LE RUBICON

Entre puissance et tension : l'électrification des armées face aux défis de la cybersécurité

Alexis Rapin, Kristen Csenkey | 2 mai 2024

Alors que l'électrification du secteur des transports est en plein essor, un nombre croissant d'armées à travers le monde réfléchissent à l'introduction progressive de véhicules électriques au sein de leurs flottes motorisées. Des États-Unis à l'Allemagne en passant par la France, le Royaume-Uni, ou l'Australie, les initiatives d'électrification abondent, sous différentes formes : là où certains pays priorisent l'hybridation de véhicules existants, d'autres envisagent le développement de nouvelles plateformes entièrement électriques. Bien que de nombreuses questions restent à élucider en la matière, l'électricité comme source de mobilité dans les armées est en voie de devenir une réalité. D'une valeur de 5,8 milliards de dollars en 2023, le marché mondial des véhicules électriques militaires devrait selon certaines estimations doubler d'ici 2027.

Ces initiatives d'électrification sont non seulement liées aux stratégies environnementales nationales de décarbonation, mais doivent aussi permettre de moderniser les véhicules militaires en vue de répondre à différents défis futurs. Pour autant, cette évolution soulève également un enjeu majeur, encore sous-estimé : la cybersécurité. De fait, les véhicules électriques incluent de plus en plus de systèmes embarqués informatisés, et sont dépendants d'une infrastructure de charge de plus en plus connectée. Il est clair que les vulnérabilités découlant de l'électrification et de la connectivité des véhicules varient selon les contextes et les applications envisagées. Organisations civiles et militaires diffèrent passablement dans leur emploi de tels véhicules, qu'il s'agisse de sources d'énergie, de réseaux, d'infrastructures de charge, ou de fournisseurs impliqués, entre autres.

Comme nous allons le voir, cependant, certaines vulnérabilités inhérentes à ces véhicules transcendent les secteurs, et laissent entrevoir que des acteurs malveillants puissent prochainement tenter de les exploiter, que ce soit pour collecter de l'information stratégiquement sensible, ou porter atteinte à l'efficacité opérationnelle d'une armée. Comment de tels scénarios pourraient-ils se matérialiser ? Quels pourraient être leurs impacts sur l'appareil de défense d'un État ? Et comment les forces armées peuvent-elles mieux se préparer à gérer ce défi ?

Un processus à trois vitesses : électrification, hybridation et connectivité

Il importe, dans un premier temps, de bien distinguer les différentes évolutions à l'œuvre en matière de mobilité militaire. De fait, au moins trois grands axes d'innovation peuvent actuellement être observés dans ce domaine, chacun soulevant des enjeux distincts sur le plan de la cybersécurité.

Une première évolution concerne l'adoption de véhicules proprement électriques par les appareils de défense. Pour l'heure, celle-ci concerne surtout la conversion au tout-électrique des flottes de véhicules déployés « à l'arrière », autrement dit les véhicules de soutien utilisés sur les bases d'une armée ainsi que certains engins de transport léger. C'est notamment à quoi s'emploient déjà des pays comme le Canada. Plus rares, certains projets visant le développement de véhicules de combat électriques sont toutefois aussi à l'étude sur certains segments. Aux États-Unis par exemple, GM Defense travaille actuellement sur un véhicule tactique léger intégralement électrique. En sus de diminuer l'empreinte carbone des appareils de défense, ces initiatives offrent aussi de réduire partiellement la dépendance des forces armées à un marché mondial du pétrole dont les flux et les prix demeurent largement soumis aux turpitudes de la géopolitique.

Un second axe d'innovation actuel porte sur l'hybridation progressive de véhicules de combat plus lourds. Il s'agit dans la plupart des cas de convertir des plateformes existantes à une motorisation de type « full hybride » (encore que des réflexions soient également menées quant à l'adoption de véhicules hybrides rechargeables). Ainsi, l'US Army planche par exemple actuellement sur une version hybride du véhicule blindé Stryker et même, à terme, du char de combat Abrams. Au-delà du gain escompté en termes d'efficience énergétique, ces innovations laissent entrevoir certains avantages sur le plan tactique : la réduction de l'empreinte thermique et sonore induite par une motorisation électrique partielle, par exemple, pourrait augmenter la discrétion (et donc la survivabilité) des troupes sur le champ de bataille. Les batteries haute-performance propres aux véhicules hybrides pourraient aussi contribuer à augmenter l'endurance d'unités consacrées à de la « garde silencieuse » (*silent watch*), qui mobilise des équipements de surveillance sur la longue durée, mais à l'arrêt.

