Le Monde
DIMANCHE 23 - LUNDI 24 OCTOBRE 2022

Ukraine L'extension hybride du domaine de la guerre

L'explosion inexpliquée des gazoducs Nord Stream 1 et 2, fin septembre, nourrit les préoccupations sur les actions non conventionnelles que la Russie pourrait mener contre les alliés occidentaux de Kiev. Plusieurs alertes sont survenues ces derniers mois en Europe, au fil des revers subis par Moscou sur le terrain

Un tube d'acier éventré et une tranchée creusée dans la vase, à quelque 80 mètres de fond… Ces images, filmées par un robot piloté à distance dans les eaux sombres de la mer Baltique et publiées, le 18 octobre, par le quotidien suédois *Expressen*, donnent un aperçu des dégâts provoqués par les explosions, survenues le 26 septembre, sur les deux gazoducs Nord Stream reliant l'Allemagne à la Russie pour alimenter l'Europe en hydrocarbures. Une fois balayée par les sismologues l'éventualité d'un tremblement de terre, les allégations de « sabotage » ont fusé. Les capitales européennes soupçonnent Moscou ; le Kremlin accuse la centrale du renseignement américain – le tout sur fond de « bataille du gaz », la Russie réduisant au fil des semaines ses exportations énergétiques vers les Etats européens, qui redoutent des pénuries cet hiver.

Si elles mettent en lumière la vulnérabilité des infrastructures stratégiques européennes, ces images permettent aussi une plongée inédite dans « la guerre dans la guerre » qui se profile, en marge des combats en cours en Ukraine : l'extension possible aux alliés de Kiev, sous une forme « hybride », du conflit déclenché par Moscou. *« Il s'agit d'une nouvelle dimension dans la guerre, plus seulement contre l'Ukraine, mais dans le contexte plus large de la confrontation entre la Russie et l'Ouest »*, estime Arsalan Bilal, chercheur associé à l'université arctique de Norvège sur les questions de sécurité. *« L'idée,* poursuit-il, *est à la fois d'étrangler l'Europe et de creuser le fossé entre les opinions publiques et les gouvernements, en jouant de l'arme énergétique pour affaiblir les économies dépendant du pétrole et du gaz, et inciter une partie des populations à demander la fin des combats et l'ouverture de négociations. »*

UN « ACTE DÉLIBÉRÉ »

Les explosions spectaculaires sur le Nord Stream sont loin d'être élucidées, mais de premiers éléments accréditent la thèse selon laquelle seul un acteur étatique peut en être à l'origine : il s'agit d'un *« acte délibéré »*, rapporte un document conjoint de la Suède et du Danemark remis le 30 septembre aux Nations unies, commis à l'aide *« d'engins explosifs d'une puissance équivalente à 500 kilos de TNT »*, selon des informations recueillies la veille par *Der Spiegel* auprès des autorités allemandes. Et quel que soit le coupable, les dommages sont d'ores et déjà considérables. Outre les conséquences environnementales du rejet colossal de méthane dans l'atmosphère et les doutes qui planent désormais sur la remise en fonctionnement – à moyen ou long terme – de ces gazoducs, le sentiment d'insécurité grandit dans de nombreux pays, européens pour la plupart, récemment victimes d'attaques de type « hybride ».

Le terme de « guerre hybride » (*hybrid warfare*) – selon une définition encore mal établie et dont les contours flous ne cessent de s'élargir depuis son apparition aux Etats-Unis, sous la plume de Robert H. Walker, officier américain des marines, en 1998 – désigne la combinaison coordonnée d'outils militaires conventionnels et non conventionnels (acteurs non étatiques, sabotages, cyberattaques) et de méthodes subversives (désinformation, trolling, etc.). Son objectif est de déstabiliser un adversaire et de lui infliger le maximum de dommages sur les plans sécuritaire, économique, politique, énergétique. Sa particularité tient aussi à son caractère ambigu : l'auteur de ces actions et leur commanditaire agissant dans l'ombre, ils sont souvent difficiles à identifier, ce qui complique la tâche des pays ciblés lorsqu'il s'agit d'y répondre.

