LIGNES DIRECTRICES SUR LA CYBERSÉCURITÉ DES VÉHICULES AU CANADA

Transports Canada Transport Canada

Canada

This publication is also available in English under the following title Canada's Vehicle Cyber Security Guidance.

TP 15440F

TC-1006429

PRINT

Cat. No. T46-61/2020F-PDF

ISBN 978-0-660-34037-1

PDF

Cat. No. T46-61/2020F-PDF

ISBN 978-0-660-34037-1

Préparé par Transports Canada.

TABLE DES MATIÈRES

MESSAGE DU MINISTRE DES TRANSPORTS

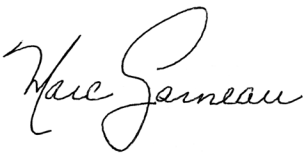
C'est avec plaisir que je vous présente les *Lignes directrices sur la cybersécurité des véhicules au Canada*, un document qui renferme des principes directeurs neutres sur le plan technologique et non normatifs en vue de garantir la cybersécurité des véhicules pour les Canadiens.

Le réseau de transport du Canada est hautement interconnecté et complexe, et chaque mode – qu'il s'agisse du transport routier, maritime, aérien ou ferroviaire – traverse une période de transformation numérique qui pourrait accroître la sécurité et l'efficacité des déplacements des biens et des personnes. Grâce aux progrès technologiques prometteurs, y compris la technologie des véhicules automatisés et connectés (VC/VA), il est possible de rehausser la sécurité sur les routes du Canada. Cependant, ces progrès technologiques entraînent de nouveaux défis sur le plan de la cybersécurité, qui soulignent l'importance d'intégrer la cyberrésilience au réseau de transport.

La cybersécurité est une responsabilité partagée entre tous les ordres de gouvernement, le secteur privé et les particuliers. La cybersécurité des véhicules est un enjeu particulièrement complexe sur lequel se penchent plusieurs partenaires horizontaux, comme les partenaires du secteur de la fabrication des véhicules et du secteur du marché secondaire. La cybersécurité soulève également d'importantes questions de sécurité pour l'avenir, car de plus en plus de véhicules sont dotés de technologies qui reposent sur la sécurité de systèmes numériques interconnectés.

Transports Canada continue de préconiser une approche axée sur la sécurité pour adopter les VC/VA, en reconnaissant le besoin de favoriser l'innovation et de conserver une attitude neutre sur le plan technologique, tout en priorisant la sécurité sur les routes. En tirant parti du solide régime de sécurité des véhicules automobiles du Canada, le Ministère continue d'adapter son cadre de réglementation en y intégrant des politiques, des directives et des outils stratégiques qui contribuent à soutenir une approche nationale flexible pour la mise à l'essai et la mise au point sécuritaires des VC/VA. Le document intitulé *Lignes directrices sur la cybersécurité des véhicules au Canada* est un important ajout à cette série d'initiatives qui peuvent aider l'industrie et les intervenants non techniques à élaborer une approche uniforme en matière de cybersécurité des VC/VA.

J'aimerais ainsi remercier les nombreux partenaires nationaux qui ont formulé des commentaires et appuyé les *Lignes directrices sur la cybersécurité des véhicules au Canada*. Je me réjouis à l'idée de poursuivre ces partenariats solides au fur et à mesure que nous collaborerons pour garantir la sécurité et la sûreté du réseau de transport du Canada pour les années à venir.



L'honorable Marc Garneau, C.P., député
Ministre des Transports

SOMMAIRE

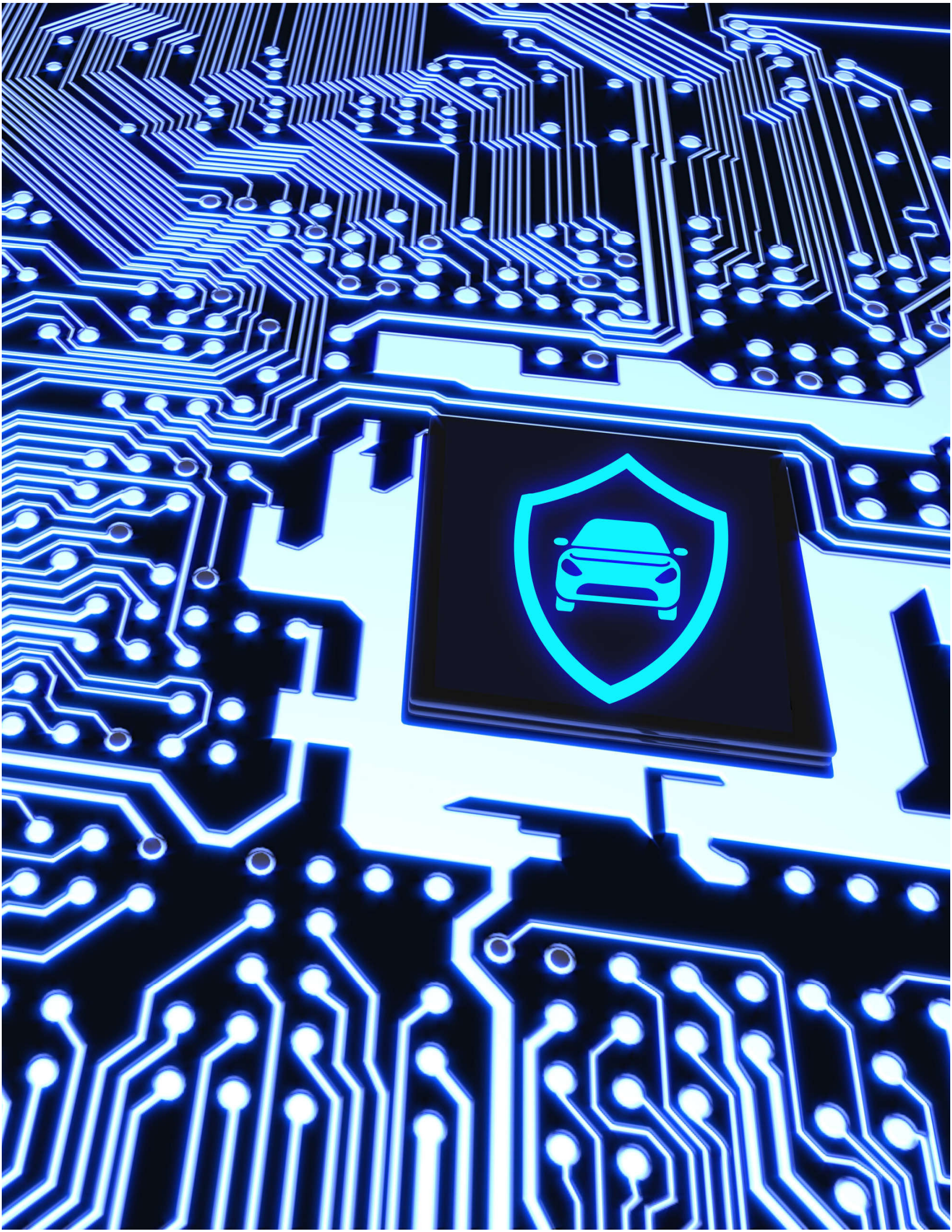
La technologie des véhicules modernes pourrait améliorer la sécurité routière pour tous les Canadiens et offrir de nouvelles formes de mobilité. Cependant, l'augmentation du nombre de fonctions automatisées et branchées fait en sorte que les menaces à l'égard de la cybersécurité des véhicules prennent de l'ampleur et deviennent de plus en plus complexes. Le document intitulé *Lignes directrices sur la cybersécurité des véhicules au Canada* (lignes directrices sur la cybersécurité) a été élaboré dans le but d'accroître la cybersécurité des véhicules au Canada.

Les *Lignes directrices sur la cybersécurité des véhicules au Canada* visent à appuyer les intervenants de l'industrie en leur fournissant des principes directeurs d'application facultative, qui sont neutres sur le plan technologique et qui ne sont pas normatifs afin de renforcer la cybersécurité à toutes les étapes du cycle de vie des véhicules. Ce document, qui tire parti sur les pratiques exemplaires actuelles dans le domaine de la cybersécurité, est basé sur une approche axée sur les risques pour aider les intervenants de l'industrie automobile à atténuer et à gérer les risques pour la cybersécurité des véhicules.

Les principes contenus dans ce document encouragent les organisations à :

- Déterminer la manière dont elles géreront les risques sur le plan de la cybersécurité;
- Protéger l'écosystème des véhicules en mettant en place des mesures de protection appropriées;
- Détecter et surveiller les événements touchant la cybersécurité et intervenir lorsque de tels événements surviennent;
- Assurer une reprise rapide et sécuritaire de leurs activités et renforcer leur sécurité à la suite d'événements mettant en cause la cybersécurité.

La sécurité et la sûreté sont inextricablement reliées dans les véhicules modernes. Le gouvernement et l'industrie sont conscients qu'il est nécessaire d'intégrer des pratiques de cybersécurité efficaces au réseau de transport pour tirer parti de tous les avantages que présentent les technologies des véhicules sur le plan de la sécurité. Qu'il s'agisse de la sécurité intégrée au concept ou de pratiques de gestion de données responsables, en passant par les considérations postérieures au déploiement, il est essentiel de prioriser la cybersécurité à toutes les étapes du cycle de vie des véhicules. Les *Lignes directrices sur la cybersécurité* soulignent l'engagement de Transports Canada à travailler en étroite collaboration avec les intervenants et les experts en cybersécurité afin d'appuyer l'introductio de nouvelles technologies de véhicules sur les rou canadiennes.



