LE RUBICON

De la dissuasion aux stratégies opaques : repenser les opérations cyberoffensives

Jonathan Guiffard | 10 juin 2026 | ARTICLES

Le 17 février 2026, la branche de Google chargée de l'étude des menaces cyber, Google Threat Intelligence Group alertait sur une campagne de cyber-espionnage durant laquelle un groupe de hackers chinois (surnommé UNC6201 et qui pourrait être lié au groupe Silk Typhoon) serait resté 18 mois à exploiter une faille 0-day sans être détecté, c'est-à-dire en exploitant une vulnérabilité logicielle ou matériel inconnue de l'éditeur concerné, mais détectée par des acteurs malveillants (ici au sein d'un programme Dell de point de récupération pour machine virtuelle). Les hackers auraient donc pu évoluer dans les réseaux de leurs cibles, voler des informations ou subvertir le fonctionnement des machines pendant 18 mois : c'est long et risqué, surtout dans un contexte où l'administration Trump souhaite désormais répondre de manière plus agressive aux cyberattaques.

Alors que se multiplient les cyberattaques dans le monde, les États n'ont pas trouvé la parade pour s'en protéger durablement ni pour dissuader leurs adversaires, qu'ils soient étatiques ou non étatiques : en 2025, l'Agence nationale de sécurité des systèmes d'information (ANSSI) a eu connaissance de 1 361 incidents de sécurité en France, contre 831 en 2022. Selon SentinelOne, le nombre moyen de cyberattaques par semaine dans le monde en 2026 est de 1 968, soit une augmentation de 18 % par rapport à 2025 et de 70 % par rapport à 2023. De même, entre 2013 et 2022, le nombre de fuites de données a augmenté de 200 %.

Afin de clarifier le propos, nous évoquons plusieurs termes proches mais distincts : les cyberattaques qui « consistent à porter atteinte à un ou plusieurs systèmes informatiques dans le but de satisfaire des intérêts malveillants », mais aussi la cyberdéfense définie comme l'« ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité ». La cyberdéfense inclut les opérations cyberoffensives – que la cyberdéfense française appelle aussi Lutte informatique offensive (LIO) ou surnomme « arme cyber » –, qui sont, par exemple, définies par Marcus Willett, ancien responsable du Government Communications Headquarters (GCHQ) britannique, comme des opérations « principalement destinées à produire un effet *via* le cyberespace plutôt qu'à recueillir des renseignements ou à assurer une protection "de pointe" des réseaux ». Selon nous, cette définition est

trop restrictive et doit inclure les opérations de renseignement par des moyens cyber, car, comme nous allons le voir, elles constituent un préalable essentiel ainsi qu'une opportunité pour des opérations cyberoffensives.

Dans ce contexte, les débats académiques et stratégiques ont soulevé la question de la possibilité de dissuader un adversaire de mener ces attaques. Les travaux pionniers de Thomas Schelling (1966) ont défini la dissuasion comme une stratégie visant à « prévenir une action par peur des conséquences », en démontrant que l'apparition de l'arme nucléaire rendait le conflit conventionnel irrationnel et qu'il convenait désormais de convaincre l'adversaire de sa détermination et de la crédibilité de sa menace de destruction en retour pour le dissuader d'une attaque. Pour sa part, Patrick Morgan (1983) a montré que cette vision était limitée, notamment en soulignant que la détermination de l'agresseur était aussi un facteur important pour établir le succès ou l'échec d'une stratégie de dissuasion. Il a donc défini la dissuasion comme une « situation dans laquelle un acteur considère attaquer, un autre le sait et énonce des menaces d'une réponse punitive, et le premier décide comment agir, en gardant en tête ces menaces ». Joseph Henrotin définit la dissuasion comme un « mode préventif de la stratégie d'interdiction se donnant pour but de détourner un adversaire d'une initiative en lui faisant prendre conscience que l'entreprise qu'il projette est irrationnelle ». En France, on théorise la dissuasion par punition, en lien avec sa dimension nucléaire. Comme le rappelle David Pappalardo, elle inclut aussi des approches variées, qu'il s'agisse de la dissuasion par déni (diminuer les chances de succès adverses), par résilience (réduire ses gains) ou par imposition de coûts directs et collectifs (accroître le coût de son action). Toutefois, nous pouvons nous demander si les opérations cyberoffensives peuvent seulement être dissuadées d'une manière qui se rapprocherait de ces formes de dissuasion nucléaire ou conventionnelle ? Peut-on dissuader un acteur malveillant d'attaquer dans le cyberespace, alors même que ces pratiques se situent sous le seuil de déclenchement de la guerre ?