Enfin, une troisième évolution majeure, qui se superpose partiellement aux deux précédentes, concerne la connectivité croissante des véhicules à usage militaire, qu'ils soient électriques, hybrides ou entièrement à combustion. Bien que globalement centrée sur la circulation massive de données, cette mue se décline sous plusieurs formes. Celle-ci inclut d'une part l'introduction dans les flottes « de l'arrière » de véhicules électriques civils qui, de par leur conception, s'avèrent très informatisés et connectés (notamment à internet). D'autre part, on observe aussi un nombre croissant de programmes visant le développement de véhicules proprement militaires « intelligents », semi-dronisés, voire autonomes, dont une bonne part sont appelés à inclure une motorisation électrique.

En quoi ces grandes évolutions actuelles de la mobilité militaire soulèvent-elles des enjeux en matière de cybersécurité ?

Des véhicules « cyber-sensibles »

Il importe de le souligner d'emblée que la vulnérabilité aux menaces cyber n'est pas le propre des véhicules électriques. Comme le montrent diverses expériences menées depuis plusieurs années, les véhicules à combustion sont eux aussi tout à fait piratables, suivant leur degré d'informatisation. C'est bien cette caractéristique, l'électronique embarquée (et la connectivité qui l'accompagne), qui fonde en grande partie la fragilité cyber d'un véhicule. Et c'est bien la démocratisation de cette électronique embarquée qui vient aujourd'hui soulever des craintes quant à la cybersécurité des automobiles. Alors que des véhicules civils de moyenne gamme comportent aujourd'hui jusqu'à 100 millions de lignes de code dans leurs logiciels de bord, les automobiles produites par l'industrie civile s'apparentent de plus en plus à des ordinateurs à quatre roues.

Cet essor de l'électronique embarquée va de pair avec une complexification des chaînes de valeur. Les véhicules connectés intègrent désormais un nombre important de logiciels, fréquemment mis à jour et provenant d'une diversité de fournisseurs. En 2020, Volkswagen estimait par exemple que 90% du code intégré à ses véhicules avait été développé par des entreprises tierces, dont le nombre dépasse parfois la cinquantaine. La chaine d'approvisionnement cyber des véhicules connectés, en d'autres termes, est actuellement très étendue et représente aussi un possible vecteur d'infection : en attaquant un petit fournisseur, des pirates pourraient par exemple piéger une mise à jour logicielle appelée à être injectée dans de nombreux véhicules. À ceci s'ajoute, pour les véhicules électriques ou hybrides rechargeables, l'enjeu d'un réseau de charge lui aussi de plus en plus informatisé et « intelligent », qui peut constituer un autre vecteur de vulnérabilité cyber.

Les différents virages adoptés par l'industrie automobile dessinent ainsi des véhicules du futur très « cyber-sensibles », dont la vulnérabilité joue sur deux niveaux. D'une part, une première catégorie de risques est générée non pas directement par l'essor de la motorisation électrique, mais par le fait que cet essor, au plan commercial et industriel, s'accompagne bien souvent d'un accroissement de facto de l'électronique embarquée. D'autre part, une seconde catégorie de risques cyber s'avère quant à elle propre à l'enjeu de la motorisation : en étant dépendants d'une infrastructure de charge elle-même de plus en plus connectée, les véhicules électriques sont parallèlement soumis à d'autres vulnérabilités cyber par l'intermédiaire de leur procédé d'alimentation.

Quels risques concrets cette nouvelle réalité génère-t-elle vis-à-vis de l'électrification des armées ? Et comment ceux-ci se déclinent-ils d'une situation à une autre ?

Des yeux sur la route : l'enjeu de la circulation des données

Un premier ensemble de risques découle de la superposition entre électrification et connectivité, et se rapporte aux flux de données transitant par les véhicules connectés. Qu'il s'agisse des véhicules électriques et connectés de l'arrière, ou de futurs systèmes d'arme « intelligents » potentiellement déployés à l'avant, nombre de véhicules militaires sont appelés à amasser et échanger de plus en plus de données. Les véhicules modernes intègrent en effet un nombre croissant de capteurs dont les signaux transmis, si interceptés, peuvent livrer du renseignement précieux à un adversaire : position et patterns de déplacement d'un véhicule via sa géolocalisation, messages échangés via ses appareils embarqués, conversations tenues à bord via kit mains libres, images filmées par les caméras de recul, etc.

