UNION EUROPÉENNE

La population doit-elle s'inquiéter de « la guerre hybride » ?

Sabotages, drones, cyberattaques, désinformation… L'Europe est confrontée à une multiplication d'actions attribuées à la « guerre hybride » russe. Mais que recouvre vraiment cette notion ? Quatre questions pour comprendre.

DÉCODAGE

LINA AATTACHE (ST.)
UGO SANTKIN

Mi-septembre, deux drones ont encore été détectés au-dessus de l'aéroport de Zaventem deux nuits de suite. © AFP.

Une tentative d'attaque via un drone chargé d'explosifs sur un avion-cargo ukrainien à l'aéroport de Leipzig début août. Des fabricants d'armes fournissant l'Ukraine incendiés en Bulgarie, en Italie et en Estonie entre mi-août et mi-septembre. Des avions de chasse de l'Otan abattant il y a dix jours un drone (supposément venu de Biélorussie) au-dessus de la Lituanie. Un hélicoptère militaire russe faisant, mardi dernier, une incursion dans l'espace aérien polonais. En Pologne encore, mercredi, un incendie déclaré dans une station de communications par satellite utilisée par Varsovie et Kiev.

Ce sont là de simples exemples des dernières semaines, mais depuis des mois, les « attaques hybrides » sur le sol, dans le ciel ou dans les eaux du Vieux Continent se multiplient. Des attaques derrière lesquelles on suspecte quasi systématiquement la main du Kremlin. Si ces « incidents » poussent certains leaders européens à durcir leur discours vis-à-vis de la Russie, l'Europe s'est abstenue d'accuser frontalement Moscou, sauf à propos des évènements de Leipzig.

Des actions très différentes, donc, mais qui sont de plus en plus réunies sous une même appellation : la « guerre hybride ».

1

Qu'entend-on par « guerre hybride » ?

Il n'existe pas de définition officielle de la guerre hybride. Pour Roger Housen, ancien colonel belge et expert en défense, il s'agit d'« une guerre menée à la fois avec des moyens militaires et non militaires, comme des attentats, des incendies criminels ou encore du sabotage, mais aussi de la désinformation ou des fake news ». L'Otan y ajoute les cyberattaques, la pression économique ou encore le recours à des groupes armés irréguliers. Pour les autorités européennes, l'instrumentalisation des migrants par Minsk et Moscou, notamment lors des crises de 2021 et 2023 aux frontières de l'Union, relève également de cet arsenal de déstabilisation.

Le terme apparaît au milieu des années 2000, au sein de l'armée américaine, pour désigner un mélange de guerre conventionnelle, de guérilla et d'autres modes d'action, comme le terrorisme. Son usage évolue en Europe après 2014, avec le déclenchement du conflit dans l'est de l'Ukraine. « A partir de ce moment, il va être employé de plus en plus souvent au sein de l'Otan et de l'UE pour définir un certain nombre d'actions entreprises principalement par la Russie », explique Samuel Longuet, chargé de recherche au Grip (Groupe de recherche et d'information sur la paix et la sécurité).

Le chercheur reste toutefois critique envers le concept : « On utilise le terme de "guerre hybride" pour désigner des actions qui restent sous le seuil d'un "conflit armé", tel que défini par le droit international. » Pour lui, le concept banalise, d'une part, l'emploi du mot « guerre » et constitue, d'autre part, un « fourre-tout » regroupant espionnage, pressions économiques, désinformation, cyberattaques, sabotages ou survols de drones. Des actions très différentes par leur nature, leurs auteurs et leurs effets.

2

En quoi la Belgique est-elle touchée par des actions dites « hybrides » ?

La présence des institutions européennes, du siège de l'Otan et de l'organisme financier Euroclear fait de la Belgique une cible particulièrement exposée, estiment plusieurs observateurs.

Les survols de drones au-dessus de bases militaires, d'aéroports et d'autres infrastructures critiques, comme les centrales énergétiques, ont marqué les esprits depuis l'automne 2025. Mi-septembre, deux drones ont encore été détectés au-dessus de l'aéroport de Zaventem deux nuits de suite. « Plusieurs tentatives de sabotage, certes infructueuses, ont récemment été perpétrées contre des entreprises belges du secteur de la défense », relève Roger Housen. Selon une enquête de la RTBF, environ 150 signalements de drones ont été enregistrés en Belgique depuis le début de l'année.

3

Quelles stratégies adopter face aux pressions hybrides ?

Pour les autorités, le défi est double : identifier ces actions, ce qui est compliqué en raison de leur caractère difficilement attribuable, puis être capable d'y répondre et de les sanctionner de manière coordonnée. La difficulté tient aussi au fait que ces actes, pris séparément, peuvent sembler relever de faits divers ou d'incidents isolés.