L'explosion des tubes de Nord Stream ne constitue pas la première alerte. Dès le mois de janvier, les services de renseignement occidentaux s'étaient alarmés d'une attaque perpétrée en Norvège contre un câble en fibre optique alimentant SvalSat, la plus grande station de réception de données satellitaires au monde, installée dans l'archipel du Svalbard et utilisée, notamment, par la NASA et l'Agence spatiale européenne. Cette coupure, liée à *« une intervention extérieure »*, selon la police norvégienne, n'avait pas entraîné de rupture des communications, car un second câble avait pu prendre le relais. Mais deux mois ont été nécessaires pour réparer le lien endommagé. *« Cette opération ressemble à un test grandeur nature, destiné à s'assurer de la faisabilité du sabotage d'un câble de télécommunication sous-marin »*, juge François Heisbourg, conseiller pour l'Europe de l'International Institute for Strategic Studies, à Londres. Quelques mois plus tôt, en novembre 2021, un autre incident s'était produit sur le réseau sous-marin LoVe (Lofoten-Vesteralen), destiné à surveiller les passages de submersibles en mer de Norvège, sans que l'on puisse là non plus en attribuer l'origine.

La menace, s'accordent les experts – qui se gardent d'identifier formellement un coupable –, est montée en puissance au fur et à mesure des revers subis sur le terrain ukrainien par les forces russes. *« Sur le plan militaire, la Russie est coincée en Ukraine ; elle ne pourra pas lancer de nouvelle offensive avant trois ou quatre mois. Vladimir Poutine n'a donc d'autre choix que de mondialiser la guerre,* tranche François Heisbourg. *Pour cela, il dispose de deux options : le nucléaire ou la guerre hybride. Cette dernière lui permet d'élargir le champ de la lutte sans pour autant se mettre en péril, à la différence de l'arme atomique. »* C'est d'ailleurs l'un des effets recherchés de ces pratiques, qui, pour être efficaces et à moindre coût, doivent rester en deçà du seuil à partir duquel elles seraient assimilées à des agressions armées.

L'OTAN, qui s'est penchée à plusieurs reprises sur la question des « menaces hybrides » au cours de la décennie 2010, s'est attelée à s'équiper de moyens de prévention et de dissuasion, sans parvenir à définir un mécanisme de réponse. *« Le but* [des activités hybrides] *est de rendre plus ardue la distinction entre guerre et paix, et de semer le doute dans l'esprit des populations qui sont prises pour cible. Ces activités visent à déstabiliser et à ébranler la société »*,explique-t-on sur le site officiel de l'Alliance atlantique. *« C'est au pays contre lequel est dirigée une menace ou une attaque hybride qu'il incombe d'agir en premier ressort »*, y est-il indiqué. Est également rappelée une déclaration publique de l'OTAN, datant de 2016, selon laquelle *« ses pays membres pourraient décider d'invoquer l'article 5 du Traité de l'Atlantique Nord si un ou plusieurs d'entre eux étaient la cible d'activités hybrides »*.

Un conditionnel qui montre ses limites à l'heure où la menace devient prégnante et d'autant plus diffuse que l'origine des attaques est complexe à établir, ou réservée à la connaissance de la seule communauté du renseignement. *« Cela ne vaut pas toujours la peine d'attribuer l'action à un Etat. D'abord, il faut être en mesure d'en apporter la preuve, ce qui peut impliquer d'exposer ses sources et ses méthodes. Ensuite, cela peut pousser les gouvernements* [ciblés] *à réagir, alors qu'ils sont déjà sous pression »*, relève Maxime Lebrun, chercheur au Centre d'excellence européen pour la lutte contre les menaces hybrides, un organe de recherche implanté à Helsinki, placé sous la tutelle de l'OTAN et de l'Union européenne. *« Une attaque hybride crée toujours de l'inconfort stratégique »*, ajoute-t-il.