Dans le domaine militaire, pirater des véhicules électriques/connectés pourrait ainsi servir aussi bien à espionner des hauts gradés qu'à suivre des mouvements d'unités ou à localiser et surveiller des installations sensibles. Hypothétiques en apparence, de tels scénarios sont néanmoins déjà pris très au sérieux par certains appareils de défense : depuis 2021 l'armée chinoise interdit la présence de Teslas sur ses installations, craignant que leurs caméras embarquées ne puissent être piratées à des fins d'espionnage.

En l'occurrence circonscrite à des véhicules électriques issus de l'industrie civile, cette problématique pourrait néanmoins s'étendre prochainement aux engins proprement militaires. Aux États-Unis par exemple, certaines voix appellent à faire de certains véhicules de combat des « Tesla kaki », à la fois électrifiés et hautement connectés. Une telle évolution soulèverait de toute évidence d'importants défis en matière de sécurité opérationnelle. Si ce virage est loin d'être acté, il importe de noter que l'engouement des appareils de défense pour l'intelligence artificielle crée des incitatifs en la matière : les armées de demain pourraient être tentées d'adopter des véhicules bardés de capteurs et hautement connectés, afin que ceux-ci servent de fermes à données destinées à nourrir et entraîner des IA.

Passagers clandestins : les menaces liées au véhicule

Un deuxième type de menace potentielle découle lui aussi de la superposition entre électrification et connectivité, mais se rapporte quant à lui à l'intégrité des systèmes embarqués des véhicules modernes. En plus de générer d'importants flots de données, ceux-ci assument aussi différentes fonctions s'étendant désormais largement au contrôle physique du véhicule : allumage/extinction des phares selon la visibilité, freinage d'urgence à proximité d'un obstacle, etc. L'essor de cette télématique automobile, sans surprise, crée divers canaux potentiels d'accès frauduleux pour les pirates informatiques. En 2015 déjà, un duo de hackers américains faisait sensation en parvenant à pirater un Jeep Cherokee et en contrôlant à distance sa transmission, son volant et ses freins.

De tels scénarios sont évidemment les plus préoccupants, en ce qu'ils laissent entrevoir que des pirates puissent mettre en danger la vie des passagers ou tenter d'infliger des dégâts à un véhicule. Ils sont toutefois loin d'être les plus probables, du fait que de telles opérations requièrent a priori un temps et une expertise considérables, et nécessitent l'existence de failles informatiques bien particulières. Des déclinaisons plus probables (parce que plus aisées) de ce genre de piratages pourraient cependant impliquer par exemple le système de démarrage de véhicules, en vue de réduire la disponibilité d'un parc motorisé. Début 2024, dans le cadre du grand exercice DEFNET, des unités françaises ont par exemple simulé la neutralisation en rase campagne d'un véhicule blindé Griffon, à la suite d'un piratage de ses systèmes embarqués.

La susceptibilité effective des véhicules militaires à ce type de menaces dépendra évidemment du degré d'informatisation qui leur sera conféré dans le futur. Pour l'heure de tels risques concernent essentiellement les flottes de véhicules

électriques/connectés de l'arrière, dont l'importance opérationnelle pour une armée est moindre. Deux faits importants sont néanmoins à considérer. D'une part, l'adoption de véhicules tactiques inspirés de modèles commerciaux (à l'instar du Hummer électrique développé par GM Defense pour l'US Army) laisse entrevoir que des failles cyber issues de l'industrie civile puissent *in fine* être exploitables contre des forces armées. D'autre part, l'intérêt grandissant pour des véhicules militaires « intelligents » ou dronisés soulèvera immanquablement des enjeux de ce type. En 2011 déjà, l'Iran parvenait à prendre possession d'un drone d'observation américain, après avoir piraté à distance son système de guidage pour l'amener à atterrir sur une base iranienne. Ce qui est téléopéré est par définition connecté, et ce qui est connecté est par essence piratable.

Entre circuit court et court-circuit : l'enjeu des infrastructures de charge

Enfin, un troisième type de menaces cyber, cette fois propre aux véhicules électriques (ou hybrides rechargeables), concerne les vulnérabilités liées aux infrastructures de charge des véhicules. Très informatisées et fréquemment connectées à internet, les bornes d'alimentation électrique représentent en effet un autre vecteur potentiel de cyberattaque. Début 2022, des pirates pro-Ukraine sont par exemple parvenus à compromettre des stations de charge en Russie, les rendant inutilisables pour les usagers.

