Déjouer le brouillard informationnel : l'attribution comme outil de résilience et de dissuasion de l'OTAN

Angèle Billaud

Analyste en droit international, sécurité internationale, cybersécurité et défense, diplômée de l'Université Grenoble Alpes, France.

16 décembre 2025

ISSN : 2739-3283

Comment citer cette publication :

Angèle Billaud, *Déjouer le brouillard informationnel : l'attribution comme outil de résilience et de dissuasion de l'OTAN,* Institut d'études de géopolitique appliquée, Paris, 16 décembre 2025.

Institut d'études de géopolitique appliquée
66 avenue des Champs-Élysées, 75008 Paris
Courriel : secretariat@institut-ega.org - Site internet : www.institut-ega.org

AVERTISSEMENT

Déjouer le brouillard informationnel : l'attribution comme outil de résilience et de dissuasion de l'OTAN

L'Institut d'études de géopolitique appliquée (Iega) est l'un des *think tanks* français de référence dans l'analyse des relations internationales. Depuis sa fondation, l'Iega est guidé par la volonté d'associer société civile, acteurs institutionnels et scientifiques dans le domaine de l'analyse géopolitique. Guidé par le souci d'indépendance et d'objectivité tout autant que par l'aspect humain, il œuvre en ce sens à travers la publication de travaux scientifiques en libre-accès, ainsi que par l'organisation d'événements et de formations accessibles au plus grand nombre.

Cette étude est publiée dans le cadre du programme *Jeunes chercheurs* de l'Institut d'études de géopolitique appliquée, en partie financé par la Direction générale des relations internationales et de la stratégie (Dgris) du ministère français des Armées.

Les opinions exprimées dans ce texte n'engagent que la responsabilité de l'auteure.

ISSN : 2739-3283

Institut
EGA

Sommaire

Introduction

À l'ère des manipulations informationnelles, la capacité d'une organisation militaire à distinguer le vrai du faux conditionne directement sa cohésion interne et son efficacité opérationnelle. Les attaques informationnelles, qu'elles prennent la forme d'intrusions numériques, de falsifications de contenus ou d'opérations psychologiques, cherchent avant tout à introduire le doute. Ce doute affecte ensuite la lisibilité de la situation, fragilise la chaîne de commandement et complique la prise de décision. Au sein d'une alliance multinationale comme l'OTAN, où trente-deux États sont amenés à interpréter simultanément des signaux, à partager leurs analyses et à agir de manière coordonnée, cette vulnérabilité est amplifiée.

Dans ce contexte, l'attribution joue un rôle central. Il s'agit de la capacité à identifier l'auteur d'une attaque à partir de preuves techniques, opérationnelles et stratégiques[1]. Elle ne fait pas disparaître les ingérences, mais permet d'en restaurer la compréhension, de réduire l'incertitude et de consolider la confiance, laquelle constitue non pas un simple état psychologique, mais un prérequis fonctionnel à la coordination militaire.

Les campagnes de manipulation actuelles, amplifiées par les réseaux sociaux, visent à créer une forme d'« isolement cognitif ». L'objectif est de brouiller les repères d'une population et de compromettre la lecture fiable des événements, affaiblissant ainsi la cohésion nationale, la confiance dans les institutions et la capacité de défense. Autrement dit, il s'agit de couper la population, et par extension l'État, d'informations fiables afin de la maintenir dans une bulle de manipulation et de contrôler le récit. Le conflit russo-ukrainien en fournit un exemple emblématique : depuis 2014, la diffusion de deepfakes de responsables militaires, les défacements de sites officiels et la pollution volontaire des flux d'information ont érodé la confiance de la population envers les institutions, fragmenté les perceptions et entravé la prise de décision[2].

Dans la sphère militaire, une armée dont les capteurs sont saturés de signaux falsifiés, dont les personnels doutent de l'authenticité d'un ordre ou dont les alliés suspectent une compromission se trouve affaiblie dans sa réactivité stratégique. Au sein d'une alliance multinationale, l'incertitude informationnelle se transforme alors en une arme susceptible de provoquer une paralysie opérationnelle collective.

[1] Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe, *Opportunities for Public and Private Attribution of Cyber Operations*, Tallinn Paper No. 12, CCDCOE, 2021, p. 5

[2] CSS CYBER DEFENSE PROJECT, *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict*, Risk and Resilience Team, Center for Security Studies (CSS), Zürich, October 2018.

Face à ce risque, l'OTAN est confrontée à un défi central : comment restaurer et maintenir la confiance dans la chaîne de commandement et entre Alliés ? Développer une capacité nationale et otanienne d'attribution fiable, constante et largement reconnue apparaît comme une première voie à explorer.

