LA CYBERDÉFENSE AMÉRICAINE SOUS LE PREMIER MANDAT DE TRUMP
U.S. Cyber Defense Under Trump's First Term



Saibi Zineddine
École Nationale Supérieure de Sciences Politiques
saibi.zineddine@yahoo.com

Date de soumission: 05/03/2026 Date d'acceptation: 26/05/2026 Date de publication: 10/06/2026

Résumé:

Cet article traite de l'évolution de la cyberdéfense américaine durant le premier mandat de Trump (2017-2021), en analysant les réflexions doctrinales autour des concepts de defend forward et de persistent engagement, ainsi que l'élévation de l'US Cyber Command au rang de commandement unifié, qui constitue le pilier organisationnel de la cyberdéfense. Le tout s'inscrit dans le contexte des ingérences électorales russes et des attaques de type SolarWinds, qui ont révélé la vulnérabilité des chaînes d'approvisionnement.

***Mots clés**: cyberdéfense, cyberespace, trump, cyber command, doctrine militaire*

***classification JEL:** H56; D74.*

Abstract:

This article examines the evolution of U.S. cyber defense during Trump's first presidential term (2017–2021), analyzing doctrinal reflections on the concepts of defend forward and persistent engagement, as well as the elevation of U.S. Cyber Command to a unified combatant command, which constitutes the organizational pillar of cyber defense. This analysis is situated within the context of Russian electoral interference and the SolarWinds attacks, which revealed the vulnerability of supply chains.

***key words**: cyber defense, cyberspace, trump, cyber command, military doctrine*

***JEL classification:** H56; D74.*

Introduction :

Depuis la fin de la Guerre froide, et plus encore depuis la généralisation des Nouvelles Technologies de l'Information et de la Communication (NTIC), le cyberespace s'est imposé comme un domaine stratégique de confrontation, au même titre que la terre, la mer, l'air et l'espace. Pour les États-Unis, la cyberdéfense occupe une place centrale dans la protection des infrastructures critiques, la garantie de la supériorité opérationnelle et la projection de puissance dans un environnement numérique de plus en plus conflictuel. Sous l'administration Trump (2017-2021), cette dynamique a pris une importance accrue : face à la multiplication des intrusions attribuées à des acteurs étatiques et non étatiques, Washington a veillé à demeurer à la pointe de l'innovation en matière d'organisation de la cybersécurité nationale et d'anticipation des cybermenaces, en particulier durant le premier mandat de Donald Trump.

Ce mandat présente un intérêt particulier en ce qu'il s'ouvre et se clôt par deux cyberattaques majeures menées par des acteurs étrangers, probablement le même, d'ailleurs. En effet, l'évaluation conjointe de la CIA, du FBI et de la NSA du 6 janvier 2017 conclut que la Russie a conduit une campagne coordonnée d'influence et d'intrusions visant l'élection présidentielle américaine de 2016. Le mandat s'achève sur la révélation de l'incident SolarWinds, en décembre 2020 : une compromission massive de la chaîne d'approvisionnement logicielle ayant touché de multiples agences fédérales et entreprises, attribuée par la suite au "SVR", le Service des renseignements extérieurs de la Fédération de Russie.

Ces deux jalons, l'ingérence électorale initiale et l'opération de cyber espionnage d'envergure en fin de mandat, structurent la problématique de la cyberdéfense aux États-Unis durant la première administration Trump. La présente étude se propose d'examiner les principaux incidents cyber survenus au cours de cette période, ainsi que les adaptations politiques, organisationnelles et doctrinales mises en œuvre par l'administration. Ainsi, notre question de recherche à laquelle on doit répondre est : **Quels apports l'administration Trump a-t-elle apportés à la doctrine américaine de cyberdéfense** ?

Chapitre 1 : L'ingérence russe dans les élections présidentielles de 2016

L'ingérence russe dans l'élection présidentielle américaine de 2016 a déplacé la sécurité électorale au cœur de la cybersécurité. L'opération, menée sous le seuil de la guerre, a combiné intrusions informatiques et opérations d'influence en ligne, dans une logique de mesures actives adaptée au cyberespace. La finalité recherchée n'était pas la destruction d'infrastructures, mais l'altération de la confiance publique et la perturbation du débat démocratique. Les travaux de référence décrivent ce type d'action comme une « campagne » composée d'opérations reliées visant des effets stratégiques sans recours à la force armée, ce qui éclaire la dynamique observée en 2016.