Or, si l'on en croit les recherches actuelles, bien d'autres scénarios sont de l'ordre du possible. D'une part, différentes études portant sur des systèmes de charge commerciaux suggèrent que les bornes pourraient dans certaines circonstances être utilisées par des hackers pour extraire des données sensibles, voire injecter des logiciels malveillants, dans un véhicule venant « faire le plein ». D'autre part, le piratage de bornes de charge pourrait aussi servir à interrompre ou empêcher un cycle de charge, ou même à en altérer le voltage en vue d'endommager le véhicule. Des acteurs malveillants pourraient donc passer par l'infrastructure de charge pour, à nouveau, s'adonner à de l'espionnage ou porter atteinte à la disponibilité d'un parc de véhicules militaires.

Si l'on peut supposer que les infrastructures de charge adoptées par les armées seront soit non-connectées à internet, soit dotées de hauts standards de sécurité, d'épineuses questions se poseront néanmoins quant aux procédures à suivre hors des installations militaires. Une analyse menée en 2021 sur les systèmes de charge domestiques commercialisés par six fournisseurs très présents sur les marchés européens et américains révélait d'ores et déjà d'importantes vulnérabilités informatiques. Autorisera-t-on les véhicules militaires à utiliser des stations de charge civiles ? Certaines seulement, ayant été vérifiées et approuvées au préalable ? Quelles seront les conditions à satisfaire en la matière ? Quid des forces déployées à l'étranger, où les standards en place pourraient être très différents ? Si l'une des grandes promesses de l'électrification est le raccourcissement et l'allègement de la chaîne logistique actuellement induite par les carburants fossiles, reste que la gestion des infrastructures de charge produira elle aussi son lot de complexités.

Pour ne rien arranger, la compromission d'infrastructures de charge pourrait aussi servir à déstabiliser voire endommager un réseau électrique tout entier. De fait, les véhicules électriques recourent de plus en plus à des systèmes de charge ultra-rapides reposant sur des puissances très importantes. Différentes études démontrent qu'une cyberattaque visant l'activation (ou la désactivation) subite et coordonnée de très nombreuses bornes de chargement pourrait amener un réseau électrique à craquer sous la pression, causant ainsi des dommages considérables. En sus des risques aux véhicules eux-mêmes, des cyberattaques contre les systèmes de charge pourraient donc également permettre à un adversaire de perturber, voire saboter des réseaux électriques de l'État visé. On mesure ainsi que le choix des systèmes de charge appelés à desservir une armée sera un processus tout aussi sensible que la sélection des véhicules électriques eux-mêmes.

Risques à géométrie variable

Ce portrait des menaces théoriques, *in fine*, ne s'applique aux armées actuelles que de manière très variable, selon les catégories de véhicules et la temporalité considérée.

L'adoption progressive de véhicules électriques civils à l'arrière, par exemple, implique que les risques induits par la circulation des données, la télématique embarquée et la vulnérabilité des infrastructures de charge sont probablement déjà une réalité. Les projets en cours d'hybridation de véhicules de combat ne sont en revanche que peu concernés, dans la mesure où ceux-ci n'impliquent pas forcément un accroissement de la connectivité des véhicules, ou une dépendance à une infrastructure de charge piratable. Il pourrait néanmoins en être autrement des projets de plus long terme, qui visent par exemple le

développement de véhicules tactiques légers 100% électriques, hybrides rechargeables, ou de véhicules plus lourds fortement connectés.

Quoi qu'il en soit, ces menaces diverses ne doivent pas nécessairement décourager les armées d'acquérir et d'opérer des véhicules électriques/connectés à l'avenir. Elles doivent toutefois susciter des réflexions quant à comment sécuriser au mieux les futurs véhicules militaires. Sur le plan purement technologique, au moins trois grands axes de prévention des risques s'offrent aux acteurs appelés à investir dans l'électrification.