L'attribution comme condition de la confiance opérationnelle au sein de l'OTAN

Pour l'OTAN, l'enjeu fondamental est d'éviter ce que l'on pourrait qualifier de « paralysie du doute ». En effet, l'Alliance repose sur la confiance mutuelle entre ses Membres et sur l'interopérabilité des forces, ce qui la rend particulièrement vulnérable à cette éventualité. Les attaques hybrides contemporaines créent un brouillard informationnel qui vise précisément à produire des divergences d'interprétation entre États Membres. Lorsque le doute s'installe, la décision se fragilise, les analyses se fragmentent et la cohérence stratégique s'affaiblit. La manipulation de l'information devient alors une arme de déstructuration interne de l'Alliance.

Dans l'affaire CyberCaliphate, la Russie avait agi sous fausse bannière, se faisant passer pour un groupe iranien soutenant l'État islamique[3]. Initialement attribuée à l'Iran, puis finalement reliée à la Russie, cette manœuvre illustre comment l'incertitude sur la source d'une information peut réorienter les suspicions et les réponses stratégiques. Cette incertitude aurait pu conduire les Alliés à adopter des postures stratégiques et politiques divergentes, voire contradictoires, rompant ainsi la cohésion de l'Alliance et sa crédibilité sur la scène internationale.

À l'inverse, plusieurs cas récents démontrent qu'une attribution réussie renforce la cohésion. L'attaque NotPetya de 2017 a donné lieu à une attribution collective à la Russie par plusieurs États Membres, ce qui a permis d'affirmer une posture diplomatique synchronisée et a notamment conduit à l'adoption de sanctions à l'encontre des entités responsables par le Conseil de l'UE[4]. Dans l'affaire SolarWinds en 2020, la coopération analytique entre plusieurs Alliés a donné lieu à une déclaration du Conseil de l'Atlantique Nord appuyant l'attribution

[3] Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe, *Opportunities for Public and Private Attribution of Cyber Operations*, op.cit., p. 12
[4] Conseil de l'Union européenne, L'UE impose les toutes premières sanctions à la suite de cyberattaques, communiqué de presse, 30 juillet 2020.

émise par les États-Unis[5]. Ces exemples montrent que l'attribution, lorsqu'elle est collective et publiquement reconnue, consolide la solidarité et la confiance interalliée.

Comprendre la portée stratégique de l'attribution nécessite de distinguer trois niveaux interdépendants : technique, stratégique et politique[6]. L'attribution technique consiste à identifier les outils, les infrastructures et les signatures numériques d'une attaque, en s'appuyant notamment sur l'analyse forensique, c'est-à-dire la reconstruction précise des mécanismes techniques employés. L'attribution stratégique vise à comprendre les motivations, les intérêts et les comportements des acteurs soupçonnés, grâce à des renseignements provenant de sources militaires, diplomatiques ou économiques. Enfin, l'attribution politique consiste à décider de rendre cette attribution publique, décision qui fonde la légitimité d'une riposte diplomatique, économique ou juridique[7] et réduit mécaniquement la probabilité d'impunité.

Une capacité d'attribution robuste augmente ainsi le coût stratégique des opérations hostiles[8]: elle rend visible ce que les adversaires cherchent à maintenir dans l'ombre. De ce fait, l'attribution constitue un outil de dissuasion non négligeable, en démontrant la capacité d'un acteur à éclairer les zones opaques de la conflictualité contemporaine. Cependant, cette capacité n'est crédible que si elle repose sur une validation publique significative, elle-même liée à la fiabilité de l'attribution. Cette dernière exige une combinaison rigoureuse des deux premiers niveaux d'attribution, c'est-à-dire des indicateurs techniques et stratégiques[9]. La dimension publique de l'attribution impose, quant à elle, un équilibre délicat : il faut révéler suffisamment de preuves pour emporter l'adhésion, sans pour autant compromettre des sources sensibles ou des capacités de renseignement[10].

Si l'attribution fiable est un exercice ardu, c'est précisément cette complexité qui en fait un marqueur stratégique. Elle atteste de la maîtrise technique, technologique et analytique de l'acteur qui l'énonce et contribue ainsi à renforcer ses capacités dissuasives. Par ailleurs, parmi les réponses initiales envisageables face à une attaque de cette nature, le Centre d'excellence pour la cyberdéfense en coopération de l'OTAN (CCDCOE) souligne que l'attribution constitue la réponse la plus pertinente à privilégier[11].