Nous pensons que ce n'est pas le cas et que ce débat est mal posé pour appréhender la nature des opérations cyberoffensives et, plus généralement, de la conflictualité dans le cyberespace. Dans cet article, nous tentons de montrer que les grilles analytiques de la dissuasion sont peu pertinentes pour appréhender la nature de la cyberconflictualité étatique, car ces opérations constituent avant tout des stratégies opaques, c'est-à-dire des stratégies de conflictualité mises en œuvre dans l'objectif de masquer au maximum ses objectifs, ses effets ou ses modes opératoires. Le paradigme du renseignement et de l'opacité nous apparaît sensiblement plus pertinent pour penser ces opérations, leur usage opérationnel, leur utilité stratégique et les manières de s'en défendre.

Aux origines du débat sur la dissuasion en cyber

Lorsque nous parlons de dissuasion dans le domaine cyber, nous faisons ici référence à la possibilité pour un État d'en dissuader un autre de l'attaquer dans l'espace numérique. Cette question est posée de longue date dans les débats académiques et stratégiques aux États-Unis, au sein de l'Organisation du traité de l'Atlantique Nord (OTAN) ou en France avec le concept de découragement. De la même manière que les États occidentaux parviennent aujourd'hui à dissuader généralement l'usage de la force à leur encontre, au risque de déclencher une guerre, les stratèges cherchent le moyen pour les États de se protéger durablement des cyberattaques.

La géopolitique critique lacostienne nous offre des outils pertinents pour comprendre l'émergence et la persistance d'un débat en ces termes. En effet, les représentations géopolitiques des responsables politiques américains et de la sécurité nationale expliquent le chemin théorique choisi. Aux États-Unis, ces débats pionniers sur le domaine cyber sont ainsi influencés par des représentations faussées de la conflictualité dans le cyberespace. Le film *War Games* (1983) résonnait comme un coup de tonnerre pour la classe politique américaine qui craignait que les attaques cyber puissent manipuler le dilemme nucléaire entre les États-Unis et l'Union des républiques socialistes soviétiques (URSS). En 1997, ce débat « apocalyptique » s'est prolongé et a mis en lumière, au sein d'une commission dédiée, les risques systémiques pour les infrastructures critiques vitales. Il coagule ensuite dans les années 2010, avec les craintes américaines de la surprise stratégique et de l'échec du renseignement, qui amènent le secrétaire à la Défense, Léon Panetta, à alerter sur les risques d'un « Cyber Pearl Harbor » ou le secrétaire d'État, John Kerry, à parler des hackers comme des « armes nucléaires du XXIe siècle ». Après trois décennies de réflexion théorique sur le sujet, les responsables politiques américains se persuadent que la conflictualité dans le cyberespace est en mesure d'avoir des conséquences cataclysmiques pour la société américaine.

Or, si ces représentations s'ancrent et perdurent, c'est qu'elles prennent racine dans un système de représentations plus large, au sein duquel des responsables politiques et sécuritaires américains mêlent sentiment de vulnérabilité et solutionnisme technologique. En effet, nos recherches montrent que les représentations géopolitiques américaines sont ancrées dans un sentiment de vulnérabilité, présent dès l'origine des États-Unis, et renforcé au cours des siècles qui ont suivi. Les grands chocs, tels que Pearl Harbor ou le 11 septembre 2001, les réactivent intensément. Ces représentations sont aussi fortement nourries

par un solutionnisme technologique qui, dans le cas présent, influence la lecture stratégique : les armes cyber, comme les armes nucléaires auparavant, forment une nouvelle menace technologique pour la survie du projet américain.