Sécuriser, tester, encrypter

Le premier concerne la sécurité par design, autrement dit, l'intégration des impératifs de cybersécurité au processus de conception et de développement même des véhicules et des systèmes de charge. Cela peut passer par l'instauration de standards et de contrôles stricts imposés en amont aux fabricants, par exemple en exigeant la présence de systèmes de bord conçus pour détecter une intrusion. C'était là une des leçons majeures tirées de l'expérience du Jeep Cherokee en 2015 : les deux chercheurs avaient été en mesure de trafiquer et tester leurs altérations du code des logiciels du véhicule pendant de longs mois, sans que le système ne réagisse à une activité pourtant hautement anormale (et donc détectable). L'approche par design implique aussi une sécurisation de la chaine d'approvisionnement cyber, afin d'assurer que les composants et logiciels des futurs véhicules soient non seulement fiables, mais proviennent aussi de fournisseurs de confiance. Depuis plusieurs années maintenant, les États-Unis font la chasse aux technologies de fabrication chinoise ayant subrepticement intégré leurs systèmes d'armes au gré de la mondialisation des chaînes de valeur. Une sécurisation par design peut aider à éviter un tel scénario à l'égard des futurs véhicules électriques et/ou connectés.

Un second axe de prévention passe par le *red teaming*, c'est-à-dire l'emploi de hackers « éthiques » pour tester activement les vulnérabilités d'un système, en l'occurrence un véhicule. Les tests de pénétration, par exemple, mobilisent des hackers externes maîtrisant déjà bien un certain type de systèmes, en vue d'émuler le comportement d'un agresseur potentiel. Ceux-ci ont pour mission de chercher méthodiquement comment compromettre un véhicule, pour ensuite permettre au concepteur d'en remédier les failles. Pris au sens large, le *red teaming* peut aussi inclure des programmes de « primes au bug » (*bug bounty*), mécanisme par lequel une organisation s'engage à verser une récompense à des hackers qui lui révèlent des failles logicielles découvertes dans ses produits. Pratiqué de longue date par les géants du numérique, le *bug bounty* commence à s'étendre à l'industrie automobile : la compétition Pwn2Own Automotive, tenue pour la première fois au Japon en janvier 2024, a par exemple vu différentes équipes de pirates présenter des vulnérabilités découvertes dans des Tesla ou des stations de charge Ubiquiti et Emporia (le tout pour des primes atteignant 100'000$). Adaptées aux exigences de confidentialité propres au domaine de la défense, ces pratiques de *red teaming* pourraient aider à sécuriser de futurs véhicules électriques militaires ou leurs systèmes de charge. Aux États-Unis, le département de la Défense emploie d'ores et déjà des chercheurs en cybersécurité agrées pour mener des tests de pénétration sur certains systèmes d'armes. C'est là un exemple de mesures novatrices qui pourrait inspirer d'autres pays.

Enfin, un troisième axe de prévention passe par la sécurisation des flux de données appelés à transiter massivement par les véhicules connectés – jusqu'à 25 GB par heure pour un véhicule civil selon certaines estimations. De fait, au-delà des véhicules eux-mêmes, c'est toute l'infrastructure avec lesquels ceux-ci sont mis en réseau qui peut être porteuse de risques : objets connectés, systèmes de mise à jour à distance, serveurs communiquant avec les logiciels embarqués, etc. Le recours aux technologies d'encryption, notamment, progresse dans l'industrie automobile pour assurer la confidentialité et l'intégrité des données échangées entre les différents nœuds composant le réseau d'un véhicule connecté. L'enjeu, cependant, sera de maintenir des standards d'encryption adaptés aux constants progrès des hackers en la matière, ce qui pourrait s'avérer un défi pour des véhicules militaires dont la durée de vie opérationnelle peut atteindre 20 ou 30 ans. Le F-35 américain, archétype d'un programme d'armement de très longue haleine, fait aujourd'hui face à des vulnérabilités cyber que ses concepteurs d'origine n'auraient même pas pu imaginer. Un autre enjeu sera d'assurer au besoin la compatibilité des systèmes d'encryption avec ceux des plateformes alliées – ou tout simplement ceux d'autres services – avec qui une armée sera appelée à coopérer. La standardisation et l'harmonisation des systèmes, on le voit, seront un enjeu omniprésent dans le processus d'électrification des armées.