« LA GUERRE HYBRIDE PERMET D'ÉLARGIR LE CHAMP DE LA LUTTE SANS POUR AUTANT SE METTRE EN PÉRIL, À LA DIFFÉRENCE DE L'ARME ATOMIQUE »

FRANÇOIS HEISBOURG
conseiller pour l'Europe de l'International Institute for Strategic Studies

Cet *« inconfort stratégique »* s'est intensifié et, surtout, élargi à l'ensemble de l'Europe au moment où le président russe a paru entamer une inéluctable fuite en avant. Après plusieurs semaines d'humiliantes déconvenues militaires face à la redoutable contre-offensive ukrainienne, Vladimir Poutine a provoqué un choc dans son propre pays en décrétant, le 21 septembre, la mobilisation de 300 000 réservistes russes. Il a resserré son emprise en scellant officiellement, le 30 septembre, l'annexion des régions de Louhansk, Donetsk, Kherson et Zaporijia, en partie occupées par ses troupes et soumises, depuis le 19 octobre, à la loi martiale. Et haussé le ton contre les soutiens de Kiev, en brandissant la menace d'une confrontation nucléaire.

Dans cette même période, entre fin septembre et début octobre, plusieurs vols de drones inhabituels sont observés par le Danemark, à plus de 200 kilomètres à l'ouest de ses côtes, en mer du Nord, près des champs gaziers Halfdan B et Roar, tous deux exploités par le groupe français TotalEnergies. Sans que soit établie de relation de cause à effet, la Norvège annonce l'arrestation de sept ressortissants russes, accusés d'avoir fait illégalement voler des drones ou d'avoir violé des interdictions de photographier dans le royaume. En Allemagne, le 8 octobre, le trafic ferroviaire est paralysé dans la moitié nord du pays. En cause, deux câbles sectionnés, en même temps, à 540 kilomètres de distance : *« un sabotage d'origine étatique est envisageable »*, selon un rapport de la police judiciaire allemande (Bundeskriminalamt), dont des extraits sont révélés, dès le lendemain, par le quotidien *Bild*.

