# De la Défense Passive à la Riposte Active : Le Hack-back comme Révélateur de la Mutation Sécuritaire

Posted on juillet 9, 2026 by Shizneider BAPTISTE

Résumé/Abstract

**Le hack-back, ou cyberdéfense active, incarne un tournant stratégique majeur dans la manière dont les États et, potentiellement, les entreprises privées envisagent la riposte aux agressions numériques. Longtemps cantonné à la sphère théorique ou à des pratiques clandestines, il s'inscrit désormais dans des doctrines officielles et des projets législatifs, signalant une évolution profonde des paradigmes de sécurité internationale. Cet article analyse les dimensions doctrinales, juridiques, opérationnelles et géostratégiques du hack-back, en mettant en lumière ses implications pour la souveraineté numérique, la dissuasion cybernétique et la gouvernance internationale de la cybersécurité. Il soutient que le hack-back représente non seulement une nouvelle modalité de riposte, mais aussi un révélateur des transformations structurelles affectant la sécurité numérique à l'ère de la cyberguerre explicite.**

## Introduction : le hack-back comme révélateur d'une mutation stratégique

Le hack-back, défini comme l'action de pénétrer, perturber, voire endommager les systèmes informatiques de l'agresseur en réponse à une cyberattaque subie, constitue bien plus qu'une simple évolution technique dans l'arsenal de la cybersécurité. Il incarne un tournant stratégique majeur, signalant une transformation profonde des doctrines de sécurité internationale et des modalités de l'affrontement numérique. Initialement évoqué aux États-Unis à la suite de la série d'attaques de 2014 (Office of Personnel Management, JP Morgan, Target), il a été progressivement rebaptisé « cyberdéfense active » pour en atténuer la connotation offensive et faciliter son intégration dans des cadres juridiques et stratégiques plus larges. Cette évolution terminologique reflète une volonté des décideurs de normaliser une pratique autrefois perçue comme marginale, voire

illégale, et de l'insérer dans une logique de légitimation étatique et de gouvernance internationale. Le hack-back n'est donc pas seulement une nouvelle technique de riposte ; il est un révélateur des transformations structurelles affectant la sécurité numérique à l'ère de la cyberguerre explicite, où la frontière entre défense et offense s'estompe au profit d'une posture de défense active, voire préemptive.

## Contexte émergent : la crise de la défense passive et l'impératif de riposte

Le concept de hack-back s'inscrit dans un contexte de multiplication et de sophistication des cybermenaces, où les mécanismes traditionnels de défense passive (pare-feu, détection d'intrusion, réponse à incident) apparaissent insuffisants face à la persistance et à l'ampleur des campagnes hostiles. Les statistiques récentes montrent une augmentation exponentielle des attaques ciblant les infrastructures critiques, les chaînes d'approvisionnement numériques et les systèmes de gouvernance étatique. Dans ce contexte, la défense passive, bien que nécessaire, ne suffit plus à garantir la résilience des systèmes ni à dissuader les agresseurs. Le hack-back émerge alors comme une réponse à cette crise de la défense passive, offrant une modalité de riposte plus dynamique, plus immédiate et, surtout, plus crédible sur le plan de la dissuasion. Il permet de renverser la logique asymétrique qui a longtemps caractérisé la cyberguerre, où l'agresseur bénéficiait d'un avantage structurel en termes d'anonymat, de rapidité et de faible coût d'opération. En introduisant la possibilité d'une riposte active, le hack-back rétablit une forme de symétrie stratégique, obligeant l'agresseur à anticiper non seulement les défenses de sa cible, mais aussi les contre-mesures potentielles dirigées contre ses propres infrastructures.

## Évolution doctrinale et législative : du tabou à la normalisation

Plusieurs pays ont officiellement intégré le hack-back dans leur posture stratégique, signalant une évolution doctrinale majeure. Aux États-Unis, bien que le Congrès n'ait pas adopté l'ACDC (Active Cyberdefense Certainty Act) en 2017 et 2019, un nouveau projet de loi, le Scam Farms Mark and Reprisal Authorization Act, déposé en août 2025, propose d'autoriser des entités privées à saisir des biens ou personnes impliqués dans la cybercriminalité transnationale, via des lettres de marque présidentielles. Ce projet, bien que controversé, reflète une tendance plus large à la délégation de missions de sécurité nationale à des acteurs privés, dans un

contexte de saturation des capacités étatiques. En Allemagne, en 2026, Berlin a intégré le hack-back dans sa doctrine de cyberdéfense, permettant la neutralisation directe des serveurs attaquants. Cette décision marque un tournant majeur dans la posture stratégique allemande, traditionnellement centrée sur la défense passive et la coopération internationale. Au sein de l'Union européenne et de l'OTAN, depuis 2023-2024, le Conseil de l'UE et l'OTAN encouragent le développement de capacités de cyberdéfense proactive, incluant la détection, la dissuasion et, le cas échéant, la riposte active. Des pays comme l'Australie, le Japon et la Chine ont également annoncé des politiques de cyberdéfense active, ciblant prioritairement les cybercriminels et les infrastructures de commande et contrôle de logiciels malveillants. Cette évolution doctrinale et législative signale une normalisation progressive du hack-back, qui passe d'une pratique marginale à une composante centrale des stratégies de sécurité numérique.