Ces représentations géopolitiques expliquent aussi la prégnance de la question nucléaire dans le débat stratégique étasunien. Ainsi, les enjeux cyber émergent sous l'influence des dilemmes de dissuasion du domaine nucléaire. Si les États-Unis parviennent à dissuader leurs adversaires stratégiques, en premier lieu la Russie et la Chine, de faire usage de leur arsenal nucléaire, ils devraient pouvoir en faire de même dans le domaine cyber. Cette vision persiste jusqu'en 2018, ce qui est tard pour un pays pionnier de l'informatique qui identifie le risque cyber dès 1965. Tout en mettant en lumière les spécificités de ce nouvel espace numérique et de la conflictualité qui s'y déroule, les débats peinent à sortir du cadre de la dissuasion. Les alertes des experts en cybersécurité et en cyberdéfense de la National Security Agency (NSA), dès les années 1990, ne parviennent pas à changer les termes du débat : la Russie et la Chine mènent déjà un grand nombre de cyberattaques à la fin des années 1990 et au début des années 2000, illustrant l'absence de dissuasion effective.

Ce phénomène est renforcé par une incompréhension des enjeux cyber de la part des responsables politiques. En effet, bien que ces derniers prennent les choses en main sur le plan politique dès les années 1980, la technicité du domaine le leur rend indéchiffrable. La cybersécurité, même au sein de l'État, a longtemps été considérée comme une pratique dévolue uniquement aux ingénieurs et techniciens réseaux : il ne s'agit « que » de la protection des systèmes d'information. Un métier pour les « *geeks* », et non un métier central pour la conflictualité et la résilience de nos nations. Cette incompréhension conduit les politiques, mais aussi les responsables militaires nouvellement chargés de commander ces enjeux, à réappliquer les grilles de lecture maîtrisées de la dissuasion. Si, en 2015, le président Obama négocie diplomatiquement avec la Chine pour qu'elle arrête de mener des attaques cyber, cette dernière ne s'exécute pas. En 2016, l'administration étasunienne envisage de mettre en place des bombes cyber dans les infrastructures critiques russes afin de les punir de l'ingérence dans le processus électoral et de les dissuader de recommencer. Pourtant, les Russes ont réitéré leurs attaques à chaque élection.

Prenant conscience que cette posture n'est plus tenable, et sous la pression des professionnels de la NSA et de l'US Cyber Command (CyberCom), l'administration Trump I change les règles en 2018 et permet une transformation radicale de doctrine. Le CyberCom met en œuvre une posture dite d'engagement persistant (« Persistent Engagement ») visant à mener des attaques cyber régulières contre les adversaires des États-Unis, notamment face aux menaces persistantes avancées (APT) russes, chinoises, iraniennes et nord-coréennes. Inspirée par un long travail de doctrine réalisé par la NSA et le CyberCom, en étroite articulation avec la théorie de la cyberpersistance d'Emily Goldman, de Richard Harknett et de Michael Fischerkeller, cette doctrine reste néanmoins ancrée dans le paradigme de la dissuasion : l'engagement persistant contre les adversaires doit les décourager et les amener progressivement à cesser d'attaquer les États-Unis, dans une logique de campagne militaire peu à peu dissuasive. Le jeu ne doit plus en valoir la chandelle. Sur le papier, cette doctrine est assez révolutionnaire.

Pourtant, nous pensons que son ancrage dans le paradigme de la dissuasion la rend théoriquement partiellement inadéquate, tout en étant utile sur le plan pratique. En effet, même dans une logique de campagne, force est de constater qu'en 2026, cette doctrine ne dissuade toujours pas les adversaires des États-Unis de passer à l'acte ; les attaques menées par les groupes chinois Volt Typhoon, Salt Typhoon, Silk Typhoon et Flax Typhoon le prouvent. La volonté d'une posture plus offensive de la part de l'administration Trump II ou la nécessaire mutation d'un CyberCom, encore jugé inefficace, en sont aussi des illustrations.