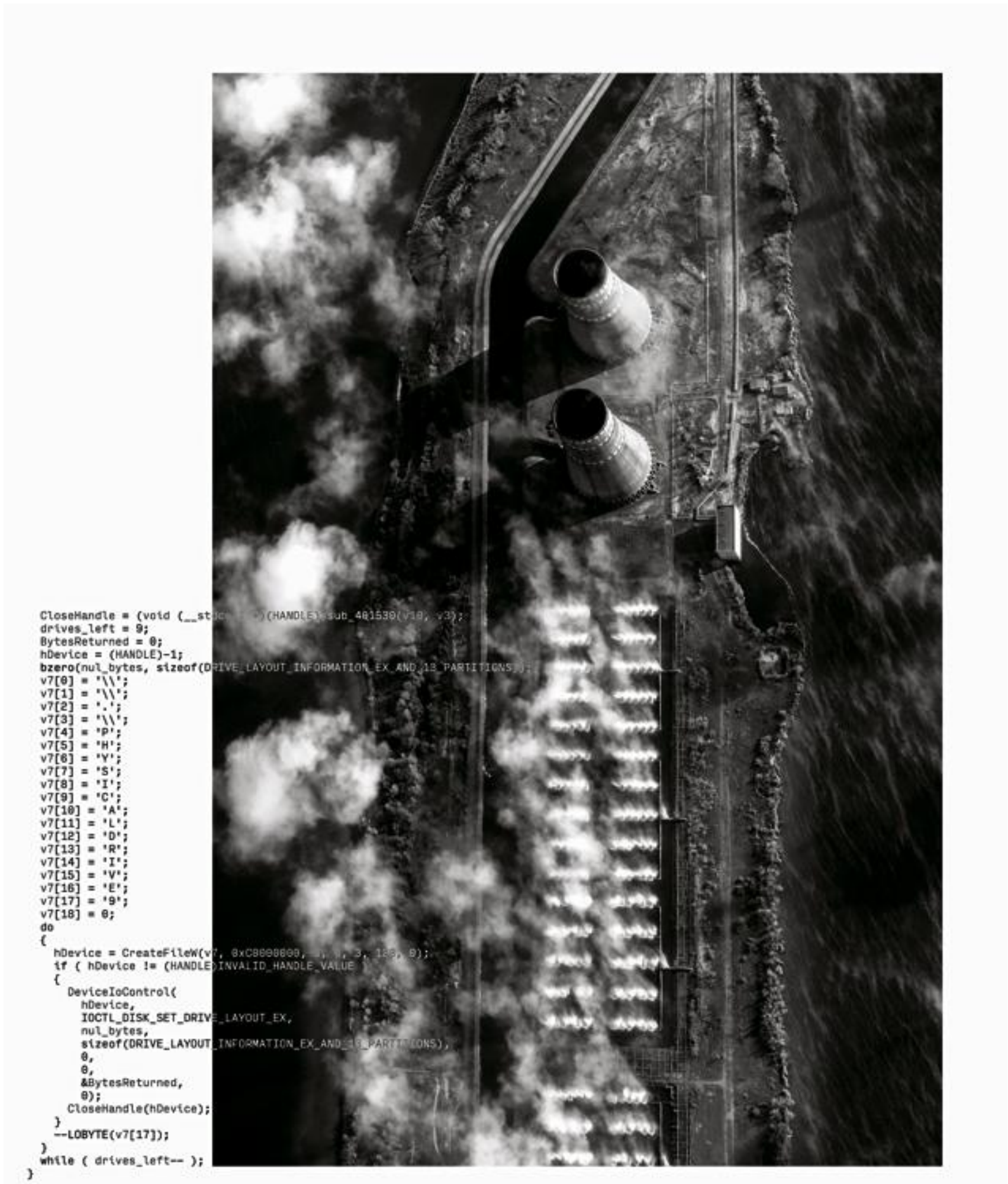
Le 10 octobre, non loin des lieux des déflagrations sur les gazoducs Nord Stream, l'île danoise de Bornholm est victime d'une coupure générale d'électricité. L'opérateur danois Energinet a finalement indiqué qu'il s'agissait d'une *« panne locale »*. Le même jour, de l'autre côté de l'Atlantique, des cyberattaques, attribuées à un groupe de hackeurs prorusses baptisé « Killnet », bloquent les sites Internet de plusieurs grands aéroports américains – notamment à Atlanta, Chicago, Los Angeles, New York et Denver. Plus que de menaces graves pour la sécurité, ces attaques sont qualifiées de *« nuisances publiques »* par John Hultquist, vice-président du renseignement chez Mandiant, une société américaine de cybersécurité, qui ajoute que celles-ci restent très *« efficaces pour attirer l'attention du public »*.

UN MIROIR AUX ALOUETTES

Influencer les opinions publiques occidentales, peser sur les choix de leurs dirigeants… A écouter les analystes, tel serait aujourd'hui l'objectif du maître du Kremlin. Selon Arsalan Bilal, c'est dans cette optique qu'il faut analyser l'attitude de Vladimir Poutine au cours du récent sommet de la Conférence sur l'interaction et les mesures de confiance en Asie, à Astana, au Kazakhstan. En suggérant, le 13 octobre, à son homologue turc, Recep Tayyip Erdogan, de *« transférer vers la mer Noire les volumes perdus du gazoduc Nord Stream qui transitaient auparavant par la Baltique »* et en lui promettant *« davantage de gazoducs sous-marins »*, le président russe a laissé miroiter à la Turquie un avenir de plaque tournante du gaz. Un miroir aux alouettes, peut-être, mais une proposition aussitôt acceptée par ce membre de l'OTAN aussi turbulent que précieux, à un moment où les Européens cherchent désespérément à se débarrasser de leur dépendance aux hydrocarbures russes.