Sur le versant technique, deux groupes étroitement associés aux services russes, Cozy Bear (APT29) et Fancy Bear (APT28), ont mené dès 2015 des campagnes de hameçonnage ciblant le Comité national démocrate et des responsables de campagne. Ces intrusions ont permis l'exfiltration de courriels à haute valeur politique, notamment ceux du directeur de campagne de Hillary Clinton, John Podesta. La publication séquencée des documents volés a été synchronisée avec le calendrier médiatique afin d'accroître la visibilité et l'impact des fuites.

Sur le versant informationnel, l'Internet Research Agency a acheté des publicités ciblées et diffusé des contenus amplifiant des clivages sociaux préexistants. Les estimations publiques de portée, fondées sur les données des plateformes, évoquent une exposition de plusieurs dizaines de millions d'utilisateurs américains. L'évaluation inter-agences américaine publiée en janvier 2017 a conclu que Moscou cherchait à miner la confiance dans le processus démocratique, à dénigrer Hillary Clinton et à nuire à son éligibilité. L'effet escompté résidait dans la désorientation de l'espace informationnel plus que dans la coercition immédiate d'acteurs institutionnels.

Cette configuration correspond à une stratégie de « guerre politique » où l'espionnage sert la manipulation, avec une signalisation volontairement ambiguë pour réduire le risque d'escalade et préserver la dénégation plausible. Les analyses comparatives soulignent que, dans ce registre, l'utilité coercitive directe demeure faible et que les bénéfices recherchés sont cumulatifs, latents et liés à la polarisation sociale.

Les données disponibles étayent trois constats. Premièrement, l'exposition aux contenus offensifs a été substantielle, tant par la diffusion de données volées que par l'amplification sur les réseaux socio-numériques. Deuxièmement, si l'on observe une synchronisation efficace entre exfiltration et divulgation, la littérature ne documente pas de modification de préférences électorales à grande échelle attribuable à ces opérations ; l'effet plausible porte plutôt sur la polarisation, la défiance et la délégitimation procédurale. Troisièmement, l'efficacité stratégique tient à la persistance de la campagne et à l'ambiguïté de l'attribution, plus qu'à un levier de compellence explicite. Ces conclusions convergent avec les études qui décrivent les cyber-campagnes contemporaines comme orientées vers la perturbation et l'espionnage, avec des rendements coercitifs limités mais des effets cumulatifs sur la confiance publique.

L'épisode 2016 a agi comme catalyseur pour l'appareil américain de cyberdéfense entre 2017 et 2021. Sur le plan organisationnel, la décision présidentielle d'août 2017 d'élever l'U.S. Cyber Command (USCYBERCOM) au rang de commandement unifié, couplée à la montée en puissance du Cyber Mission Force (environ 6 200 personnels organisés en 133 équipes), a consolidé la capacité d'action continue et la priorisation de la mission « défendre la Nation » dans et par le cyberespace. Cette consolidation a renforcé la préparation et l'intervention face aux campagnes d'ingérence sous le seuil.

Sur le plan doctrinal, la réponse s'est inscrite dans une approche de compétition persistante, qui valorise l'anticipation, la détection et l'entrave en continu des acteurs hostiles. Dans ce cadre, la notion d'Active Cyber Defense telle que définie par le Département de la défense — capacité synchronisée à découvrir, détecter, analyser et mitiger en « temps pertinent » — a fourni un référentiel pour accélérer la boucle défensive, sans préjuger d'options offensives. En parallèle, la nécessité d'un couplage étroit entre autorités fédérales, États fédérés, acteurs privés et plateformes s'est imposée, en cohérence avec les recommandations d'une approche « société entière » visant à réduire la surface d'attaque informationnelle et à améliorer le partage de signaux faibles.

En somme, l'ingérence de 2016 a consacré la sécurité des processus démocratiques comme bien critique de la cybersécurité nationale. Elle a soutenu, sous l'administration Trump, une évolution institutionnelle et doctrinale orientée vers la présence opérationnelle, la coordination inter-agences et l'automatisation

des défenses, dans une perspective de compétition stratégique prolongée sous le seuil.