INTRODUCTION

Les technologies automobiles font leur apparition à un rythme effarant, de sorte que les véhicules modernes sont devenus des systèmes cyberphysiques très complexes. Le passage généralisé aux véhicules automatisés et connectés (VC/VA) est bien enclenché au Canada et génère des avantages énormes sur le plan de la sécurité pour les Canadiens. Parallèlement, cette transformation numérique entraîne de nouveaux défis sur le plan de la cybersécurité qui rehaussent l'importance de prioriser la cyberrésilience au sein du réseau de transport du Canada.

Avec l'aide du gouvernement, de l'industrie et des organismes de normalisation, le secteur de l'automobile a déjà réalisé des progrès importants dans le renforcement de la cybersécurité des véhicules, notamment en participant à des forums de partage d'information, en investissant dans la recherche et les essais, et en contribuant à l'élaboration de normes, de directives et d'outils. Cependant, la possibilité de cyberattaques s'accroît à mesure que les écosystèmes des véhicules deviennent de plus en plus sophistiqués et interconnectés. Il incombe donc à tous les intervenants (par exemple, les gouvernements, les associations industrielles, les fabricants, etc.) d'élaborer une approche en matière de VC/VA qui priorise la sécurité, la sûreté et la protection de la vie privée.

Afin d'exploiter le plein potentiel de sécurité des véhicules modernes, les gouvernements doivent encourager le développement et le déploiement responsables de nouvelles technologies. L'approche de TC tire parti de cadres stratégiques souples, de directives et d'outils non réglementaires, ainsi que de lois et de règlements modernisés pour appuyer les essais et le déploiement des VC/VA tout en accordant une importance primordiale à la sécurité. Les *Lignes directrices sur la cybersécurité* sont un élément clé du cadre de réglementation prospectif de TC et renferment des principes stratégiques qui devraient être pris en compte tout au long du cycle de vie des véhicules.

OBJET

Les *Lignes directrices sur la cybersécurité* répondent à un engagement clé de TC d'élaborer des lignes directrices destinées à assurer la cybersécurité dans le secteur des transports, comme il est mentionné dans le rapport de 2018 du Comité sénatorial permanent des transports et des communications.[1] Les principes qu'on retrouve dans ces lignes directrices sont conformes aux pratiques exemplaires à l'échelle internationale et représentent un cadre essentiel pour renforcer la cybersécurité des véhicules au Canada.

Les *Lignes directrices sur la cybersécurité* fournissent des principes directeurs d'application facultative, qui sont neutres sur le plan technologique et qui ne sont pas normatifs afin de renforcer la cybersécurité tout au long du cycle de vie des véhicules. Ces lignes directrices visent à aider les intervenants à développer, à déployer et à tenir à jour des technologies de véhicules cyberrésilients et à réduire la probabilité de cyberattaques contre les systèmes installés à bord des véhicules. On encourage les intervenants à lire ce document parallèlement aux pratiques exemplaires et aux normes techniques actuelles (voir l'annexe 2 : Documents de référence).

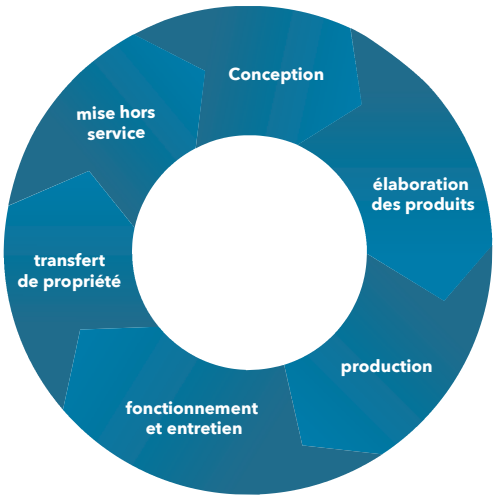
1 Source : Sénat du Canada, Paver la voie : Technologie et le futur du véhicule automatisé. Janvier 2018. https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_f.pdf (consulté le 4 juin 2019).

PORTÉE

Le présent document fournit une orientation stratégique en matière de cybersécurité pour toutes les phases du cycle de vie du véhicule et, le cas échéant, pour l'infrastructure de soutien de véhicules, y compris les systèmes d'information, les services et les données externes, mais connexes. Les lignes directrices sur la cybersécurité sont axées sur la sécurité du véhicule et/ou du produit, ce qui comprend les composants et l'information qui sont installés sur ou qui sont reliés directement au véhicule ou au produit.[2]

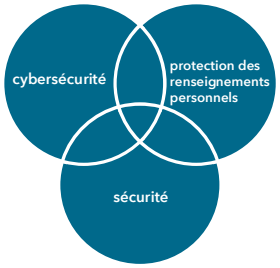
Ces lignes directrices ont été conçues principalement pour les véhicules légers de transport de passagers, quel que soit leur niveau d'automatisation, avec ou sans dispositifs connectés, y compris les véhicules plus anciens, mais peuvent également s'appliquer à d'autres types de véhicules, comme les véhicules lourds.3 Les lignes directrices s'appliquent au secteur de la postproduction, y compris les concessionnaires, les fournisseurs de pièces de rechange et les prestataires de services, et s'adresser aux personnes et aux organisations chargées de concevoir, de fabriquer, de fournir et de tenir à jour les systèmes, les logiciels et les services destinés aux véhicules automobiles et au matériel automobile.

Cycle de vie du véhicule



CONTEXTE

Les nouvelles technologies automobiles transforment le secteur du transport routier. Des véhicules de promenade aux véhicules commerciaux, les véhicules deviennent des cybersystèmes physiques sophistiqués. Souvent qualifiées d'ordinateurs sur roues, ces voitures sont munies d'unités de commande électroniques (UCE) embarquées exécutant des millions de lignes de codes qui contrôlent les systèmes mécaniques et/ou électroniques du véhicule, y compris les fonctions essentielles à la sécurité, comme le groupe motopropulseur, le freinage, le contrôle de stabilité et les systèmes de retenue supplémentaires. Parallèlement, les véhicules sont de plus en plus connectés à des dispositifs et à des infrastructures externes grâce à des technologies de communication variées, comme les réseaux cellulaires, la technologie Wi-Fi, le système Bluetooth, les systèmes de communications dédiées à courte portée (CDCP), etc. Une telle combinaison de connectivité et d'informatisation dans les véhicules modernes fait en sorte que la cybersécurité est inextricablement liée à la sécurité et à la vie privée.



Les véhicules dépendent d'une vaste gamme de renseignements essentiels et de technologies opérationnelles pour fonctionner comme prévu. La complexité croissante de l'architecture des systèmes des véhicules a donné lieu à une surface d'attaque vaste et diversifiée comportant de multiples points d'accès physiques, des interfaces de communication réseau, une gamme de capteurs, y compris LIDAR, RADAR, des caméras, des GPS et du matériel informatique, des micrologiciels et des logiciels embarqués.[4] Une atteinte à la cybersécurité, qu'elle soit délibérée ou accidentelle, pourrait avoir de graves conséquences, en compromettant par exemple la sécurité du véhicule, entre autres, l'accès non autorisé à des

2 L'infrastructure du transport routier en général constitue un élément important de l'écosystème des véhicules connectés, mais elle ne représente pas le sujet principal de cette ligne directrice. Veuillez consulter la section 5.0 - Considérations et possibilités pour le Canada où l'on décrit d'autres projets de cybersécurité liés à l'écosystème des véhicules connectés.

3 Il existe des considérations uniques sur le plan de la cybersécurité qui concernent les autres types de véhicules, comme les transporteurs routiers commerciaux (**camions commerciaux des classes 6 à 8**) et qui font appel à la norme SAE 1939 « ouverte » en matière de réseautage et de communications.