Jeudi 20 octobre, c'est encore un câble sous-marin reliant les îles Shetland à l'Ecosse qui est rompu, privant les 23 000 habitants de l'archipel d'Internet et de services téléphoniques. Un *« incident majeur »*, selon le groupe British Telecom, leader dans le secteur au Royaume-Uni.

La menace est prise très au sérieux par les gouvernements occidentaux, car Moscou dispose d'importants moyens d'action pour pousser ses pions, en particulier dans la mer Baltique appelée à devenir, au large des côtes russes, un vaste « lac otanien » dans la perspective de l'adhésion de la Finlande et de la Suède à l'Alliance atlantique. La direction principale de la recherche en eaux profondes, connue sous l'acronyme GUGI (*Glavnoye Upravleniye Glubokovodnykh Issledovaniy*) et rattachée au ministère de la défense russe, possède des navires océanographiques et des sous-marins susceptibles d'espionner les



Le travail « Cyberguerre » du photographe indépendant **Michel Slomka** traite de la série de cyberattaques ayant eu lieu en Ukraine la veille de l'invasion russe, le 23 février 2022, à 17 heures, sur les systèmes informatiques d'un grand nombre d'acteurs institutionnels et économiques ukrainiens. Il superpose des images satellites recueillies par Maxar Technologies et l'analyse des lignes des codes des malwares récupérés par une multitude d'acteurs de la cybersécurité, dont SentinelLabs (une division de recherche sur les risques cyber de SentinelOne), qui décrivent le fonctionnement et la nocivité des logiciels « wipers », destinés à détruire un système informatique. Ces représentations des villes de Kiev, de l'aciérie de Marioupol et de la centrale nucléaire de Zaporijia (photo ci-contre) soulignent que le cyberespace connecte les infrastructures vitales d'un pays, qui sont désormais un théâtre d'opération à part entière, en parallèle du conflit militaire.

communications transitant par les câbles sous-marins, mais aussi de mener des actions hostiles dans les abysses – jusqu'à 6 000 mètres de profondeur – grâce à des drones et à des « hydronautes » considérés comme l'élite de la marine russe.

Le navire océanique russe *Yantar* a ainsi été repéré à plusieurs reprises,naviguant à proximité de câbles numériques sous-marins stratégiques. A l'été 2021, sa trajectoire avait suscité l'inquiétude en épousant le tracé des câbles Celtic Norse et AEConnect-1, qui relient respectivement l'Irlande à l'Ecosse et aux Etats-Unis. L'arsenal du GUGI a été renforcé, en juillet, par la livraison du *Belgorod,* un sous-marin de 184 mètres, présenté comme le plus long de la planète. *« Pour vaincre "l'Occident collectif", il suffit à la Russie de couper l'un des vingt câbles de données situés dans l'Atlantique, et elle en a la capacité »*,prévient François Heisbourg.

« ÉVEILLER LES CONSCIENCES »

Près de 99 % des échanges Internet et de téléphonie mobile transitant par les câbles sous-marins, une rupture *« aurait des conséquences extrêmement dramatiques »*, a souligné Stéphane Bouillon, secrétaire général français de la défense et de la sécurité nationale (SGDSN), devant la commission des affaires étrangères, de la défense et des forces armées du Sénat, le 5 octobre. *« La destruction d'éléments des gazoducs Nord Stream 1 et 2 démontre que les infrastructures civiles (satellites, câbles…) sont des cibles pour des Etats sans scrupule. Parallèlement, le prix des hydrocarbures et les risques de pénurie d'énergie sont des moyens de pression utilisés par la Russie sur les populations européennes. Nous travaillons donc à organiser les choses de façon que, par exemple, d'éventuels délestages* (…) *n'aient pas d'effets mal maîtrisés »*, a indiqué Stéphane Bouillon. La question doit être abordée dans la future loi de programmation militaire, dont la présentation est prévue en 2023.