Une attribution crédible, expliquée et documentée de manière transparente, contribue à renforcer la confiance interalliée. En restaurant la lisibilité de l'environnement, elle atténue l'impact de l'isolement cognitif et réaffirme la stabilité de la chaîne de commandement. De ce fait, en démontrant que l'OTAN est capable de rétablir la vérité opérationnelle dans un

[5] OTAN, Déclaration du Conseil de l'Atlantique Nord suite à l'annonce par les États-Unis de mesures concernant la Russie, 15 avril 2021.
[6] Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe, *Opportunities for Public and Private Attribution of Cyber Operations*, op. cit.
[7] *Id*. p. 5.
[8] *NATO's approach to counter information threats*, Endorsed by Allied Defence Ministers on 18 October 2024.
[9] Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe, *Opportunities for Public and Private Attribution of Cyber Operations*, op. cit., p. 6.
[10] *Ibid*.
[11] *Ibid*.

environnement saturé de falsifications, l'attribution rassure tant les personnels militaires que les populations civiles, en montrant qu'aucune ingérence informationnelle ne peut durablement obscurcir la compréhension de la menace.

Il convient néanmoins de préciser le rôle exact de l'OTAN dans ce domaine. Contrairement aux États, l'Alliance ne dispose pas d'une compétence souveraine en matière d'attribution[12]. Elle ne peut pas, à elle seule, attribuer une attaque à un acteur étatique. Elle dépend des évaluations nationales, du renseignement intégré et des analyses menées notamment par le CCDCOE. En revanche, elle peut publier une position collective, dont la portée politique est considérable. L'attribution au sein de l'OTAN est donc moins un acte isolé qu'un processus coordonné, fondé sur la convergence analytique et diplomatique des États Membres.

Dans un contexte où l'information est continuellement contestée, la capacité d'attribution de l'OTAN, fiable, constante et reconnue comme telle, apparaît comme un levier indispensable pour garantir la confiance à chaque échelon de la chaîne de commandement. Elle constitue l'une des conditions de la résilience opérationnelle et structurelle de l'Alliance dans un environnement stratégique façonné par le doute et les manipulations.

Bâtir une capacité d'attribution nationale et otanienne comme pilier de résilience

Extension moderne des principes fondateurs de l'OTAN, la résilience repose sur la capacité de chaque Membre à renforcer individuellement et collectivement sa résistance[13]. Le renforcement de l'attribution s'inscrit pleinement dans cette logique.

La consolidation des capacités techniques nationales constitue une première étape essentielle. L'attribution requiert une expertise avancée en analyse forensique, en renseignement multi-sources et en étude des modes opératoires adverses[14], impliquant le développement de formations professionnelles et universitaires capables de réduire l'écart entre les ressources humaines disponibles et la force nécessaire. Le secteur privé joue également un rôle central dans cette dynamique. Le CCDCOE estimait en 2021 que 65 % des attributions provenaient du secteur privé, 25 % du secteur public et 10 % d'une combinaison

[12] OTAN, Communiqué du sommet de Bruxelles, 14 juin 2021
[13] Edward Hunter Christie and Kristine Berzina, *NATO and Societal Resilience: All Hands on Deck in an Age of War,* Policy Brief, GMF, 2022, p.2 ; Article 3, Traité de l'Atlantique Nord, 4 avril 1949
[14] NATO, *Allied Joint Doctrine for Cyberspace Operations*, AJP – 3.20, 2020, p. 13.

des deux[15]. L'apport des acteurs privés est précieux, car ils disposent souvent de davantage de ressources humaines, financières et technologiques, ainsi que d'une visibilité privilégiée sur les infrastructures numériques et les activités dans le cyberespace. Le secteur privé constitue ainsi un appui essentiel à la capacité d'attribution d'un État, comme l'illustre l'analyse du CCDCOE : en 2021, la quasi-totalité des opérations cyber offensives attribuées à un État reposaient sur un partenariat public-privé[16].

Toutefois, la coopération avec le secteur privé impose une articulation claire entre expertise privée et attribution publique, compte tenu des conséquences diplomatiques, économiques ou militaires potentielles. Si certains craignent que les faisceaux d'indices issus du secteur privé ne soient pas toujours entièrement fiables, risquant de provoquer des tensions internationales[17], un cadre structuré permet de canaliser ces contributions. L'État conserve alors le monopole de la décision politique d'attribution, assurant que sa publicité tienne compte des informations confidentielles et des risques stratégiques à l'échelle internationale. En définissant clairement les rôles respectifs, un État peut bénéficier de l'expertise privée pour renforcer la fiabilité de l'attribution, tout en préservant la légitimité et l'avantage de l'attribution publique.