Chapitre 2 : « Defend Forward » et « Persistent Engagement » dans la doctrine cyber américaine

Entre 2018 et 2021, la doctrine américaine passe d'une posture principalement réactive à une logique de contestation continue des activités adverses, assumée « au plus près de leur origine ». Le Summary of the Department of Defense Cyber Strategy (2018) consacre « defend forward » et précise que le DoD « perturbera ou interrompra à la source » des activités malveillantes, y compris sous le seuil du conflit armé. La Command Vision du Cyber Command (USCYBERCOM) affirme la nécessité d'« opérations persistantes et intégrées » et de « défendre en avant, au plus près de l'origine de l'activité adverse », dans un environnement de « contact constant ». La mise en œuvre bénéficie, la même année, d'un allègement procédural via NSPM-13, mémorandum présidentiel qui délègue au secrétaire à la Défense des autorités bien définies pour des opérations cyber « sensibles au temps ».

Deux diagnostics fondent cette réorientation. Le premier est la nature compétitive du cyberespace, caractérisée par des campagnes continues sous le seuil de la force, qui imposent de contester l'adversaire dans la durée plutôt que d'attendre une agression manifeste. Cette lecture — conceptualisée par Fischerkeller et Harknett — soutient que l'« engagement persistant » structure une « compétition acceptée » et peut stabiliser l'interaction en façonnant les attentes. Le second concerne l'illusion d'un avantage offensif « structurel » : l'analyse de Slayton montre que le rapport offense/défense dépend de contextes organisationnels et technologiques précis, et qu'il ne saurait fonder, à lui seul, une stratégie tournée vers l'offense.

Dans les textes doctrinaux de 2018, « defend forward » renvoie à une posture d'anticipation et de déni conduite aussi hors des réseaux américains, afin d'empêcher en amont des effets sur le territoire et sur les forces. « Persistent engagement » désigne un mode d'action soutenu, sériel et intégré, qui vise à conserver l'initiative, à éroder les capacités adverses dans le temps et à influencer leurs calculs de coûts et de risques. Les deux notions sont

complémentaires : la première définit l'aire et la proximité de l'action, la seconde en organise le tempo et la continuité.

L'ancrage normatif provient des documents officiels de 2018 (DoD Cyber Strategy ; Command Vision), qui entérinent la proactivité et l'activité quotidienne de compétition. Les travaux académiques sur les « campagnes cyber » précisent l'idée que les effets stratégiques résultent d'opérations liées et répétées plutôt que d'actions ponctuelles isolées. Les controverses portent sur l'escalade et la signalisation : pour certains, l'engagement persistant peut clarifier les attentes et limiter les surprises ; pour d'autres, il entretient l'ambiguïté des seuils. Dans le registre des garde-fous, Schneider a proposé une « no-first-use » stratégique appliquée au cyber, destinée à dissocier la compétition quotidienne des atteintes susceptibles d'affecter la stabilité nucléaire.

L'élévation d'USCYBERCOM au rang de commandement unifié (2018) et l'atteinte du full operational capability par la Cyber Mission Force structurent la capacité d'exécuter des campagnes soutenues. En mai 2018, les 133 équipes prévues atteignent ce jalon ; l'effectif projeté se situe autour de 6 200 personnels. La défense n'est plus cantonnée à la DoDIN (Department of Defense Information Network), réseau d'information du DoD, mais s'étend vers l'« avant » afin de détecter et contester l'adversaire « au plus près de l'origine ». Sur le plan opérationnel, plusieurs épisodes publics illustrent cette logique : en 2018, USCYBERCOM perturbe l'accès Internet de l'Internet Research Agency le jour des midterms ; en 2020, il vise le botnet TrickBot pour réduire les risques pesant sur les infrastructures électorales. Des révélations de presse (2019) font par ailleurs état d'implants dans des réseaux électriques russes, indicateurs d'une capacité de pression en profondeur cohérente avec « defend forward ».

L'objectif est de réduire le dwell time adverse, d'augmenter les coûts de l'opération offensive, et d'imposer des frictions récurrentes qui modifient les calculs adverses sans franchir le seuil de l'emploi de la force. La réussite dépend d'un renseignement actionnable, de l'intégration inter-agences et d'une gouvernance des risques alignée sur le rythme des opérations, conditions explicitement mises en avant dans la Command Vision. L'économie générale de la doctrine reste compatible avec une lecture prudente du rapport offense/défense, qui souligne l'importance d'investissements organisationnels pour rendre la défense plus coûteuse à contourner.