4 Pour connaître les taxonomies détaillées des menaces et des vulnérabilités auxquelles sont exposés les véhicules, consultez : Groupe de travail des Nations Unies sur la cybersécurité et la sûreté des transmissions sans fil : Ébauche de recommandation sur la

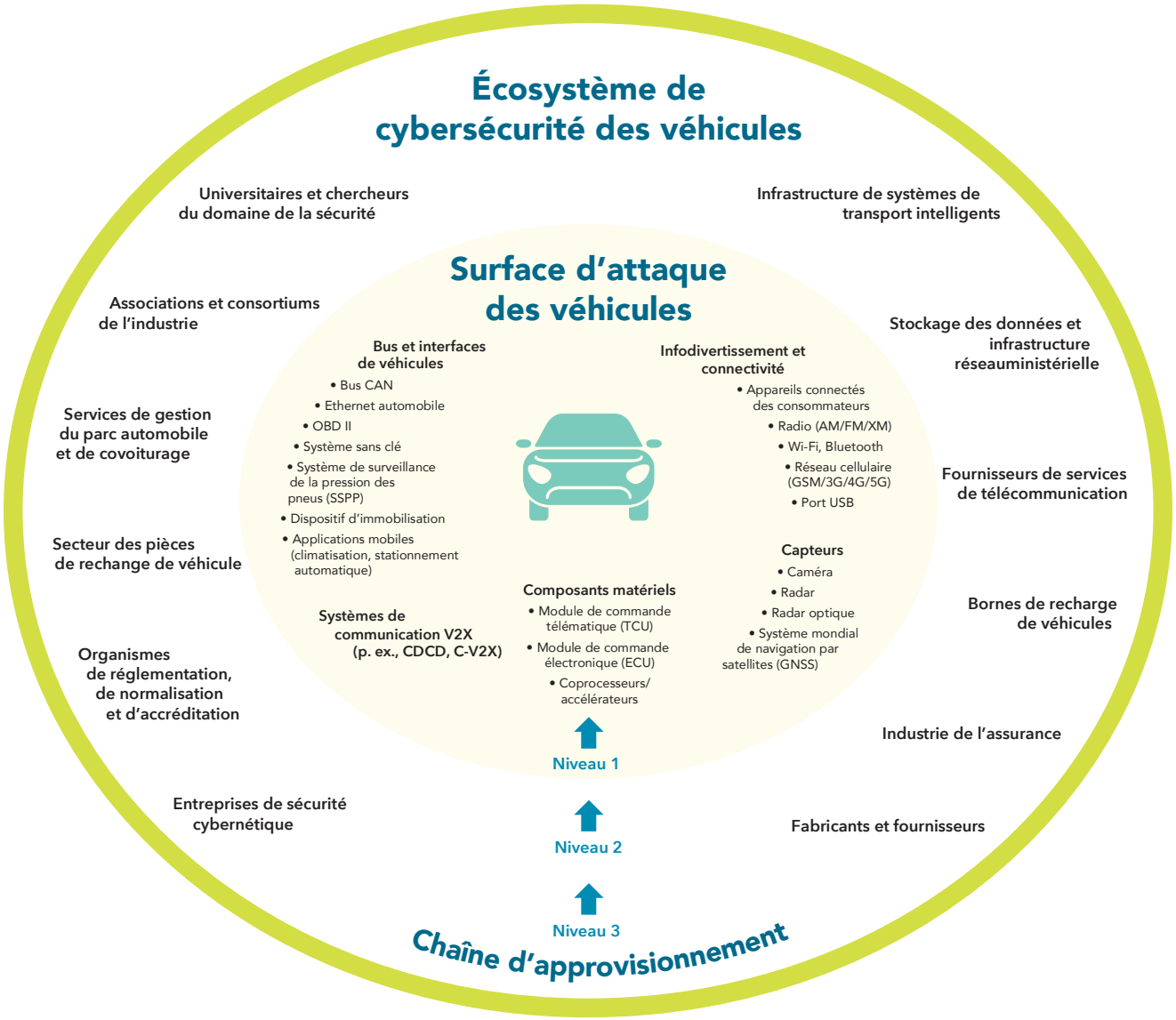
renseignements confidentiels ou le vol du véhicule. La compréhension organisationnelle du contexte de la menace visant les véhicules est primordiale afin de pouvoir gérer et atténuer de manière efficace les risques sur le plan de la cybersécurité.

Alors que les exemples les plus dramatiques de cyberattaques ont été démontrés par des chercheurs spécialisés dans le domaine de la cybersécurité (casque blanc), les cyberattaques malveillantes visant le secteur des véhicules sont à la hausse, et l'environnement riche en données généré par l'écosystème des véhicules connectés représente une cible attrayante.[5] De plus, les véhicules peuvent recueillir et traiter des quantités importantes de renseignements personnels (par exemple, communications, données de localisation, comportement du conducteur) grâce à une variété de capteurs, fonctionnalités et services embarqués. Les données représentent un élément indispensable du développement, de l'essai, du déploiement, du fonctionnement sécuritaire et de l'entretien des véhicules. La collecte, l'utilisation et la divulgation responsables des renseignements personnels constituent un volet essentiel du développement et du déploiement de nouvelles technologies automobiles.

L'environnement de cybersécurité des véhicules est complexe. Les véhicules ont un long cycle de vie au cours duquel les logiciels, les micrologiciels et le matériel devront faire l'objet d'un soutien pour demeurer cyberrésilients dans un environnement où les menaces évoluent continuellement. La fabrication et l'entretien de véhicules cyberrésilients sont d'autant plus compliqués en raison d'une chaîne d'approvisionnement multiniveaux de plus en plus non traditionnelle dans laquelle les vendeurs et les fournisseurs de services doivent prioriser la cybersécurité dans le cycle de vie de leurs produits, ainsi qu'au cours de leurs opérations pour contribuer à la sécurité et à la sûreté globales de l'écosystème. La chaîne d'approvisionnement s'étend jusqu'au secteur des pièces de rechange où les fabricants de dispositifs automobiles, les services de diagnostic et de réparation et ceux qui altèrent ou modifient des véhicules ont accès aux systèmes et aux données des véhicules. Les organisations devront unir leurs efforts pour veiller au maintien d'une interopérabilité sûre et sécuritaire des systèmes et des services des véhicules.

cybersécurité du Groupe de travail sur la cybersécurité et la sûreté des transmissions sans fil de l'UNECE WP.29 GRAVA. 9 septembre 2018 https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf; Agence de cybersécurité de l'Union européenne. ENISA Good Practices for Security of Smart Cars. Novembre 2019. https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars; prochainement, la norme technique sur la cybersécurité ISO/SAE 21434

5 Upstream Security: Upstream Security Global Automotive Cybersecurity Report 2019: Research into Smart Mobility Cyber Attack Trends. 2018 https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/



Ce graphique n'est fourni qu'à titre indicatif; il ne s'agit pas d'une liste exhaustive de la surface d'attaque des véhicules et de l'écosystème de cybersécurité des véhicules.

RÔLES ET RESPONSABILITÉS EN MATIÈRE DE CYBERSÉCURITÉ AU CANADA

Au Canada, la cybersécurité est une responsabilité partagée par tous les ordres de gouvernement, le secteur privé et les Canadiens. À l'échelle fédérale, Sécurité publique Canada (SPC) assure le leadership national en matière de cybersécurité par l'entremise de la *Stratégie nationale de cybersécurité du Canada* (Stratégie de cybersécurité), qui repose sur trois piliers : la sécurité et la résilience, l'innovation en matière de politique de cybersécurité ainsi que le leadership et la collaboration.[6] Les ministères fédéraux appuient SPC et la Stratégie de cybersécurité en supervisant la cybersécurité des infrastructures essentielles de leur secteur.

TC a élaboré une approche à plusieurs volets, qui est axée sur la sécurité, pour favoriser les essais et le déploiement sûrs et sécuritaires de nouvelles technologies automobiles, y compris les VC/VA. Le Ministère collabore avec les intervenants afin de moderniser les cadres législatif et réglementaire du Canada pour appuyer les nouvelles technologies

6 Sécurité publique Canada. Stratégie nationale de cybersécurité. 2018 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx (consulté le 4 juin 2019).

automobiles, et continue parallèlement d'élargir sa suite de politiques nationales et non réglementaires qui établissent des attentes claires pour l'essai et le déploiement sécuritaires des VC/VA au Canada. Les *Lignes directrices sur la cybersécurité* représentent un élément important de cette approche.

Le Centre canadien pour la cybersécurité (le Centre pour la cybersécurité) du Centre de la sécurité des télécommunications Canada (CST) aide TC et d'autres ministères fédéraux à gérer la cybersécurité dans leurs secteurs respectifs. Le Centre pour la cybersécurité est la source centrale de renseignements et de conseils fiables du gouvernement fédéral en matière de cybersécurité pour le gouvernement, l'industrie, les propriétaires et exploitants d'infrastructures essentielles, ainsi que le public canadien. Le Centre pour la cybersécurité compte également sur l'Unité nationale de coordination de la lutte contre la cybercriminalité (NC3) de la Gendarmerie royale du Canada (GRC). Le NC3 est une nouvelle initiative et, à ce titre, des activités de mise en œuvre sont en cours. Une fois établie, l'Unité coordonnera les opérations canadiennes d'application de la loi en matière de cybercriminalité et collaborera avec des partenaires internationaux, prodiguera des conseils et une orientation en matière d'enquêtes numériques aux services de police canadiens, produira des renseignements concrets en lien avec la cybercriminalité, et établira un nouveau mécanisme national de signalement public permettant aux Canadiens et aux entreprises de déclarer les incidents de cybercriminalité et de fraude aux organismes d'application de la loi.

Innovation, Sciences et Développement économique Canada (ISDE) joue un rôle de premier plan dans le soutien de l'introduction sûre et sécuritaire des VC/VA sur les routes canadiennes. ISDE doit établir et assurer la conformité aux normes techniques et aux exigences en matière de licences pour les technologies sans fil intégrées aux véhicules et aux infrastructures qu'on retrouve en bordure des routes. ISDE est également le ministère fédéral responsable des questions connexes concernant les données, la propriété intellectuelle et la vie privée, en plus de promouvoir l'innovation et les compétences et d'investir à ces niveaux dans les secteurs, comme la technologie numérique et la cybersécurité destinées aux automobiles et au transport. En ce qui concerne la vie privée, ISDE administre les lois fédérales sur la protection des renseignements personnels dans le secteur privé. Le ministre d'ISDE administre la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et s'assure qu'elle protège les consommateurs en plus de soutenir la croissance économique et l'innovation. Le Commissariat à la protection de la vie privée du Canada (CPVP), qui est un agent du Parlement, veille au respect de la LPRPDE.