Renforcer l'attribution implique également de développer à l'échelle nationale une véritable résilience cognitive. Celle-ci permettrait notamment de concentrer les efforts sur les attaques sophistiquées et d'éviter une dilution des moyens face à une multitude de campagnes de moindre envergure. La défense psychologique, par exemple, est un concept qui vise à préserver la capacité de discernement, la stabilité du moral et la résistance aux manipulations, tant au sein de la population qu'au sein des forces armées[18]. Le modèle suédois, avec son Agence de défense psychologique, illustre ce que peut offrir une approche institutionnalisée : éducation informationnelle, détection des narratifs hostiles, sensibilisation du public au fonctionnement de la propagande[19]. Un tel dispositif permet notamment aux militaires de transposer, dans leurs missions, les réflexes de prudence et la conscience critique face aux signaux informationnels douteux, acquis dans la sphère civile.

Enfin, la mise en place d'une harmonisation OTAN constitue une étape indispensable. Les États Membres s'appuient aujourd'hui sur des méthodologies, des définitions et des seuils de preuves hétérogènes. Or l'efficacité de l'attribution dépend d'une large reconnaissance. Son absence à l'échelle interne renvoie l'image du doute mutuel des Alliés sur la fiabilité de leurs attributions respectives, affaiblissant leur cohésion, leur crédibilité, leur force de dissuasion et leurs capacités opérationnelles à l'extérieur de l'OTAN. L'établissement d'une taxonomie commune, de standards forensiques partagés, de processus conjoints d'examen et de validation, ainsi que de seuils de preuve harmonisés, conférerait une légitimité supplémentaire aux

[15] Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe, *Opportunities for Public and Private Attribution of Cyber Operations*, op. cit., p. 9.
[16] *Id*. p. 9.
[17] *Id*. p. 10.
[18] Edward Hunter Christie and Kristine Berzina, *NATO and Societal Resilience: All Hands on Deck in an Age of War*, op.cit., p. 8.
[19] *Ibid*., Psychological Defence Agency

attributions et permettrait une reconnaissance plus vaste au sein de l'Alliance. Idéalement, cela mènerait à l'appui d'une majorité des Alliés, et potentiellement d'acteurs externes à l'Alliance. À ce titre, l'*Information Environment Assessment* (IEA), qui combine ressources humaines, méthodologies communes et technologies avancées pour produire des analyses standardisées de l'environnement informationnel, offre déjà une base solide pour structurer cette cohérence[20].

Conclusion

Dans un environnement où les manipulations visent à fragmenter les perceptions et à paralyser la décision, la confiance devient une ressource stratégique essentielle. Sans attribution fiable, la population doute, les personnels hésitent et les Alliés se soupçonnent, au risque de fragiliser la posture collective de l'OTAN. En intégrant pleinement l'attribution dans sa stratégie de résilience, l'Alliance peut renforcer sa cohésion interne, consolider sa crédibilité externe et transformer la transparence en avantage stratégique durable.

Les évolutions rapides de l'intelligence artificielle générative, la prolifération des deepfakes en temps réel et l'intensification des attaques hybrides feront de l'attribution un enjeu toujours plus central. Dans ce contexte, développer une capacité nationale et une harmonisation OTAN ne constitue pas seulement un exercice technique : c'est désormais une condition fondamentale pour restaurer et préserver la confiance à l'ère des manipulations.

[20] *NATO's approach to counter information threats*, Endorsed by Allied Defence Ministers on 18 October 2024.

Bibliographie

- Camille François et Herbert Lin, Cartographier un angle mort : la surprise stratégique des opérations informationnelles russes sur les réseaux sociaux en 2016, Géopolitique de la datasphère, Hérodote, n°177-178, Paris, 2020
- Conseil de l'Union européenne, L'UE impose les toutes premières sanctions à la suite de cyberattaques, communiqué de presse, 30 juillet 2020, pp.53
- CSS CYBER DEFENSE PROJECT, *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict, Risk and Resilience Team*, Center for Security Studies (CSS), Zürich, October 2018, pp. 56
- Edward Hunter Christie and Kristine Berzina, *NATO and Societal Resilience: All Hands on Deck in an Age of War*, Policy Brief, GMF, 2022, pp. 12
- Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe, *Opportunities for Public and Private Attribution of Cyber Operations*, Tallinn Paper No. 12, CCDCOE, 2021, pp. 20
- NATO, Allied Joint Doctrine for Cyberspace Operations, AJP – 3.20, January 2020
- *NATO's approach to counter information threats*, Endorsed by Allied Defence Ministers on 18 October 2024
- OTAN, Communiqué du sommet de Bruxelles, 14 juin 2021
- OTAN, Déclaration du Conseil de l'Atlantique Nord suite à l'annonce par les Etats-Unis de mesures concernant la Russie, 15 avril 2021
- Psychological Defence Agency
- Traité de l'Atlantique Nord, Article 3, 4 avril 1949

ISSN : 2739-3283

Institut d'études de géopolitique appliquée
66 avenue des Champs-Élysées, 75008 Paris
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org