Pourquoi le paradigme de la dissuasion n'est-il pas pertinent ?

Chercher à dissuader un adversaire de vous attaquer dans le cyberespace nous apparaît comme une erreur d'analyse. Plusieurs facteurs, propres au cyberespace et à la nature des attaques cyber, montrent que le paradigme de la dissuasion est fragile dans ce domaine de conflictualité.

Commençons par un parallèle fort : le tabou de l'arme nucléaire n'existe pas dans le cyberespace. L'arme cyber ne fait l'objet de presque aucun tabou quant à son usage. À l'inverse, l'efficacité et le danger posé par les armes cyber sont de plus en plus grands et leur usage est de plus en plus fréquent. Il ne s'agit donc pas d'une arme de dernier recours, susceptible d'impliquer une dialectique de destruction mutuelle et de dissuasion.

Cela pose aussi le problème de l'ambiguïté et de l'attribution. Dans le cyberespace, l'attribution de la responsabilité des attaques est très difficile et requiert un savant mélange de compétences techniques et de capacités de renseignement, l'apanage de peu d'États. Il est fréquent qu'une attaque soit attribuée longtemps après qu'elle a eu lieu, mais aussi que des adversaires cherchent à se faire passer pour d'autres, dans des logiques d'attaques sous fausse bannière. Dans ce contexte, mettre en œuvre une logique de dissuasion est complexe et soumise à des risques évidents : comment répondre à une attaque dont on ne sait pas

exactement qui en est le responsable ? Comment éviter de se faire manipuler par un adversaire qui chercherait à nous faire attaquer un tiers en retour ? L'ambiguïté tactique et stratégique de l'espace numérique limite l'efficacité de la dissuasion.

Cette ambiguïté est pourtant inhérente aux cyberattaques. Une cyberattaque est d'abord une intrusion dans un système d'information : celle-ci peut avoir pour objectif de renseigner (en volant des informations) ou de se positionner (pour subvertir ou détruire le système d'information), ou les deux, l'intrusion pour espionnage étant ensuite utilisée pour subvertir ou détruire. En tout état de cause, il est impossible de distinguer la finalité d'une intrusion tant que l'adversaire ne se met pas à agir sur le système d'information. En réalité, il n'y a pas vraiment besoin de distinguer, dès lors qu'un accès en renseignement peut, en cas de changement de l'environnement stratégique, devenir un accès à des fins de subversion ou de destruction. Du point de vue de l'attaquant, on peut dès lors parler de prépositionnement, matériel comme logiciel. Ainsi, du point de vue de l'attaqué, il n'y a aucune raison de ne pas considérer toute attaque comme un éventuel levier pour de futurs effets subversifs ou destructeurs, et pas uniquement une opération d'espionnage. Là encore, la dissuasion devient difficile, car l'ambiguïté dans la nature de la cyberattaque rend difficile une réponse adaptée : détruire les infrastructures critiques d'un adversaire parce qu'il vous a espionné semble disproportionné et entraîne injustement un risque d'escalade.

La dissuasion dans le cyberespace est aussi peu effective car les opérations cyberoffensives sont complexes, coûteuses et longues à mettre en œuvre. Comme le montre très bien Max Smeets, s'il est possible de mener des attaques cyber de masse contre des systèmes d'information mal protégés à des fins criminelles ou hacktivistes, comme le subissent quotidiennement les petites entreprises ou les collectivités locales, ce type d'attaque de faible complexité menace difficilement des États. Aujourd'hui, une grande partie des systèmes d'information des États et des grandes entreprises sont bien protégés et ne peuvent devenir la cible que de cyberattaques complexes. Dans ce contexte, il est impossible d'obtenir un effet de masse ou de saturation comme le suppose la dissuasion nucléaire ou conventionnelle. L'invasion russe de l'Ukraine a bien montré l'impossibilité, pour l'heure, de soutenir un volume important d'attaques cyber complexes et efficaces.