Tous les ordres de gouvernement et l'industrie doivent promouvoir une approche nationale coordonnée en matière de cybersécurité dans le secteur des transports. Les gouvernements des provinces et des territoires supervisent bon nombre des lois et des règlements régissant l'utilisation des véhicules sur les routes publiques. Les municipalités sont responsables, à divers degrés, de la gestion du transport des passagers et, ensemble, ces ordres de gouvernement se partagent la responsabilité de l'application des lois sur la circulation et de l'adaptation des infrastructures physiques et numériques pour faciliter ainsi l'essai et le déploiement des VC/VA.

Le leadership du secteur public est nécessaire pour favoriser une harmonisation mondiale sur l'élaboration à l'échelle internationale de normes, de pratiques exemplaires en matière de cybersécurité et de règlements fondés sur des éléments probants. Les gouvernements élaborent les cadres législatifs et réglementaires appropriés qui établissent les attentes fondamentales en matière de sécurité et de sûreté et favorisent le progrès technologique continu.

CADRE LÉGISLATIF DU CANADA

Au Canada, le transport automobile est une responsabilité que se partagent les gouvernements fédéral, provinciaux et territoriaux. En vertu de la *Loi sur la sécurité automobile* (LSA), TC établit des règlements de sécurité qui s'appliquent à l'importation de véhicules automobiles et d'équipement automobile prescrit, ainsi qu'au transport de véhicules automobiles nouvellement construits et de l'équipement désigné entre les provinces et les territoires. L'objectif de ces règlements est de réduire les risques de décès, de blessures et de dommages aux biens et à l'environnement.

En vertu de la LSA, les catégories réglementaires de véhicules importés et vendus au Canada doivent être conformes au *Règlement sur la sécurité des véhicules automobiles de Canada*, ainsi qu'aux *Normes de sécurité des véhicules automobiles du Canada* (NSVAC) connexes, qui établissent une vaste gamme d'exigences de sécurité qui s'appliquent à toutes les catégories réglementaires de véhicules, y compris ceux munis des technologies des VA/VC. Les entreprises doivent certifier que tous les nouveaux véhicules et équipements fabriqués, qui sont transportés d'une province à l'autre ou importés au Canada, sont conformes aux normes de sécurité définies dans le NSVAC. Les responsables du régime de sécurité des véhicules automobiles du Canada peuvent faire appel à leurs pouvoirs d'enquête, de conformité et d'application de la loi dans les cas où une défectuosité des systèmes cyberphysiques du véhicule pourrait entraîner des problèmes de sécurité. Par exemple, lorsqu'on soupçonne un défaut de sécurité dans un véhicule, y compris tout défaut attribuable à la technologie de VC/VA, TC enquête et si le défaut existe réellement, il ordonne au fabricant de le corriger.[7]

LIGNES DIRECTRICES ET NORMES INTERNATIONALES EN MATIÈRE DE CYBERSÉCURITÉ DES VÉHICULES

Les *Lignes directrices sur la cybersécurité* reposent sur les pratiques exemplaires actuelles en matière de cybersécurité des véhicules publiées par les gouvernements, les associations industrielles, ainsi que les organismes de normalisation, et s'inspirent des lignes directrices en matière de pratiques exemplaires de l'Automotive Information Sharing and Analysis Center (Auto-ISAC)[8] qui consiste à sécuriser l'écosystème des véhicules, ainsi que des pratiques exemplaires en matière de cybersécurité des véhicules publiées par des organismes de réglementation internationaux fiables.[9]

7 Pour plus de détails sur le régime de sécurité des véhicules automobiles du Canada, veuillez consulter le Cadre de sécurité du Canada pour les véhicules automatisés et connectés https://www.tc.gc.ca/fr/services/routier/documents/tc_safety_framework_for_acv_fr-s.pdf

8 Auto-ISAC a été créé en 2015 et agit comme point central de partage, de suivi et d'analyse des renseignements sur les cybermenaces, les vulnérabilités et les incidents liés aux véhicules connectés. Auto-ISAC est présent dans le monde entier et représente 99 % de tous les véhicules légers sur la route en Amérique du Nord.

9 La National Highway Traffic Safety Administration (NHTSA) des États-Unis a publié un document de pratiques exemplaires en matière de cybersécurité pour les véhicules modernes (« Cybersecurity Best Practices for Modern Vehicles.), le Royaume-Uni a publié des principes clés de cybersécurité pour les véhicules connectés et automatisés (« The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles »), l'Association des constructeurs européens d'automobiles a publié un document sur les principes de cybersécurité automobile (« Principles of Automobile Cyber Security ») et Auto ISAC a publié des lignes directrices sur les pratiques exemplaires. En l'absence de cadres législatifs et réglementaires bien élaborés, les homologues internationaux et les experts de l'industrie ont publié des lignes directrices et des principes clés sur la cybersécurité des véhicules et des infrastructures de transport routier. Par exemple, le guide de cybersécurité sur les systèmes de véhicules cyberphysiques de la SAE, intitulé « Cybersecurity Guidebook for Cyber-Physical Vehicle Systems » (SAE J3061), a été publié en 2016 et fournit des lignes directrices générales sur la cybersécurité des véhicules pour toute leur durée du cycle de vie, tout en jetant les bases de nouvelles activités d'établissement de normes. En 2019, le Groupe de travail sur la cybersécurité et les mises à jour OTA, dans le cadre du Forum mondial de l'harmonisation des règlements concernant les véhicules des Nations Unies, a conclu la phase d'essai du projet de règlement sur la cybersécurité et les mises à jour logicielles. Le matériel d'orientation technique produit par des groupes de travail multilatéraux et des experts de renommée internationale est une ressource importante pour les intervenants qui mettent à jour leur propre cadre stratégique sur les véhicules. TC encourage également les intervenants à suivre les travaux d'élaboration de normes en cours; l'Organisation internationale de normalisation (ISO) et la Society of Automotive Engineers (SAE) International ont créé un groupe de travail pour élaborer une nouvelle norme sur la cybersécurité des véhicules qui répond mieux aux besoins et aux risques du secteur automobile. La norme proposée, ISO/SAE 21434, reflète les pratiques d'ingénierie en matière de cybersécurité et permettra aux constructeurs automobiles de faire preuve de diligence raisonnable en s'assurant que les véhicules sont raisonnablement sûrs tout au long de leur cycle de vie et en démontrant qu'ils ont adopté une approche de la cybersécurité axée sur les risques. En outre, la norme ISO 26262 porte sur la sécurité fonctionnelle des systèmes électroniques et électriques des véhicules, y compris les éventuels dysfonctionnements de ces systèmes. Étant donné la nature indissociable de la sécurité et de la sûreté, cette norme

Les lignes directrices reposent également sur le cadre de cybersécurité du National Institute of Standards and Technology (NIST) des États-Unis.[10] Le cadre de cybersécurité du NIST est un cadre volontaire conçu à l'intention des propriétaires et des exploitants d'infrastructures essentielles et s'articule autour de cinq piliers : identifier, protéger, détecter, intervenir et récupérer. Le cadre s'appuie sur un grand nombre de lignes directrices et de normes détaillées sur les pratiques exemplaires en matière de cybersécurité pour garantir la planification et le fonctionnement efficaces des systèmes d'information et des systèmes cyberphysiques essentiels.

Le Canada joue un rôle de chef de file mondial dans le domaine de l'élaboration de normes pour les technologies des VC/VA et participe activement à un certain nombre de groupes de travail dans le cadre du Groupe de travail sur les véhicules automatisés/autonomes et connectés du Forum mondial de l'harmonisation des règlements concernant les véhicules (WP.29/GRVA) des Nations Unies (N.U.). Entre autres, TC copréside le groupe de travail informel sur les méthodes de validation de la sécurité lors de la conduite automatisée (VSCA) dans le cadre du GRVA, dont le mandat est d'établir des exigences internationales en matière d'essais de sécurité pour les véhicules automatisés et est actif au sein de plusieurs autres sous-groupes du GRVA.[11]

TC surveille de près les efforts déployés à l'échelle internationale pour élaborer des normes de sécurité mondiales pour les véhicules, y compris l'ébauche de règlements élaborés par le Groupe de travail sur la cybersécurité et les mises à jour par radiocommunication sous l'égide du GRVA,[12] ainsi que la prochaine norme ISO/SAE 21434 intitulée «Road vehicles- Cybersecurity engineering» dans laquelle on définit les termes communs et les critères des pratiques de génie dans le domaine de la cybersécurité à toutes les étapes du cycle de vie des véhicules.

peut aussi être appliquée globalement à la cybersécurité des véhicules.

10 National Institute of Standards and Technology's Cyber Security Framework V.1, avril 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

11 TC joue également un rôle actif au sein des groupes de travail responsables de la définition des exigences fonctionnelles des véhicules automatisés (EFVA), des fonctions de direction à commande automatique (FDCA) et du système de freinage d'urgence automatique (SFUA) qui relèvent du GRVA.

