qui en est l'auteur. En jouant sur les seuils de détection et d'attribution, les auteurs compliquent la tâche des Etats ciblés, qui peinent à mettre au point des mécanismes de réponse d'ordre stratégique ou autre. PH.DB.