À la différence de l'espace physique, l'espace numérique se recompose en permanence sous l'évolution des mises à jour logicielles régulières. Les lignes de code qui permettent aux couches physiques, logiques et sémantiques de fonctionner sont en perpétuelle évolution, ce qui fait apparaître de nouvelles vulnérabilités à exploiter, mais aussi disparaître d'anciennes vulnérabilités et d'anciens logiciels. Cette évolution a pour effet que la vie d'une arme cyber est limitée dans le temps : un *malware* prêt à l'usage exploite des failles qui risquent de disparaître à tout instant, tout comme un *malware* implanté dans un système d'information en vue de son usage futur pourra disparaître du jour au lendemain s'il est détecté par l'adversaire. Dans ce contexte, la dissuasion repose sur du sable, car l'accès à la cible peut disparaître à chaque instant : l'ambiguïté d'une présence ou non dans le réseau de l'adversaire est dissuasive, mais le fait qu'il sache que son réseau est nettoyable diminue logiquement cette ambiguïté. La coopération ukraino-américaine qui a précédé le déclenchement de l'invasion a fortement réduit l'exposition des systèmes ukrainiens aux *malwares* russes qui avaient été prépositionnés ou préparés pour l'invasion du 24 février 2022.

De même, le cyberespace permet une remédiation relativement rapide des systèmes d'information et des processus. Se voir détruire son système ou ses données est un immense problème pour les victimes, mais en cas de mise en œuvre de bonnes pratiques de cybersécurité, il est possible de remettre en marche rapidement des systèmes touchés voire de récupérer les données perdues. À l'extrême inverse, les conséquences d'une frappe nucléaire sont très difficiles à réparer : les souffrances humaines, matérielles et écologiques à court terme sont gigantesques et persistent à moyen et long terme. L'effet dissuasif est clair. Dans le cyber, il ne l'est plus du tout, dès lors que vous pouvez vous remettre rapidement d'une attaque.

En outre, lorsque vous tirez une arme nucléaire contre un adversaire, vous ne lui donnez pas les plans et les savoir-faire pour réaliser cette même arme. Ce constat s'applique globalement à toutes les armes conventionnelles, bien que la saisie de matériels de guerre permette des logiques de rétro-ingénierie. À l'inverse, l'usage d'une arme cyber en révèle en partie le code et le fonctionnement, ce qui favorise sa réappropriation et sa réutilisation, comme l'a bien montré l'affaire Shadow Brokers. Dans ce contexte, l'auteur de l'attaque, notamment s'il s'agit d'un État, se dissuade lui-même d'agir pour ne pas révéler ses savoir-faire et ses capacités. Il réserve ses armes cyber les plus développées pour des opérations vraiment stratégiques, à l'image de l'opération Olympic Games contre le programme nucléaire iranien attribuée à une coopération israélo-américaine. Ce constat peut s'intégrer dans une logique de dissuasion, mais freine sa résolution à agir, car le risque de prolifération et d'attaque en retour est très élevé.

Enfin, et surtout, qu'il s'agisse d'espionnage, de subversion ou de destruction, les opérations cyberoffensives recherchent une discrétion totale pour réussir et maximiser leurs effets. La recherche de cette discrétion permet difficilement d'établir un signal stratégique. Cette incohérence peut être poussée plus loin : révéler un arsenal et son déploiement sur des réseaux pour

crédibiliser sa menace reviendrait à signaler à l'adversaire quels sont les réseaux à nettoyer. Dans le domaine nucléaire, montrer son arsenal, son fonctionnement et sa capacité d'atteinte est nécessaire pour crédibiliser sa dissuasion. La position des sous-marins lanceurs d'engins n'est pas connue de l'adversaire, mais celui-ci est en mesure de savoir que ceux-ci disposent d'une portée suffisante pour frapper son territoire. Dans le domaine cyber, il est difficile de crédibiliser une menace pesant sur les infrastructures stratégiques d'un adversaire, à part mentionner son éventuelle présence, ce qui tient plus du bluff que du signal stratégique. Pour empêcher cela, il conviendrait donc de réussir à démontrer la crédibilité de son arsenal cyber, sur ses propres réseaux ou dans le cadre d'opérations révélées, tout en maintenant l'ambiguïté de la présence dans des réseaux stratégiques de l'adversaire.