12 TC suit également les travaux du Groupe de travail informel sur les systèmes de stockage de données pour les véhicules automatisés / enregistreur de données des événements (DSSAD/EDR) qu'on a mis sur pied sous l'égide du GRVA en juillet 2019.

LIGNES DIRECTRICES SUR LA CYBERSÉCURITÉ DES VÉHICULES : PRINCIPES CLÉS

Les *Lignes directrices sur la cybersécurité des véhicules* reposent sur une approche axée sur les risques qui permet aux organisations de toutes tailles, à divers niveaux de cybermaturité, d'appliquer les principes d'une manière compatible avec leur stratégie de gestion du risque. Une approche axée sur les risques permet de reconnaître qu'il est irréaliste d'éliminer complètement les risques sur le plan de la cybersécurité et met plutôt l'accent sur l'identification, la priorisation et la gestion du risque pour orienter la prise de mesures efficaces de réduction des risques. Les activités de gestion des risques soulignent chacun des principes, lesquels devraient être mis en application à toutes les étapes du cycle de vie d'un véhicule : conception; production, utilisation et entretien; transfert de propriété et activités en fin de vie. On recommande également d'observer une approche axée sur les risques dans l'ensemble de l'écosystème des véhicules, y compris dans la chaîne d'approvisionnement, dans le marché secondaire et dans l'infrastructure de soutien.

Les principes suivants sont destinés à un public non spécialisé et dispensent des conseils stratégiques en matière de cybersécurité destinés au secteur de la construction automobile et aux intervenants intéressés. Ils ne doivent pas être interprétés comme une norme technique ou comme une solution complète de cybersécurité des véhicules. TC (encourage les intervenants à examiner les lignes directrices sur la cybersécurité en conjonction avec les pratiques exemplaires, les lignes directrices et les normes élaborées par SP, CST, et d'autres ministères fédéraux ayant une expertise en cybersécurité, les organismes de réglementation internationaux dignes de confiance, des associations industrielles, les ressources pertinentes en cybersécurité pour les autres secteurs, et les organismes de normalisation (voir l'annexe 2 : Pratiques exemplaires en matière de cybersécurité des véhicules – Documents de référence).

1. Les organisations devraient cibler et gérer les risques sur le plan de la cybersécurité

1.1 Gouvernance de la cybersécurité

1.2 Cadres de gestion des risques

1.3 Sûreté de la chaîne d'approvisionnement

2. Les organisations devraient protéger l'écosystème du véhicule

2.1 Cyberdéfenses multidimensionnelle

2.2 Protection de la vie privée

2.3 Procédures de protection de l'information

2.4 Programmes de formation et de sensibilisation

3. Les organisations devraient détecter et surveiller les événements touchant la cybersécurité et intervenir lorsque de tels événements surviennent

3.1 Détection, surveillance et analyse des événements

3.2 Vérifications de sécurité

3.3 Plan de gestion des vulnérabilités

3.4 Gestion des incidents et intervention

4. Après un incident de cybersécurité, les organisations doivent assurer une reprise rapide et sécuritaire de leurs activités et renforcer leur sécurité

4.1 Reprise après un incident

4.2 Établissement de partenariats et partage de l'information

4.3 La cybersécurité dans le cadre d'un processus d'amélioration continue

1. LES ORGANISATIONS DEVRAIENT CIBLER ET GÉRER LES RISQUES SUR LE PLAN DE LA CYBERSÉCURITÉ

1.1 GOUVERNANCE DE LA CYBERSÉCURITÉ

La cybersécurité doit être priorisée et mise en œuvre parallèlement à la sécurité du système. Elle devrait être promue par les membres de la haute direction et transmise de manière uniforme à tout le personnel. Les organisations devraient encourager une communication ouverte sur la gestion des risques liés à la cybersécurité des produits et de l'organisation entre les équipes et entre les niveaux de travail et la direction.

Les organisations devraient élaborer des cadres de gouvernance officiels pour déterminer clairement les rôles et les responsabilités en ce qui a trait à la gestion et à l'élimination des risques pour la cybersécurité à toutes les étapes du cycle de vie des véhicules et des produits, ainsi qu'au sein même de leur structure. Le fait de rendre imputables tous les niveaux de l'organisation, y compris les cadres supérieurs, appuiera la priorité de l'entreprise accordée à la cybersécurité et contribuera à ce que les ressources financières, organisationnelles et humaines nécessaires soient affectées à la gestion efficace des risques à la cybersécurité, y compris les activités de prévention et d'atténuation des risques.

Un cadre de gouvernance rigoureux favorisera une culture organisationnelle solide et résiliente en matière de cybersécurité. Les cadres de gouvernance de la cybersécurité devraient faire régulièrement l'objet d'un examen, d'une évaluation et d'une consolidation en vertu d'un calendrier préétabli.

1.2 CADRES DE GESTION DES RISQUES

Les organisations devraient mettre en place une approche multidimensionnelle axée sur les risques en matière de cybersécurité. Les cadres de gestion des risques et les méthodologies sous-jacentes devraient être adaptés aux besoins et aux objectifs de sécurité propres à chaque organisation. La gestion des risques est un processus continu qui consiste à cerner et à analyser les risques et à intervenir. La stratégie organisationnelle de gestion des risques devrait être documentée de manière officielle en prenant soin de définir clairement les objectifs, les rôles et les responsabilités, et devrait, tout au moins, aborder les risques en matière de cybersécurité qui guettent les systèmes essentiels à la sécurité et les renseignements personnels identifiables.

Les fabricants d'équipement d'origine (FEO), les fournisseurs d'équipement et les prestataires de services devraient intégrer les processus de gestion des risques à leur cycle de vie de développement des systèmes. Des essais appropriés devraient être réalisés, à des jalons réguliers, selon un calendrier prédéterminé. (Voir le *principe 3 Les organisations devraient détecter et surveiller les événements touchant la cybersécurité et intervenir lorsque de tels événements surviennent*.)

Les FEO et les fournisseurs devraient procéder à des évaluations régulières de la menace et des risques (EMR) pour la cybersécurité à toutes les étapes du cycle de vie des produits afin de déterminer, d'évaluer et de prioriser les risques de manière systématique, y compris ceux qui sont possiblement attribuables à la chaîne d'approvisionnement (voir *Principe 1.3 Sûreté de la chaîne d'approvisionnement*). On devrait cerner les menaces, évaluer leur gravité et les éliminer par ordre de priorité.

Les stratégies de gestion des risques devraient comprendre de saines pratiques de gestion des biens. On devrait inventorier et tenir à jour les composants des véhicules, y compris les logiciels, les micrologiciels, le matériel, les connexions réseau et les interfaces, ainsi que le type de données recueillies par les véhicules. On devrait documenter la propriété des données et aviser les propriétaires de leurs responsabilités et de leurs droits à l'égard de ces données. Les biens recensés, y compris les données, devraient être évalués quant à leur valeur et à leur criticité afin que les contrôles de sûreté appropriés et fondés sur les risques puissent être mis en oeuvre.

1.3 SÛRETÉ DE LA CHAÎNE D'APPROVISIONNEMENT

Le maillon le plus faible doit être considéré pour établir le seuil minimum de sécurité. La gestion intégrée des risques de la chaîne d'approvisionnement est essentielle au bon fonctionnement des véhicules modernes. La responsabilité de la sécurisation de la chaîne d'approvisionnement de l'écosystème automobile va au-delà des FEO et doit inclure tous les niveaux de fournisseurs, sous-traitants et fournisseurs indépendants. Les évaluations de la menace et des risques devraient tenir compte de l'ensemble de la chaîne d'approvisionnement des opérations, y compris le secteur des véhicules sur le marché secondaire.

Dans tous les arrangements en matière d'acquisition, que ce soit du fabricant au fournisseur ou du fournisseur au fournisseur, les exigences et les attentes de l'organisation contractante en matière de sécurité devraient être officiellement indiquées en détail dans une entente contractuelle. Il s'agit là d'un facteur important dans le contexte des parcs de véhicules pour passagers (comme les véhicules de location) et des véhicules commerciaux.

Les fournisseurs devraient être en mesure de présenter l'assurance qu'ils ont mis en place une politique ou un programme de cybersécurité et, dans la mesure du possible, on devrait exiger une validation indépendante des produits et des processus de sécurité des fournisseurs. Les ententes contractuelles devraient également stipuler qu'on procédera de manière régulière à des vérifications et à des rapports selon un calendrier préétabli.

Les intégrateurs de systèmes devraient envisager d'établir des sources de confiance pour authentifier chaque composant du système et devraient exiger une validation de l'authenticité et de l'origine des fournitures. Toutes les organisations doivent travailler ensemble pour améliorer la sécurité de l'écosystème des véhicules, en établissant notamment des politiques responsables en matière de gestion des données. Pour favoriser une culture de cybersécurité et de partage de l'information, les FEO et les fournisseurs devraient envisager de mettre en place des programmes de divulgation des vulnérabilités et de participer activement à des forums de partage de l'information sur la cybersécurité (voir le *Principe 3.3 Plan de gestion des vulnérabilités* et le Principe *4.2 Établissement de partenariats et partage de l'information*).