## Enjeux stratégiques et controverses : dissuasion, délégation et risques d'escalade

Le hack-back constitue un tournant stratégique à plusieurs égards, soulevant des enjeux majeurs en termes de dissuasion, de gouvernance et de stabilité internationale. En premier lieu, il permet de renforcer la crédibilité de la dissuasion en rendant la riposte plus immédiate et tangible, tout en posant la question cruciale de l'attribution fiable des attaques. Sans attribution précise, le hack-back risque de devenir une arme à double tranchant, susceptible de frapper des cibles innocentes ou de déclencher des cycles de représailles incontrôlables. En deuxième lieu, la délégation à des acteurs privés de missions traditionnellement dévolues aux forces de l'ordre ou aux armées soulève des risques éthiques, juridiques et de gouvernance. Comment garantir la légitimité, la proportionnalité et la traçabilité des opérations de hack-back lorsque celles-ci sont confiées à des entreprises privées, dont les motivations peuvent être guidées par des intérêts commerciaux plutôt que par des impératifs de sécurité nationale ? En troisième lieu, le risque d'escalade et de dommages collatéraux reste une préoccupation majeure. Une riposte mal ciblée peut entraîner des effets en cascade, toucher des infrastructures tierces ou déclencher des cycles de représailles difficiles à contrôler, notamment dans un environnement international fragmenté et concurrentiel. Ces enjeux soulignent la nécessité d'un encadrement strict du hack-back, tant sur le plan national qu'international, afin d'éviter qu'il ne devienne une source d'instabilité plutôt qu'un outil de dissuasion.

## Perspectives géostratégiques : vers une cyberguerre explicite et ses implications

Le hack-back marque une transition vers une cyberguerre plus explicite, où la frontière entre défense et offense s'estompe. Il reflète une mutation des doctrines de sécurité, passant d'une logique de protection passive à une posture de défense active, voire préemptive. Cette évolution s'inscrit dans une tendance plus large visant à impliquer davantage le secteur privé dans la sécurité nationale, notamment via la symbiose opérationnelle entre agences (Cyber Command, NSA, FBI) et entreprises de cybersécurité. Sur le plan géostratégique, le hack-back redéfinit les équilibres de puissance dans l'espace numérique, en offrant aux États dotés de capacités avancées un moyen de projeter leur influence et de défendre leurs intérêts sans recourir à des moyens militaires traditionnels. Il permet également de contourner les contraintes du droit international humanitaire, en opérant dans une zone grise où les règles de l'affrontement restent floues et contestées. Toutefois, cette liberté d'action s'accompagne de risques majeurs, notamment en termes de stabilité internationale. La prolifération des capacités de hack-back, tant étatiques que non étatiques, pourrait entraîner une fragmentation de l'espace numérique, où chaque acteur développe ses propres règles et modalités de riposte, au détriment d'une gouvernance internationale cohérente. Le hack-back, loin d'être une simple technique de riposte, apparaît ainsi comme un révélateur des transformations structurelles affectant la sécurité numérique à l'ère de la cyberguerre explicite.

## Conclusion : le hack-back comme révélateur des transformations de la sécurité numérique

Le hack-back n'est pas seulement une nouvelle modalité de riposte ; c'est un révélateur des transformations en cours dans la gouvernance de la sécurité numérique, où États, entreprises et acteurs non étatiques redéfinissent les règles de l'affrontement cybernétique. Son adoption croissante signale un basculement stratégique vers une cyberguerre plus explicite, mais aussi plus risquée, nécessitant une réflexion approfondie sur ses implications juridiques, éthiques et géopolitiques. À l'heure où les États cherchent à renforcer leur souveraineté numérique et à dissuader les agresseurs, le hack-back offre une modalité de riposte plus dynamique et plus crédible, mais il soulève également des questions majeures en termes de gouvernance, de stabilité internationale et de légitimité des acteurs impliqués. L'avenir du hack-back dépendra donc non seulement de son encadrement juridique et opérationnel, mais aussi de la capacité des États à

développer une vision stratégique cohérente de la sécurité numérique, où la défense active s'inscrit dans un cadre plus large de gouvernance internationale et de stabilité stratégique.

## About The Author

Shizneider BAPTISTE

Expert et Consultant en Diplomatie et Relations internationales |
Analyste en Stratégie internationale (Sécurité et Défense) |
Analyste en Renseignement, Stratégies et Guerre d'influence

See author's posts