Le déplacement de la ligne de front vers l'« avant » peut être interprété comme une préparation d'attaque, alimentant un security dilemma si les effets débordent vers des tiers. Les débats sur l'escalade appellent des règles d'engagement traçables et des signaux de retenue sur les cibles sensibles, y compris celles liées aux systèmes d'alerte et de commandement nucléaire. Une clarification doctrinale des seuils et des objectifs, combinée à des pratiques de transparence sélective, vise à conserver les bénéfices opérationnels de l'engagement persistant tout en maîtrisant les risques de malentendu stratégique.

Au terme de la période, « defend forward » et « persistent engagement » ont été institutionnalisés comme principes d'action : ils assument la compétition continue, déplacent la défense au-delà de la seule DoDIN et cherchent à façonner les comportements adverses par des campagnes soutenues. Cette inflexion a accru l'agilité opérationnelle d'USCYBERCOM et favorisé une protection des processus électoraux par des actions en amont, tout en laissant ouverte la question de l'escalade et de ses garde-fous stratégiques.

Chapitre 3 : SolarWinds : un cas d'école de compromission de chaîne d'approvisionnement

La compromission SolarWinds est divulguée publiquement mi-décembre 2020, quand FireEye révèle une campagne d'ampleur fondée sur l'insertion d'un code malveillant dans des mises à jour du logiciel Orion, largement utilisé pour l'administration réseau. Le Department of Homeland Security publie le 13 décembre une directive d'urgence ordonnant l'arrêt et l'audit des instances Orion dans les agences civiles fédérales. L'incident remonte à des versions distribuées entre mars et juin 2020, avec une phase dormante puis une activation discrète des charges utiles. Au 5 janvier 2021, une déclaration conjointe FBI-CISA-ODNI-NSA indique que l'opération est « probablement d'origine russe » et vise du renseignement. L'attribution officielle à la SVR (APT29/Cozy Bear) est formalisée le 15 avril 2021 par la Maison-Blanche, accompagnée de mesures de rétorsion et de conseils techniques. Ces jalons s'inscrivent dans une compétition « sous le seuil », où des campagnes persistantes recherchent des effets stratégiques sans recours à la force armée.

Le mécanisme initial repose sur un binaire Orion modifié (SolarWinds.Orion.Core.BusinessLayer.dll) livrant le cheval de Troie

SUNBURST, qui établit une commande et contrôle furtive après une période d'inactivité. Les opérateurs emploient ensuite des techniques d'élévation et de mouvement latéral, avec un pivot vers des environnements Azure AD/M365. La compromission et l'abus de jetons d'authentification SAML (dit « Golden SAML ») permettent une persistance nuage et l'accès à des ressources sans alerte immédiate. Microsoft et CISA documentent l'enchaînement : persistance, vol de certificats ADFS, génération de jetons, puis exfiltration sélective. SolarWinds indique que le code malveillant a été retiré de son environnement dès juin 2020, ce qui a compliqué la détection rétrospective.

Environ 18 000 clients ont potentiellement reçu des mises à jour compromises, mais une fraction réduite a subi un « follow-on » avec accès opérationnel. La coordination inter-agences établie mi-décembre 2020 gère l'enquête et l'éviction. L'évaluation publique américaine, « haute confiance », attribue la campagne à la SVR le 15 avril 2021. Des sources officielles évoquent « moins de dix » départements fédéraux effectivement compromis, dans une logique d'espionnage ciblé plutôt que de sabotage.

La réponse immédiate combine éradication, durcissement et interdiction temporaire d'Orion. CISA publie directives, IOC, et consignes d'« eviction » incluant une reconstruction des environnements et une chasse aux abus SAML. Au niveau exécutif, l'Executive Order 14028 (12 mai 2021) impose l'adoption du « zero trust », la modernisation cloud, la journalisation centralisée, et un relèvement des exigences de chaîne d'approvisionnement logicielle. Les forces armées renforcent leurs pratiques DevSecOps et leur posture défensive en conséquence. La Maison-Blanche annonce en parallèle des sanctions et des mesures techniques contre la SVR. L'épisode met en évidence des frictions de partage d'information public-privé et des délais d'alerte, soulignés par la conseillère adjointe à la sécurité nationale pour le cyber en février 2021, et plaide pour des mécanismes de signalement plus contraignants. Dans la perspective doctrinale, SolarWinds confirme la pertinence d'une posture de « défense persistante » axée sur la détection-réponse en profondeur, la gestion des identités, et la sécurité des chaînes logicielles comme variables décisives de la puissance en deçà du seuil.