L'ensemble de ces arguments nous montre que le paradigme de la dissuasion dans le cyberespace est peu pertinent. Que l'arme cyber soit intégrée à la palette de la dissuasion conventionnelle nous apparaît logique et cohérent : un État peut effectivement se montrer dissuasif avec l'ensemble de ses moyens pour dissuader un adversaire d'agir militairement contre lui. En revanche, il nous apparaît impossible de dissuader les adversaires d'agir dans le cyberespace. Alors, quel paradigme choisir ?

Le paradigme des stratégies opaques

Le paradigme des stratégies opaques, englobant notamment le renseignement et la guerre asymétrique, nous apparaît beaucoup plus adapté pour penser le rôle stratégique des cyberattaques. Nous entendons par stratégie opaque les stratégies de conflictualité mises en œuvre par un adversaire dans l'objectif de masquer au maximum ses objectifs, ses effets ou ses modes opératoires. Il s'agit plutôt, pour les acteurs mobilisant ces stratégies opaques, de maintenir une discrétion, un secret ou une ambiguïté les plus importants possibles afin de réussir leurs opérations, à la fois pour agir avec permanence, nier toute responsabilité, maintenir un effet de surprise ou maîtriser la dimension d'escalade de la conflictualité.

La nature même du cyberespace permet des opérations opaques : discrètes, secrètes ou ambiguës ; non ou faiblement attribuables ; agiles, qu'elles soient temporaires (« *in and out* ») ou cherchant un prépositionnement dans la durée en vue d'une action future. Ainsi, les opérations cyberoffensives sont bien de trois natures : soit des opérations de renseignements, soit des opérations d'action clandestine, soit des opérations spéciales. Les premières cherchent à développer des accès à des structures cibles pour collecter du renseignement. Les secondes cherchent à mettre en œuvre un effet stratégique, politique ou militaire, sans que l'auteur ou le mode opératoire ne soit attribuable. Les troisièmes cherchent une action de combat ciblée ou un effet militaire stratégique, seul ou articulé avec une manœuvre conventionnelle, par des moyens non conventionnels. L'effet recherché est le plus discret ou le plus stratégique, sous couvert de l'opacité offerte par le réseau.

Dans ce contexte, on comprend mieux pourquoi il devient difficile, voire impossible, de les empêcher, car on ne peut pas dissuader les opérations opaques des États adverses. Quel que soit le niveau de conflictualité entre deux États, la recherche de renseignements comme la planification stratégique sont permanentes et la recherche d'un effet stratégique est régulière dès lors que les opportunités apparaissent. Les stratégies opaques sont, par nature, peu escalatoires et opèrent dans une zone grise qui évite précisément le recours à la guerre conventionnelle ou à la frappe nucléaire. La grammaire n'est plus la dissuasion mutuelle, mais le contre-espionnage et la guerre asymétrique : il faut gêner son adversaire, lui couper ses accès et se prémunir contre ses effets, plutôt que d'espérer le dissuader d'arrêter d'agir. Cela recouvre à la fois la compétition de renseignements de Joshua Rovner, la subversion de Lennart Maschmeyer, mais aussi la dimension opaque et stratégique de la conflictualité asymétrique, qu'elle soit clandestine ou conventionnelle. Qu'est-ce que cela implique concrètement ?

Le renseignement est une compétition permanente et continue. Si celle-ci s'est structurée progressivement au cours des siècles, bureaucratisée au XIXe siècle et institutionnalisée au XXe siècle, cette pratique des responsables politiques et militaires a toujours eu lieu. Il n'est pas possible de la dissuader.

À ce titre, une opération cyberoffensive est à l'image d'une opération de renseignement humain (HUMINT) : il s'agit d'un processus de développement actif d'accès à l'information, à la différence du renseignement d'origine électromagnétique (SIGINT) ou du renseignement d'origine image (IMINT) qui sont des pratiques passives de collecte de l'information. Le cyber et l'HUMINT cherchent tous deux à développer un accès durable à une structure, ce qui implique, en retour, une logique de contre-espionnage pour identifier les tentatives et les succès afin d'y mettre fin.