Si la multiplication des attaques protéiformes et la gravité des explosions sur les gazoducs de la Baltique ont eu pour effet de révéler l'ampleur de la menace, les capitales européennes sont-elles prêtes à y faire face ? *« Les Occidentaux sont assez peu préparés à la guerre hybride, car ils n'envisageaientpas jusqu'alors qu'un adversaire entre dans leur sanctuaire,* confie une source au sein de l'état-major français. *La défense opérationnelle du territoire a un rôle important à jouer en matière de cyber, de contre-ingérence, etc. Mais il faut surtout éveiller les consciences. Quand Internet sera coupé, il sera trop tard ! Il faut préparer les esprits à la guerre hybride, et il y a beaucoup de travail à faire. »*

Ces propos alarmistes ne font cependant pas l'unanimité parmi les experts. *« Je ne pense pas que l'on soit à un tournant en matière d'hybridité. La perspective d'un prolongement de la guerre sous le seuil de la violence armée est à relativiser, la guerre de haute intensité continue en Ukraine,* estime ainsi Maxime Audinet, chercheur à l'Institut de recherche stratégique de l'école militaire, spécialiste de la guerre informationnelle russe. *En revanche, il semble bien y avoir une escalade dans l'usage de certaines méthodes "hybrides", avec des opérations de sabotage et une conflictualité informationnelle rarement égalée. »*

« TOUT EST DEVENU UNE ARME : L'ÉNERGIE, LES INVESTISSEMENTS, L'INFORMATION, LES FLUX MIGRATOIRES, LES DONNÉES »
JOSEP BORRELL
haut représentant de l'UE

« Les opérations menées par la Russie ne semblent ni assez nombreuses ni assez fortes pour avoir un effet stratégique réel. Moscou a une perception erronée de la fragilité occidentale, modère Léo Péria-Peigné, spécialiste des questions militaires et chercheur à l'Institut français des relations internationales. *La guerre hybride a un effet théorique intéressant, mais qui reste à démontrer dans la pratique. C'est un concept qu'il faut manier avec précaution. »*

Bien avant l'invasion du 24 février, dans le contexte de l'annexion unilatérale de la Crimée par Moscou en 2014 et des premiers combats dans les régions séparatistes du Donbass, l'Ukraine a été le théâtre privilégié des opérations de déstabilisation lancées par son voisin. Du déploiement de mercenaires aux techniques de désinformation, en passant par le chantage énergétique, ce pays est souvent considéré comme un cas d'école, un laboratoire de la guerre hybride menée par la Russie. *« A certains égards,* poursuit Léo Péria-Peigné, *on pourrait même considérer que la guerre en Ukraine témoigne de l'échec de la guerre hybride, puisque l'essentiel des gains et des pertes de cette guerre est réalisé par des moyens conventionnels. »*

Il n'empêche, avant le Conseil européen des 20 et 21 octobre, à Bruxelles, la Commission a réitéré son appel à *« une action urgente »* pour renforcer la résilience des infrastructures critiques dans trois domaines jugés prioritaires : l'énergie, le numérique et l'espace. Elle recommande notamment aux gouvernements de mener des *« stress tests »*, afin de mettre à l'épreuve les équipements essentiels – la liste des sites sensibles doit bien sûr demeurer confidentielle. La menace hybride figurait déjà au cœur de la « boussole stratégique » adoptée au printemps par les Vingt-Sept en vue de renforcer leur défense commune.

« Tout est devenu une arme : l'énergie, les investissements, l'information, les flux migratoires, les données », a rappelé Josep Borrell lors d'un vibrant discours adressé, le 10 octobre, aux ambassadeurs européens. A propos de la guerre informationelle, le haut représentant de l'Union européenne les a encouragés à *« s'engager davantage dans la bataille des narratifs ». « Ce n'est pas secondaire ; on ne remporte pas les guerres en envoyant seulement des tanks, des missiles ou des troupes,* a-t-il martelé. *C'est un grand combat : qui va gagner les esprits et les âmes des gens ? »* ■

CÉDRIC PIETRALUNGA, PHILIPPE RICARD ET ÉLISE VINCENT