2. LES ORGANISATIONS DEVRAIENT PROTÉGER L'ÉCOSYSTÈME DU VÉHICULE

2.1 CYBERDÉFENSES MULTIDIMENSIONNELLES

Les *Lignes directrices sur la cybersécurité* ne proposent pas de solutions techniques particulières, mais elles suggèrent plutôt que les organisations adoptent un modèle de défense en profondeur qui prévoit des mesures de cybersécurité à plusieurs niveaux pour éviter un point de défaillance. Les fabricants et les fournisseurs devraient s'attaquer aux défis sur le plan de la cybersécurité au moyen d'une approche de gestion du cycle de vie axée sur les risques et sur des pratiques d'ingénierie des systèmes. Ils devraient mettre en place des processus et des essais dans le but d'assurer la confidentialité, l'intégrité et la disponibilité des données à toutes les étapes du cycle de vie des véhicules. Un modèle approfondi de défense assorti de plusieurs niveaux de contrôle de sécurité contribuera à favoriser la redondance sur le plan de la sécurité et la tolérance aux pannes en plus de réduire la probabilité d'une faille sur le plan de la cybersécurité.

On devrait, pour le moins, tenir compte des objectifs de sécurité suivants tout au long du cycle de vie des véhicules.

> **Mettre en place de contrôles de sécurité appropriés**
> Les organisations devraient mettre en place des contrôles de sécurité appropriés qui contribueront à atténuer les risques et qui favoriseront une intervention efficace en cas d'incidents de cybersécurité à toutes les étapes du cycle de vie des véhicules. À tout le moins, ces contrôles devraient tenir compte des principes fondamentaux suivants : mettre en œuvre des techniques d'isolement et de séparation dans

l'architecture du système, concevoir les véhicules de façon à assurer la sécurité et la sûreté des personnes s'ils tombent en panne, établir des limites de confiance et des contrôles d'accès appropriés, et assurer l'authentification de toutes les personnes, de tous les sous-systèmes, de tous les services, de tous les messages et de toutes les parties externes; enregistrer et vérifier les journaux d'événements et de systèmes ; et prendre en charge l'authentification des dispositifs et des micrologiciels tout au long du cycle de vie des produits.

> **Sécuriser les données**
La confidentialité et l'intégrité des données, tant au repos qu'en transit, et des communications devraient être sécurisées à l'aide d'applications cryptographiques adéquates pour le degré d'assurance évalué, conformément à une approche axée sur les risques. Les politiques de gestion des données devraient différer entre les communications et les données internes et externes aux véhicules. La sensibilité des données embarquées ou à l'extérieur des véhicules devrait être protégée au moyen de techniques cryptographiques appropriées et adaptées au degré de risque évalué. La sécurité des données devrait également comprendre la suppression garantie des renseignements personnels ou de nature délicate des systèmes véhiculaires et dorsaux lors du transfert de propriété, de la mise hors service des véhicules, ainsi qu'entre les sessions d'utilisateurs lors de services de covoiturage.

> **Sécuriser les communications à l'intérieur du véhicule**
Les communications à l'intérieur des véhicules devraient être fiables et sécurisées de sorte que soient protégées l'intégrité, la disponibilité et la confidentialité des données, y compris les messages à bord qui sont essentiels pour la sécurité. Le transfert interne des messages de sécurité essentiels entre les sous-systèmes devrait suivre les principes d'isolation et de séparation dans l'architecture des systèmes du véhicule pour éviter les bus de données communs, dans la mesure du possible. Les communications, ainsi que les données au repos devraient être sécurisées et authentifiées en faisant appel à des techniques cryptographiques appropriées et adaptées au degré de risque évalué.

> **Sécuriser les communications à l'extérieur du véhicule**
Les FEO et les fournisseurs devraient adopter une politique pour valider que toutes les interfaces de communication externes entre le véhicule/produit et l'infrastructure de soutien, comme Bluetooth, Wi-Fi, 3G/4G/5G, sont sécurisées avant d'entreprendre les phases de production et de déploiement. Les dispositifs externes pouvant interagir avec les systèmes du véhicule devraient être isolés du réseau interne du véhicule et bénéficier uniquement d'un accès limité aux systèmes requis. Les interfaces de débogage ou d'essai devraient permettre un accès limité aux dispositifs de diagnostic ou de réparation authentifiés ou certifiés.

> **Gérer l'identité et le contrôle de l'accès**
Les personnes, les systèmes et les services nécessitant l'accès au véhicule et aux systèmes, aux services ou aux données de soutien, ou utiliser possiblement ceux-ci devraient être identifiés, authentifiés et autorisés au moyen d'un processus prédéfini et reproductible. On devrait toujours appliquer le concept des droits d'accès minimaux lorsqu'on accorde l'accès à des renseignements ou à des biens techniques de nature délicate, alors que la durée des sessions, ainsi que le nombre de tentatives d'authentification devraient être limités.

- **Sécuriser le développement des logiciels**
  On doit suivre des pratiques de codage sécuritaire pour réduire au minimum le nombre de vulnérabilités éventuelles des logiciels. Les organisations devraient disposer de processus documentés pour gérer, examiner et mettre à l'essai le processus d'intégration personnalisée et par des tiers. Les logiciels devraient être utilisés dans un environnement d'essai avant de faire l'objet d'un déploiement définitif, ainsi que d'un déploiement graduel avec options de reprise permettant de revenir à un état opérationnel stable dans le cas de circonstances imprévues. Les mises à jour du micrologiciel devraient habituellement interdire les reprises pour empêcher un pirate de recourir à ce mécanisme pour retourner à une version plus vulnérable. Les organisations devraient être en mesure d'identifier la version de tout logiciel ou micrologiciel dont le véhicule est muni.
- **Sécuriser les mises à jour**
  La sécurité des logiciels et des micrologiciels doit être gérée à toutes les étapes du cycle de vie du véhicule. Les organisations devraient élaborer un processus de mise à jour de la sécurité qui soutient des mises à jour sécurisées en direct et des mises à jour par radiocommunication. Un contrôle d'authentification du micrologiciel devrait être réalisé au moment de démarrer l'appareil, ainsi que lors des mises à jour. Des mécanismes devraient être mis en place afin de valider les mises à jour signées avant l'installation. Le processus devrait assurer que des mises à jour sont effectuées de manière sûre et sécuritaire et qu'un processus est en place pour informer les utilisateurs qu'une mise à jour a été effectuée ou qu'elle est prête à être installée. Les modifications apportées à la fonctionnalité du système doivent également être signalées aux utilisateurs.
- **Sécuriser l'environnement étendu du véhicule**
  Pour sécuriser l'écosystème, il est important de tenir compte des services de soutien, de l'infrastructure et des données externes. La cybersécurité devrait être mise en œuvre dans l'ensemble de l'écosystème des véhicules, y compris dans l'infrastructure de transport routier de soutien, les systèmes de gestion de la circulation, les entreprises de télécommunications, les serveurs infonuagiques et les plates-formes de gestion du parc automobile. La cybersécurité devrait également être intégrée aux secteurs du service après-vente et de l'approvisionnement, y compris les ateliers d'entretien et de réparation, les produits automobiles du marché secondaire et les dispositifs connectés.

2.2 PROTECTION DE LA VIE PRIVÉE

La gestion des risques d'atteinte à la vie privée doit être prise en compte en combinaison avec la cybersécurité à chaque étape du cycle de vie des véhicules. La LPRPDE du gouvernement fédéral établit les règles de base sur la façon de recueillir, d'utiliser ou de divulguer les renseignements personnels dans le cadre d'activités commerciales. La LPRPDE est une loi d'application générale, neutre sur le plan technologique et fondée sur des principes qui régissent tous les secteurs de l'économie. En Colombie-Britannique, en Alberta et au Québec, des lois provinciales essentiellement similaires s'appliquent aux organisations privées dans le contexte d'activités qui ont lieu uniquement dans ces provinces. Il incombe aux organisations de veiller à ce que leurs pratiques de traitement des renseignements personnels soient conformes aux lois en vigueur. Le Commissariat à la protection de la vie privée du Canada (CPVP) veille au respect de la LPRPDE, tandis que ses homologues provinciaux appliquent les lois «essentiellement similaires» des provinces. ISDE est chargée d'administrer la LPRPDE, y compris l'élaboration des politiques liées à la Loi.

En novembre 2018, un nouveau régime de déclaration obligatoire des atteintes à la protection des données est entré en vigueur en application de la LPRPDE. Il incombe maintenant aux organisations d'aviser les personnes touchées et le CPVP de toute violation des mesures de sécurité qui : 1) entraîne la perte, le vol ou l'accès non autorisé aux renseignements personnels,[13] et 2) crée un risque réel de préjudice important pour les personnes touchées. Les organisations doivent également tenir des dossiers sur toutes les atteintes à la protection des données, sans égard au risque, et fournir ces dossiers au CPVP sur demande.