Travailler avec, s'entraîner sans

Sur le plan plus humain et opérationnel, d'autres mesures pourraient aussi se focaliser sur la mitigation des risques, afin de maintenir une certaine résilience au sein des armées. Une telle démarche passe par exemple par la préparation de plans de contingence en cas de cyberattaques importantes sur le parc de véhicules électriques ou l'infrastructure de charge. En d'autres termes, il s'agit de définir à l'avance la procédure à suivre si un piratage vient par exemple neutraliser les systèmes GPS d'une unité : s'être assuré au préalable que des stocks de cartes topographiques ont été maintenus pour y pallier, etc. Idéalement, il faudrait aussi que les troupes aient été minimalement préparées à faire face à ces éventualités (sur la base de cet exemple, s'assurer que les soldats soient encore capables d'utiliser une carte papier).

À ce chapitre, les armées françaises valorisent par exemple de plus en plus les entraînements en « conditions numériques dégradées ». C'est là un autre exemple de mesures innovantes dont d'autres pays peuvent s'inspirer. Cette pratique ne doit néanmoins pas se limiter au réflexe de rebasculer machinalement vers des méthodes ou équipements rudimentaires. De fait, l'un des caractères particulièrement pernicieux des cyberattaques est leur effet psychologique. En instillant simplement un doute sur l'intégrité d'un système, celles-ci peuvent dissuader une troupe d'utiliser un ensemble plus vaste de capacités, produisant ainsi un résultat disproportionné au regard des effets réels du piratage. De bons exercices en conditions dégradées devraient idéalement chercher à entraîner les armées à identifier et à juger rapidement quels systèmes demeurent fiables, lesquels sont effectivement compromis, et dans quelle mesure ceux-ci peuvent être rétablis. Il s'agit donc d'exercer autant le « sans numérique » que le « bon sens numérique ».

Conclusion : placer la barre haut

La recherche de résilience se base sur un constat en définitive incontournable : il serait illusoire d'espérer produire des véhicules électriques numériquement inattaquables. La cybersécurité est un processus intrinsèquement dynamique, dans lequel défenseurs et attaquants développent perpétuellement des répliques aux mouvements de l'autre. Les futurs véhicules militaires électriques/connectés, de même que leurs infrastructures de charge, seront donc inévitablement soumis à un constant processus de mise à jour.

L'enjeu, pour le défenseur, est cependant de placer la barre suffisamment haut au départ pour contraindre au maximum les possibilités de l'adversaire. La phase de réflexion, de planification ou de conception dans laquelle plusieurs forces armées se trouvent actuellement vis-à-vis de l'électrification constitue donc un moment clé pour penser autant que possible *en amont* la sécurité numérique des plateformes à venir.

Il s'agit d'une part de minimiser le nombre d'acteurs capables de poser une menace (pensons par exemple à des groupes armés non étatiques), et d'autre part de forcer ceux du haut du spectre à devoir consacrer d'importantes ressources à une éventuelle attaque – idéalement, à un degré tel que celle-ci présente un rapport coût/bénéfice peu avantageux. En d'autres termes, tous les investissements qu'un pays consent aujourd'hui pour sécuriser ses véhicules militaires sont probablement tous les investissements qu'un adversaire renoncera à consacrer demain pour tenter de les compromettre.

Ce travail a été soutenu par une subvention de coopération ciblée du programme MINDS (Mobilisation des idées nouvelles en matière de défense et de sécurité) du ministère de la Défense nationale du Canada, allouée à Kristen Csenkey (numéro de subvention 22-2-7). Les auteurs voudraient également remercier Mohammad Ali Sayed, ainsi que les relecteurs anonymes, pour leur contribution précieuse.

Photo : 7713Photography

•— ••— — • ••— •—• •••

Alexis Rapin, Kristen Csenkey

Kristen Csenkey est actuellement doctorante en gouvernance globale à la Balsillie School of International Affairs (Waterloo, Canada). Elle étudie la cyber-gouvernance et la gestion des technologies émergentes, tels que le quantique, l'internet des objets et les véhicules connectés. Elle agit également comme chercheuse principale sur plusieurs projets subventionnés par le ministère de la Défense nationale du Canada.

Alexis Rapin est chercheur en résidence à la Chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'Université du Québec à Montréal. Ses travaux portent notamment sur les transformations de la conflictualité, la cyberdéfense et les opérations d'influence. Il est également membre du comité éditorial du Rubicon.

Comment citer cette publication

Alexis Rapin, Kristen Csenkey, « Entre puissance et tension : l'électrification des armées face aux défis de la cybersécurité », *Le Rubicon*, 2 mai 2024 [https://lerubicon.org/entre-puissance-et-tension-lelectrification-des-armees-face-aux-defis-de-la-cybersecurite/].