Comme en cyber, l'accès développé en HUMINT est aussi utilisable dans le futur pour de l'action clandestine ou militaire. Les relations développées par la Central Intelligence Agency (CIA) ou la Direction générale de la sécurité extérieure (DGSE) avec l'Alliance du Nord en Afghanistan servaient, en premier lieu, à renseigner sur les actions soviétiques puis talibanes, avant de devenir des vecteurs pour de l'action clandestine ou militaire. Les opérations de renseignements, comme dans le domaine cyber,

servent à développer des accès immédiats dont l'objectif est autant d'informer que de planifier. Il s'agit toujours d'une logique de prépositionnement en vue d'un conflit, clandestin, asymétrique ou conventionnel futur.

Cette grammaire nous permet de distinguer les usages stratégiques des opérations cyberoffensives :

1. Renseignement, en collectant des informations présentes sur les systèmes d'information cibles. Cet objectif est bien la raison principale des opérations cyber, même non étatiques ;
2. Planification et modelage (*shaping*) du champ de conflictualité, qu'il s'agisse d'un modelage politique par des opérations d'influence ou de l'action clandestine, ou d'un modelage du champ de bataille pour préparer à un conflit futur, comme le propose le nouveau concept de campagne cyber de contingence (*cyber contingency campaigning*). Pour rappel, le rôle des opérations spéciales est notamment de préparer un conflit conventionnel par du renseignement et du modelage, par une action contre des cibles stratégiques et par une ouverture du théâtre opérationnel ;
3. Effet stratégique, seul ou articulé à des opérations conventionnelles. Dans le cadre d'un conflit, les opérations cyberoffensives doivent chercher à obtenir des avantages stratégiques susceptibles d'appuyer la manœuvre, plutôt que des effets tactiques ;
4. Effet politique, dans une logique d'action clandestine, d'influence et de subversion.

Dans ce contexte, les règles de l'opacité s'appliquent. Pour prévenir les attaques continues de l'adversaire, il faut accroître ses défenses, réduire sa propre exposition, gêner la manœuvre de l'adversaire, visibiliser son action, voire l'intoxiquer. Il faut augmenter le risque pour l'adversaire et prévenir sa propre vulnérabilité, en travaillant sur l'exposition (réduire la sienne, accroître celle de l'adversaire) et la résilience (l'inverse). Il s'agit donc d'une grammaire de conflictualité continue : ce n'est ni la grammaire de la dissuasion nucléaire ni celle de la guerre conventionnelle.

Se montrer plus agressif dans l'opacité

Les stratégies opaques impliquent une conflictualité permanente sous le seuil et l'absence d'une logique de dissuasion : dès lors qu'on adopte ce paradigme, pourquoi se restreindre face à des adversaires se montrant agressifs ? La nature des opérations cyberétatiques implique une conflictualité continue, dans un champ de normes et de contraintes internationales grandissant, mais qui ne pourra jamais stabiliser complètement cet espace.

Pour cette raison, nous estimons nécessaire pour la France comme pour ses alliés d'accroître significativement leur agressivité dans le cyberespace. En cohérence avec une posture stratégique réactive et défensive, elle pourrait sensiblement accroître son engagement, sans craindre l'escalade. Cette posture ne contreviendrait pas non plus à la posture diplomatique responsable de la France : le respect de nos engagements politiques et diplomatiques en matière de comportement dans le cyberespace, de respect du droit international, de proportionnalité dans les réponses aux attaques et de claire distinction entre action militaire et non militaire permet d'assurer que la grande majorité des actions des États dans le cyberespace restent contraintes. Néanmoins, ce cadre n'englobe pas, par principe, les opérations de renseignements ou les opérations clandestines, ni même militaires dès lors que ces dernières sont encadrées par un contrôle politique et juridique strict et défendable.

À quoi pourrait servir un recours plus fréquent aux opérations cyberoffensives ?