Les intervenants, y compris le CPVP et ses homologues, explorent de plus en plus le besoin de mécanismes pour aider à convertir les exigences neutres sur le plan technologique des lois sur la protection des renseignements personnels, comme la LPRPDE, dans le contexte de technologies et de modèles opérationnels particuliers. . C'est particulièrement le cas pour les technologies émergentes qui présentent de nouveaux enjeux en matière de protection de la vie privée, y compris les VC/VA. Afin de donner suite à une recommandation formulée dans le rapport de 2018 du Comité sénatorial permanent des transports intitulé *Paver la voie : Technologie et le futur du véhicule automatisé*, le gouvernement s'est engagé à collaborer avec le CPVP et d'autres intervenants à l'élaboration d'un code de pratiques exemplaires en matière de protection des renseignements personnels axées spécifiquement sur l'industrie. Le gouvernement a commencé à mettre en œuvre cet engagement dans le cadre d'un processus multipartite en 2018 et en 2019, ce qui a permis de définir les éléments clés du succès qu'on devrait retrouver dans un code de pratique. De plus, ISDE a publié en 2019 un document de travail sur la réforme de la LPRPDE dans lequel on envisageait la création d'un rôle officiel pour les codes, les normes et la certification en vertu de la Loi. Les futurs efforts déployés avec les intervenants reposeront sur ce travail afin de renforcer la protection de la vie privée dans les VC/VA.

13 La LPRPDE définit les «renseignements personnels» comme des «renseignements concernant une personne identifiable»; **il n'est pas nécessaire que les renseignements soient confidentiels ou secrets** pour être considérés comme «personnels» au sens de la loi. Cette définition très large englobe une quantité importante de données dans le contexte du véhicule.

Les « renseignements personnels » sont qualifiés de « renseignements au sujet d'un individu identifiable » dans la LPRPDE; il n'est pas nécessaire que l'information soit confidentielle ou secrète pour être qualifiée de « personnelle » en vertu de la loi. Cette définition très large englobe une quantité considérable de données dans le contexte des VC/VA. La Loi renferme les exigences générales en ce qui concerne la manipulation des données qui découlent de dix principes équitables en matière d'information :

1. **Accès individuel :** Les organisations doivent, sur demande, informer les individus de l'existence, de l'utilisation et de la communication de leurs renseignements personnels.
2. **But :** La collecte, l'utilisation et la divulgation des renseignements personnels doivent se limiter à des fins raisonnables, dont les organisations doivent informer les individus au moment de la collecte.
3. **Collecte limitée :** Les organisations doivent limiter leur collecte de renseignements personnels à ce qui est nécessaire en fonction de la raison présentée à l'individu.
4. **Consentement :** Les organisations doivent obtenir le consentement des individus pour colliger, utiliser et divulguer les renseignements personnels (sous réserve de certaines exceptions).
5. **Exactitude :** Les renseignements personnels doivent être exacts, complets et à jour.
6. **Limitation de l'utilisation, de la communication et de la conservation :** Les organisations ne peuvent utiliser ou divulguer des renseignements personnels à des fins autres que celles présentées à l'individu au moment de la collecte (sous réserve de certaines exceptions).
7. **Mesures de protection :** Les organisations doivent protéger les renseignements personnels au moyen de mécanismes de protection adaptés à la nature des renseignements.
8. **Ouverture :** Les organisations doivent être ouvertes et transparentes en ce qui concerne leurs politiques et pratiques relatives à la gestion des renseignements personnels
9. **Remise en question de la conformité :** Toute personne doit être en mesure de porter plainte à l'égard du non-respect de ces exigences directement auprès de l'organisation.
10. **Responsabilité :** Les organisations sont responsables des renseignements personnels dont elles ont le contrôle et demeurent imputables de cette information si elles devaient transférer les données à un tiers organisme de traitement.

2.3 PROCÉDURES DE PROTECTION DE L'INFORMATION

Des politiques de sécurité devraient être en place afin de protéger les systèmes d'information et les biens. Les données, les codes de source, les machines virtuelles, les fichiers de configuration, les justificatifs d'identité, ainsi que les autres biens numériques essentiels devraient être sauvegardés régulièrement et de façon sécuritaire. Les sauvegardes des données, y compris la restauration et les procédures de sauvegarde, devraient faire l'objet d'essais et de vérifications périodiques pour garantir la confidentialité, l'intégrité et la disponibilité des données, ainsi que la résilience des sauvegardes en cas d'incidents mettant en cause la sécurité.

On devrait également aborder l'environnement opérationnel physique et les pratiques de gestion du personnel dans les processus de protection de l'information. Les procédures et les plans de protection de l'information devraient être documentés, y compris :

> un plan de gestion des incidents;
> un plan de gestion des vulnérabilités;
> un plan de reprise après sinistre;
> un plan de continuité des opérations.

2.4 PROGRAMMES DE FORMATION ET DE SENSIBILISATION

Une défense efficace en matière de cybersécurité nécessite une main-d'œuvre bien informée. La cybersécurité des produits est plus efficace lorsque l'organisation d'origine est elle-même protégée. Les organisations devraient élaborer un programme de sensibilisation et de formation sur la sécurité organisationnelle à l'intention de leurs employés. La formation sur la cybersécurité devrait être obligatoire pour tous les employés, y compris les cadres supérieurs et les membres de la haute direction. Afin de promouvoir une culture de la cybersécurité, son importance doit être comprise et défendue au plus haut niveau de la direction.

En plus des programmes de cybersécurité organisationnels, les organisations devraient également élaborer des programmes de formation spécialisés à l'intention des développeurs de produits et des ingénieurs. Les programmes devraient comprendre de l'information sur les vulnérabilités possibles des produits, les stratégies d'atténuation, les normes et les pratiques exemplaires actuelles sur le plan de la cybersécurité, ainsi que l'intervention en cas d'incident, les mesures d'atténuation et les activités de reprise lors d'un événement mettant en cause la cybersécurité.

Les fabricants devraient élaborer, vendre et offrir un matériel d'éducation et de sensibilisation visant à promouvoir la cyberculture des utilisateurs, des propriétaires et des opérateurs. Sur le plan de la sûreté et de la sécurité, il est important que les utilisateurs connaissent la fonctionnalité d'un véhicule ou d'un produit et le type de données recueillies pendant sa propriété, son fonctionnement et son entretien, y compris les répercussions que le transfert de propriété ou que la mise hors service d'un véhicule ont sur les données.

3. LES ORGANISATIONS DEVRAIENT DÉTECTER ET SURVEILLER LES ÉVÉNEMENTS TOUCHANT LA CYBERSÉCURITÉ ET INTERVENIR LORSQUE DE TELS ÉVÉNEMENTS SURVIENNENT

3.1 DÉTECTION, SURVEILLANCE ET ANALYSE DES ÉVÉNEMENTS

Les organisations devraient se doter d'une capacité de détection, de surveillance et d'analyse des menaces auxquelles sont exposés les systèmes et les sous-systèmes de véhicules ainsi que l'infrastructure de soutien, et devraient avoir recours aux services d'un personnel technique qualifié et formé de façon appropriée pour effectuer la détection, la surveillance et l'analyse des menaces. Les renseignements sur les menaces devraient être communiqués à l'interne et avec les intervenants externes concernés afin de maximiser leur impact.

De façon générale, la détection rapide des incidents de sécurité est liée à la capacité d'une organisation de repérer et d'analyser les activités anormales tant dans les produits (systèmes véhiculaires et dorsaux) que dans l'environnement organisationnel. Les organisations devraient établir les niveaux d'activité et les comportements de base des systèmes véhiculaires, des réseaux, des logiciels, des flux de données et d'autres processus. Les systèmes et réseaux des véhicules et les interfaces avec les systèmes et services externes devraient être surveillés pour repérer les utilisateurs et les connexions non autorisés, ainsi que toute autre activité anormale. Les registres des systèmes et des applications devraient faire l'objet d'un examen régulier afin de détecter les activités anormales ou les activités suspectes. Les organisations devraient également examiner la possibilité d'établir un centre des opérations de sécurité afin de centraliser l'information et les activités en lien avec les possibles incidents touchant la cybersécurité.

3.2 VÉRIFICATIONS DE SÉCURITÉ

L'adoption des meilleures pratiques en matière de cybersécurité des véhicules et la mise en œuvre de contrôles appropriés doivent pouvoir être assurées et vérifiées au moyen d'évaluations régulières objectives et indépendantes et de vérifications périodiques. Les organisations devraient examiner, documenter et mettre à l'essai leurs processus de cybersécurité sur une base régulière pour en vérifier l'efficacité, car le contexte de menace et le contexte opérationnel changent constamment. Par ailleurs, des autoévaluations doivent accompagner les essais de pénétration des systèmes, des réseaux et des applications, afin de déterminer les vulnérabilités qui pourraient être exploitées, et des vérifications de sécurité indépendantes doivent être effectuées régulièrement. Les documents doivent être rédigés avec la plus grande minutie et être tenus à jour durant tout le cycle de vie du véhicule, et les versions des documents doivent être contrôlées.

3.3 PLAN DE GESTION DES VULNÉRABILITÉS

Les fabricants devraient élaborer des plans de gestion des vulnérabilités pour identifier, analyser et gérer les vulnérabilités dans leur environnement opérationnel. Les plans devraient comporter des étapes sur la manière dont une organisation procédera au triage et s'attaquera aux vulnérabilités constatées sur le plan de la sécurité. Les organisations devraient également assurer une surveillance active des ressources ouvertes pour ne pas rater les alertes et les avis de sécurité.