Conclusion

La séquence 2016–2021 constitue un tournant: des ingérences russes de 2016 à SolarWinds fin 2020, la réponse américaine a durci l'architecture (élévation d'USCYBERCOM) et consacré une bascule doctrinale vers « defend forward » et le « persistent engagement ». Cette posture inscrit l'outil militaire dans des campagnes continues sous le seuil de la guerre, visant des gains stratégiques cumulatifs plutôt que des effets décisifs uniques. Elle demeure toutefois contestée pour ses ambiguïtés et risques d'escalade, au cœur du « problème des deux seuils » identifié par la littérature. Empiriquement, SolarWinds a confirmé la prévalence de l'espionnage de supply chain sur la disruption, l'attribution « probablement russe », et mis en évidence des barrières de partage d'information que l'exécutif a cherché à corriger. Côté défense, les services ont renforcé leurs pratiques DevSecOps et la sécurisation logicielle. En sortie de mandat, la cyberdéfense américaine s'oriente vers un triptyque fait d'« active cyber defense », d'intégration ML/IA et de réformes de gouvernance, tout en butant sur des contraintes structurelles qui relativisent l'efficacité d'une posture purement défensive et nourrissent le débat sur l'équilibre offense-défense. En somme, l'ère Trump a consolidé une doctrine d'engagement persistant et une capacité institutionnelle accrues, sans clore les controverses juridiques et stratégiques; elle a surtout normalisé une compétition cyber continue sous le seuil de la guerre, qui restera la condition d'action des États-Unis.

Références

Atrews, R. A. (2020). Cyberwarfare: Threats, security, attacks, and impact. Journal of Information Warfare, 19(4), 17–28.

Bort, B. (2018). There IS no cyber defense. The Cyber Defense Review, 3(1), 41–46.

Couillard, J. (2024). Beyond USCYBERCOM: The need to establish a dedicated U.S. cyber military force. The Cyber Defense Review, 9(1), 55–72.

Davis, S. W. (2020). ML/AI and the next generation of cyber defense. American Intelligence Journal, 37(2), 49–54.

Deppa, C. S. (2017). U.S. Cyber Command: An overview. American Intelligence Journal, 34(1), 12–15.

Haataja, S. (2020). Cyber operations and collective countermeasures under international law. Journal of Conflict & Security Law, 25(1), 1–19.

Henry, S., & Brantly, A. F. (2018). Countering the cyber threat. The Cyber Defense Review, 3(1), 47–56.

Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. Journal of Strategic Studies, 42(2), 212–245.

Kallberg, J. (2016). Strategic cyberwar theory: A foundation for designing decisive strategic cyber operations. The Cyber Defense Review, 1(1), 113–128.

Kelly, W. E. (2017). Alleged Chinese cyberspies: An American dilemma. American Intelligence Journal, 34(1), 16–20.

Noel, G. E., & Reith, M. G. (2021). Cyber warfare evolution and role in modern conflict. Journal of Information Warfare, 20(4), 30–44.

Paul, C., Porche, I. R., III, & Axelband, E. (2014). Cyber forces and U.S. Cyber Command. In The other quiet professionals: Lessons for future cyber forces from the evolution of special forces (Chap. 4). RAND Corporation.

Schneider, J. (2020). A strategic cyber no-first-use policy? Addressing the US cyber strategy problem. The Washington Quarterly, 43(2), 159–175.

Slayton, R. (2016). What is the cyber offense-defense balance? Conceptions, causes, and assessment. International Security, 41(3), 72–109.

Webber, R. W. (2017). Persistent operational intelligence: An intelligence strategy for Joint Force 2020. American Intelligence Journal, 34(1), 59–68.

Williams, A. M. (2020). Strategic culture and cyber warfare: A methodology for comparative analysis. Journal of Information Warfare, 19(1), 113–127.

Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. Journal of Strategic Studies, 45(4), 534–567.