1. À renseigner pour accroître la capacité de suivi et d'anticipation de la France sur l'évolution de la situation géopolitique ;
2. À prépositionner des capacités ou développer des accès futurs, activables dans une logique d'action clandestine ou spéciale dans le futur ;
3. À saboter les capacités cyberoffensives d'un adversaire hostile ou engagé contre un allié de la France, dans une logique d'action clandestine ou spéciale ;
4. À saboter les capacités militaires ou industrielles d'un adversaire hostile ou engagé contre un allié de la France, dans une logique de guerre asymétrique ;
5. À subvertir l'espace informationnel et sémantique, afin de créer de l'incertitude et de la gêne chez un adversaire hostile ou engagé contre un allié de la France, soit directement en agissant contre les vecteurs médiatiques, soit indirectement par des actions de vol et de publication d'informations (*hack and leak*). La visibilisation des turpitudes, erreurs et corruptions des adversaires, qui peut apparaître dans des documents, échanges de mails ou discussions internes au sein des autocraties, est susceptible d'avoir des effets ;
6. À subvertir les réseaux de pouvoir, dans une logique d'action clandestine, pour mettre en lumière les dissensions et rivalités internes aux structures adverses ;
7. À créer une incertitude stratégique chez l'adversaire, notamment dans la présence supposée ou réelle dans des systèmes d'information stratégiques. L'effet causé par l'attaque Volt Typhoon dans les cercles stratégiques américains est un bon

exemple de l'effet politique possible ;

8. Enfin, et surtout, à augmenter les défenses collectives de la France et de ses alliés, en renseignant sur les outils et modes opératoires des adversaires. Ainsi, même la logique défensive impose une dimension active, tout comme dans le contre-espionnage.

*
* *

Il a été proposé, en septembre 2025, que la France et le Royaume-Uni renouent avec une tradition de guerre asymétrique issue de la Seconde Guerre mondiale en l'adaptant au cyberespace : la guerre russe contre l'Ukraine et contre l'Europe nous semble justifier la mise en œuvre d'un « Special Operations Executive » numérique (« Digital SOE »), logique proposée par Marcus Willett dans un ouvrage de novembre 2024 et qui ne concernait alors que le Royaume-Uni, afin de « mettre le feu aux infrastructures numériques et militaires russes » et d'accroître le coût de la guerre pour Moscou. Ce Digital SOE mettrait en œuvre une campagne coordonnée d'opérations cyberoffensives contre l'effort de guerre russe, avec une coordination fine entre le GCHQ britannique, la DGSE française, le Commandement pour la cyberdéfense et la National Cyber Force, chacun dans son domaine de spécialité. Cette stratégie n'est pas sans poser des défis politiques, légaux et éthiques, qui ne sont toutefois pas insurmontables. Cette logique aboutit, d'une autre manière, à l'approche par campagne proposée récemment par Richard Harknett et Monica Kello.

Afin de limiter le risque d'escalade, nous invitons le lecteur à regarder la caractérisation des actions opaques déjà menées par la Russie sur le sol français et européen depuis le début des années 2010. Comme toute stratégie opaque, la mise en œuvre d'un canal de désescalade est susceptible d'en assurer le contrôle, comme cela existe dans le domaine du renseignement.

Crédit photo : gorodenkoff

Jonathan Guiffard

Jonathan Guiffard (@joeguiffard) est chercheur indépendant, doctorant à l'Institut français de géopolitique (université Paris 8 Vincennes-Saint-Denis) et *senior fellow* à l'institut Montaigne. Ses travaux académiques portent sur les stratégies dans l'espace numérique des acteurs américains du renseignement et du cyber. Auparavant, il a travaillé 12 ans dans des ministères régaliens, développant une connaissance approfondie des enjeux diplomatiques et militaires en Afrique de l'Ouest et au Moyen-Orient, ainsi qu'une expertise des politiques publiques dans ce domaine.

Comment citer cette publication

Jonathan Guiffard, « De la dissuasion aux stratégies opaques : repenser les opérations cyberoffensives », *Le Rubicon*, vol. 6, 10 juin 2026 [https://lerubicon.org/de-la-dissuasion-aux-strategies-opaques-repenser-les-operations-cyberoffensives/].