Contre-attaque : l'OTAN doit passer à l'offensive

Trop de membres de l'OTAN ne comprennent pas les risques liés au cyberespace et la nécessité de riposter aux agresseurs. C'est la recette de l'échec.

Par Emily Otto

29 octobre 2025 / https://cepa.org/article/counterpunch-nato-must-take-the-offensive/

L'OTAN a investi massivement dans la cyberdéfense depuis 2016, mais la plupart de ses membres continuent de se concentrer sur la protection des réseaux nationaux plutôt que de prendre l'initiative.

À partir de 2020, l'alliance s'est retrouvée dans une position déséquilibrée : le partage des menaces s'améliore, mais l'offensive et la lutte contre les adversaires très actifs de l'OTAN dans le cyberespace ne sont assurées que par quelques-uns. Cet écart est important car le cyberespace est un domaine de contact constant, où la passivité cède l'avantage.

Cinq ans plus tard, peu de choses ont changé : la posture cybernétique de l'OTAN reste faible, ancrée dans la défense passive, tandis qu'une poignée d'États assument la charge des opérations offensives dans le cyberespace.

L'OTAN reconnaît le cyberespace comme un domaine opérationnel, mais ses membres divergent fortement dans la pratique. La plupart des alliés se concentrent sur la défense des réseaux, en mettant en place des équipes d'intervention en cas d'incident et des cadres de résilience axés sur la « protection » et la « sécurité ». Peu d'entre eux mentionnent explicitement des actions offensives. Seuls quelques-uns, comme les États-Unis, le Royaume-Uni et le Canada, « contrent », « combattent » et « produisent des effets » grâce à des forces cyberoffensives dirigées par l'armée. Il en résulte une posture inégale : beaucoup défendent, mais peu combattent.

Une poignée de membres ont progressivement adopté une posture cyber plus active, mais sans pour autant perturber de manière persistante leurs adversaires. Les Pays-Bas, par exemple, reconnaissent la nature constante des ingérences étrangères, mais limitent leur réponse au partage et à la coordination des renseignements, ce qui constitue une amélioration par rapport aux opérations réservées aux temps de guerre, mais reste néanmoins réactif. Les groupes soutenus par la Russie exploitent cette hésitation. Que

cela plaise ou non, l'OTAN est déjà engagée dans un conflit cyber, mais refuse simplement de l'admettre.

L'offensive est importante. Le cyberespace est en constante évolution : chaque correctif, chaque mise à jour et chaque nouvelle application modifie le terrain. Attendre pour réagir revient à céder l'initiative à l'adversaire. Les opérations offensives peuvent perturber l'infrastructure des ransomwares, démanteler les nœuds de commandement et de contrôle et empêcher les adversaires de se faufiler dans les réseaux alliés pour y causer des dommages. Tant que cette capacité offensive ne sera pas adoptée, l'OTAN continuera à céder l'initiative à ses adversaires.

Soyons clairs. L'aversion pour les opérations cyberoffensives est d'ordre politique, et non technique. De nombreux alliés considèrent l'offensive comme illégale ou contraire à l'éthique, intégrant ainsi un parti pris défensif dans leur doctrine et leur mission.

La position officielle de l'OTAN est d'encourager les États membres à poursuivre les intérêts de l'alliance dans le cyberespace, faisant ainsi de la cyberguerre de l'alliance une activité volontaire. En conséquence, rares sont ceux qui s'engagent, tandis que d'autres profitent de la situation. Il en résulte une alliance politiquement prudente qui s'appuie sur l'offensive de quelques-uns pour défendre la majorité. Et compte tenu de la vague de cyberattaques dont sont victimes les États membres de l'OTAN, cette approche ne fonctionne clairement pas.

En restant passifs, de nombreux États membres de l'OTAN invitent leurs adversaires à redoubler d'efforts. Comme l'affirment Michael Fischerkeller, Emily Goldman et Richard Harknett dans leur ouvrage Cyber Persistence Theory publié en 2022, le cyberespace est un domaine de contact permanent : les sondages ne s'arrêtent jamais, les exploiteurs ne se reposent jamais.

La dissuasion n'est pas une stratégie qui fonctionne réellement dans le domaine cybernétique : les attaques n'atteignent pas le seuil de la guerre, leur attribution est floue et elles ont rarement des conséquences. Lorsque les alliés se limitent à une défense passive et à la résilience, cela témoigne en soi d'un manque de volonté politique. Les pirates informatiques continuent d'essayer parce que l'offensive est payante. À quoi servent les agences de renseignement qui collectent des informations sur les menaces si les militaires ne peuvent pas agir rapidement ?

Ce déséquilibre a des conséquences réelles. La posture cybernétique de l'OTAN repose sur quelques États pour mener le combat, tandis que d'autres se contentent d'une défense qui, en réalité, n'offre qu'une illusion de sécurité. Les petits alliés peuvent penser que cela suffit, mais ce n'est vraiment pas le cas. Non seulement cela ne permet pas d'assurer une

défense adéquate, mais cela nuit également à l'alliance dans son ensemble. La taille n'est pas une excuse ; dans le cyberespace, même les petits États peuvent avoir un impact considérable.

Il est temps de lever les obstacles : lois obsolètes, organisations rigides et ressources limitées. Le cyberconflit entre l'OTAN et ses adversaires est déjà une réalité. Des attaques ont lieu quotidiennement.

L'absence de contre-mesures efficaces permet aux adversaires d'éroder les sources de pouvoir stratégique des membres de l'OTAN. Ils exploitent les failles entre les positions des membres.

Cette voie risque d'entraîner des coûts énormes et des défaites continues dans la sphère cybernétique. L'OTAN doit améliorer son action à grande échelle et exiger la participation de tous ses membres.

Emily Otto est chercheuse non résidente au CEPA. Elle est titulaire d'une bourse de doctorat Alperovitch à la Johns Hopkins School of Advanced International Studies, après avoir quitté l'armée, où elle a passé dix ans à travailler dans le domaine du renseignement sur les menaces et des cyberopérations.