La semaine dernière, la présidente de la Commission européenne, Ursula von der Leyen, a lancé la piste d'un « manuel de riposte aux menaces hybrides ». Ce mécanisme devrait aider les capitales à réagir aux « incidents » qui se situent « en deçà d'un conflit armé mais menacent clairement notre sécurité nationale ».

Pour Samuel Longuet, la réponse ne doit toutefois pas être essentiellement militaire : « C'est une autre faiblesse du concept : on parle de "guerre" alors que la plupart de ces actions n'impliquent que marginalement la défense. » Il estime qu'une réponse efficace doit associer une diversité d'acteurs : services de renseignement et de sécurité intérieure, professionnels de l'information et de l'éducation, acteurs publics et privés de la cybersécurité.

En Belgique, « la menace est prise très au sérieux par le gouvernement », assurait jeudi le ministre de l'Intérieur, Bernard Quintin (MR), à la Chambre. Si un Conseil national de sécurité, qui doit « justement déboucher sur des mesures supplémentaires », est en cours de préparation par tous les services de sécurité et de renseignement, la réponse à ces enjeux doit se faire au niveau européen, « mais aussi avec les Américains et d'autres alliés », assure le libéral.

4

La population doit-elle s'inquiéter ?

« Ne pas considérer ces incidents comme une véritable guerre est une grave erreur », estime Roger Housen. Selon lui, une approche trop défensive risque de laisser aux acteurs hybrides « une longueur d'avance ». Il plaide pour que les Européens définissent plus clairement leurs « lignes rouges » et adoptent une stratégie plus affirmée, pouvant aller jusqu'à des mesures de rétorsion contre la Russie, notamment dans le cyberespace ou sur le terrain de l'information.

Samuel Longuet reconnaît l'existence d'actions de déstabilisation visant la Belgique et l'Europe susceptibles, selon lui, d'être coordonnées par la Russie. Mais il appelle à relativiser leur impact sur la vie quotidienne : « La population doit être consciente qu'il existe des actions entreprises contre la Belgique, mais ça ne veut pas dire pour autant qu'il faut bouleverser nos modes de vie. » Pour le chercheur, les citoyens doivent surtout rester vigilants : vérifier et croiser leurs sources, adopter de bons réflexes en matière de cybersécurité et ne pas céder à la peur.

Face aux députés, le ministre de l'Intérieur a annoncé que la deuxième phase d'information à la population menée par le Centre de crise national, dans le but de « relever la résilience de la société », serait bientôt entamée. « Notre société doit absolument renforcer sa culture de sécurité », défend Bernard Quintin. « Tout le monde a une responsabilité à prendre : le niveau politique et les services de sécurité, évidemment, mais notre population aussi. »

Les actions hostiles de la Russie sur le sol européen au menu de la réunion des ministres de la Défense

Il n'y a pas que sur les villes d'Ukraine que la Russie intensifie ses attaques. Les responsables européens constatent aussi, ces derniers mois, une solide escalade de la campagne d'actions hostiles attribuée à Moscou sur le sol même de l'Union européenne. « Une affaire sérieuse, une menace qui prend rapidement de l'ampleur », reconnaît un haut responsable de l'UE. Ces violations à répétition de l'espace aérien, ces actes de sabotage ou encore le « flux incessant de désinformation russe » dénoncé par l'UE seront au menu de la réunion, ce lundi, des ministres européens de la Défense.

La lutte contre ces attaques « hybrides » à caractère parfois « kinétique », comme la tentative d'attentat sur l'aéroport de Leipzig en août, est avant tout du ressort du pays visé : « A eux de calibrer la réponse », reprend le responsable de l'UE. Mais les Européens pourraient décider de réagir collectivement à ces attaques qui, « sans aller jusqu'à constituer une agression armée, menacent clairement notre sécurité », comme le disait la présidente de la Commission, Ursula von der Leyen, lors de son discours de rentrée.

Von der Leyen avançait ainsi l'idée d'un « protocole de sécurité d'urgence », afin de « coordonner une réponse européenne » en cas d'action hostile. Les Etats membres attendent d'y voir plus clair avant de donner leur feu vert, et certains, dont la Belgique, se méfieront d'un « doublon » avec l'Otan. Mais cette piste, parmi d'autres, y compris l'utilisation des « outils existants » (les sanctions, notamment), devrait être discutée ce lundi. La réunion doit aussi conduire au partage d'informations sur les événements des deux derniers mois.

PH.R.