Les programmes de divulgation des vulnérabilités constituent un moyen efficace de communiquer les vulnérabilités possibles dans l'écosystème des véhicules automobiles. Ces programmes permettent aux organisations, y compris les fournisseurs et les fabricants, de recevoir les rapports de vulnérabilité des chercheurs dans le domaine de la cybersécurité. Le fournisseur devrait suivre un programme de divulgation responsable qui permet aux chercheurs et aux autres entités de l'extérieur de découvrir les vulnérabilités que présente le système (appareils, applications mobiles ou systèmes dorsaux) pour ensuite les signaler, les suivre et les atténuer. Les programmes de vulnérabilité devraient comporter

suffisamment de dispositions juridiques pour protéger les chercheurs.

3.4 GESTION DES INCIDENTS ET INTERVENTION

Les organisations devraient suivre un plan de gestion des incidents (PGI) et procéder à des exercices réguliers pour se préparer à faire face et à réagir aux incidents touchant la cybersécurité. Le PGI devrait définir clairement les processus, les rôles et les responsabilités, ainsi que les ressources nécessaires pour enquêter et intervenir en cas d'incident; les processus permettant de déterminer, de trier et de faire passer à un niveau supérieur un incident; les mécanismes de coordination des activités techniques et opérationnelles pour obtenir, corriger et rétablir un incident; les processus pour clore les activités d'intervention.[14]

Le PGI devrait être exécuté lorsqu'un incident a été détecté et vérifié. Les avis provenant des systèmes de détection des événements de sécurité devraient être évalués, priorisés et enquêtés. Les incidents, les exploits et les vulnérabilités devraient être signalés aux intervenants internes et externes concernés. Les cyberincidents peuvent être signalés au Centre pour la cybersécurité par l'entremise du Centre de contact (contact@cyber.gc.ca). En plus du CCCS, on encourage les intervenants à partager les renseignements avec l'Auto-ISAC au profit de la communauté. Les organisations devraient signaler les incidents à leur organisme local d'application de la loi ou à la GRC lorsqu'on soupçonne un cyberincident d'être de nature criminelle. Les organisations devraient également aviser le Centre antifraude du Canada (CAFC) en composant le 1-888-495-8501 ou en écrivant à l'adresse www.antifraudcentre.ca si le cyberincident s'accompagne d'une activité frauduleuse.

On recommande de contenir tout incident impliquant la cybersécurité d'un véhicule afin de limiter son impact. Cela pourrait consister, entre autres, à bloquer temporairement les interfaces externes ou les services du réseau, à limiter les capacités des systèmes ou à fermer les systèmes du véhicule de manière sécuritaire. Après avoir contenu un incident dans le but de limiter sa gravité, on recommande de prendre sans tarder des mesures appropriées pour corriger l'incident, par exemple en procédant à l'entretien du véhicule ou en déployant une mise à jour par la voie des airs. Après avoir corrigé un incident, les organisations devraient disposer d'un moyen de rétablir la fonctionnalité du système et les opérations normales (voir le *principe 4.1 Reprise après un incident*).

4. APRÈS UN INCIDENT DE CYBERSÉCURITÉ, LES ORGANISATIONS DOIVENT ASSURER UNE REPRISE RAPIDE ET SÉCURITAIRE DE LEURS ACTIVITÉS ET RENFORCER LEUR SÉCURITÉ

4.1 REPRISE APRÈS UN INCIDENT

Après un incident, on s'attend à ce qu'une analyse soit réalisée afin de déterminer les vulnérabilités connexes, d'établir des solutions et de documenter les leçons apprises. On recommande de procéder à un diagnostic minutieux du système afin d'identifier les données modifiées, les codes modifiés ou insérés, ainsi que toute application malicieuse qui aurait pu être installée. Au besoin, on recommande de procéder à des sauvegardes afin de ramener les systèmes, les données et les incidents dans l'état qu'ils présentaient avant l'incident et d'aviser les autorités concernées. Lorsqu'on soupçonne un geste de nature criminelle, on recommande de recourir à des procédures judiciaires afin de recueillir des preuves. Advenant des répercussions plus profondes et des pannes pouvant touchant les activités ou les opérations, on devrait utiliser un plan de continuité des activités ou, s'il y a lieu, un plan de reprise après sinistre.

Les équipes de la haute direction et de gestion devraient être avisées des activités de restauration et de reprise, des échéances, des rapports d'état et des résultats. Les parties concernées devraient être

14 Auto-ISAC. Intervention en cas d'incident : Guide des pratiques exemplaires, version 1.2. 18 Janvier 2018. https://www.automotiveisac.com/best-practices/download-best-practice-guides/ (consulté le 6 juin 2019).

avisées et des communiqués appropriés devraient être remis aux partenaires, aux fournisseurs, aux utilisateurs finaux, aux autorités publiques et, dans certains cas, aux médias, afin de leur transmettre une information valide au sujet de l'événement et des mesures d'atténuation.

4.2 ÉTABLISSEMENT DE PARTENARIATS ET PARTAGE DE L'INFORMATION

Le domaine des cybermenaces est complexe. Une défense efficace en matière de cybersécurité exige une collaboration entre de multiples intervenants, y compris les fabricants d'équipement d'origine (FEO), les fournisseurs à chaque niveau de la chaîne d'approvisionnement, les fournisseurs de pièces de rechange et de services, la communauté de la sécurité, les organismes gouvernementaux et des associations de l'industrie. On encourage les organisations à échanger de l'information sur les menaces touchant les véhicules avec les pairs, les organismes du renseignement, les consommateurs et le gouvernement.

On encourage également les organisations à collaborer de près avec le gouvernement du Canada, y compris TC, le Centre pour la cybersécurité, ISDE, la GRC, les autres ministères fédéraux, ainsi que les gouvernements des provinces, des territoires et les municipalités. On encourage aussi fortement la mise sur pied de partenariats et l'échange d'information avec le secteur privé par l'entremise d'organisations, comme Auto-ISAC, qui facilite l'échange d'information entre les fabricants d'origine et les fournisseurs de l'industrie sur les questions touchant la cybersécurité.

4.3 LA CYBERSÉCURITÉ DANS LE CADRE D'UN PROCESSUS D'AMÉLIORATION CONTINUE

La cybersécurité n'est pas un état final, mais un processus d'amélioration continue. Les organisations devraient tenir à jour une base de données afin de consigner les menaces, les incidents et les leçons apprises pour se préparer et empêcher qu'un incident de cybersécurité similaire se produise dans l'avenir. Les organisations devraient améliorer et adapter continuellement leurs mécanismes et leurs processus de cybersécurité afin de s'adapter au contexte des menaces en constante évolution. Grâce à des évaluations rigoureuses, des examens de la sécurité et la mise à l'essai des processus et des contrôles de cybersécurité, les organisations continueront de renforcer leur cyberrésilience.

CONSIDÉRATIONS ET POSSIBILITÉS POUR LE CANADA

La cybersécurité des véhicules est un défi global qui doit faire l'objet d'une collaboration à l'échelle internationale. En collaborant avec ses partenaires, le Canada est bien placé pour jouer un rôle de chef de file dans le développement de technologies sûres et sécuritaires pour les véhicules. Le Canada possède un secteur bien établi dans le domaine de la fabrication d'automobiles et des capacités incomparables dans les technologies de l'information et des communications, l'intelligence artificielle et la cybersécurité. À l'avenir, tous les intervenants devront continuer d'investir afin d'attirer des talents dans le domaine de la cybersécurité et d'encourager l'innovation dans le secteur de l'automobile.

Même si la cybersécurité ne connaît, à plusieurs égards, aucune frontière, le contexte législatif et réglementaire au Canada est unique et les différentes instances devront unir leurs efforts pour établir une approche cohérente à l'échelle nationale. La sécurité des véhicules automobiles est une responsabilité que se partagent le gouvernement fédéral, les provinces et les territoires, ainsi que les municipalités, alors que chaque ordre de gouvernement joue un rôle essentiel dans la promotion de la cybersécurité des véhicules. Les lois uniques du Canada en matière de protection des renseignements personnels, notamment la LPRPDE, la *Loi sur la protection des renseignements personnels*, ainsi que les lois provinciales et municipales touchant la vie privée, présenteront également certains éléments exclusivement canadiens pour les intervenants qui conçoivent et développent des technologies de VC/VA (voir le *principe 2.2 Protection de la vie privée*). La collaboration d'ISDE avec le CPVP, y compris TC et d'autres intervenants, représente une étape importante de l'élaboration d'un code de pratiques exemplaires propres à l'industrie en matière de protection des renseignements personnels dans l'écosystème des VC/VA.

Bien qu'il y ait eu des progrès importants, le contexte de la cybersécurité des véhicules demeure complexe, et il existe des possibilités de relever les défis actuels et émergents. Par exemple, la cybersécurité des véhicules aura probablement des répercussions sur l'industrie de l'assurance, ce qui justifiera une inspection plus minutieuse en étroite collaboration avec les intervenants. Il existe également des possibilités de collaborer avec les intervenants afin de mieux comprendre et d'atténuer les risques sur le plan de la cybersécurité dans certains secteurs de l'écosystème des véhicules, comme l'infrastructure du transport routier, le créneau des pièces de rechange, y compris les ateliers d'entretien et de réparation, ainsi que les prestataires de services de télématique; et l'intelligence artificielle dans les systèmes de conduite hautement automatisés, pour n'en nommer que quelques-uns.

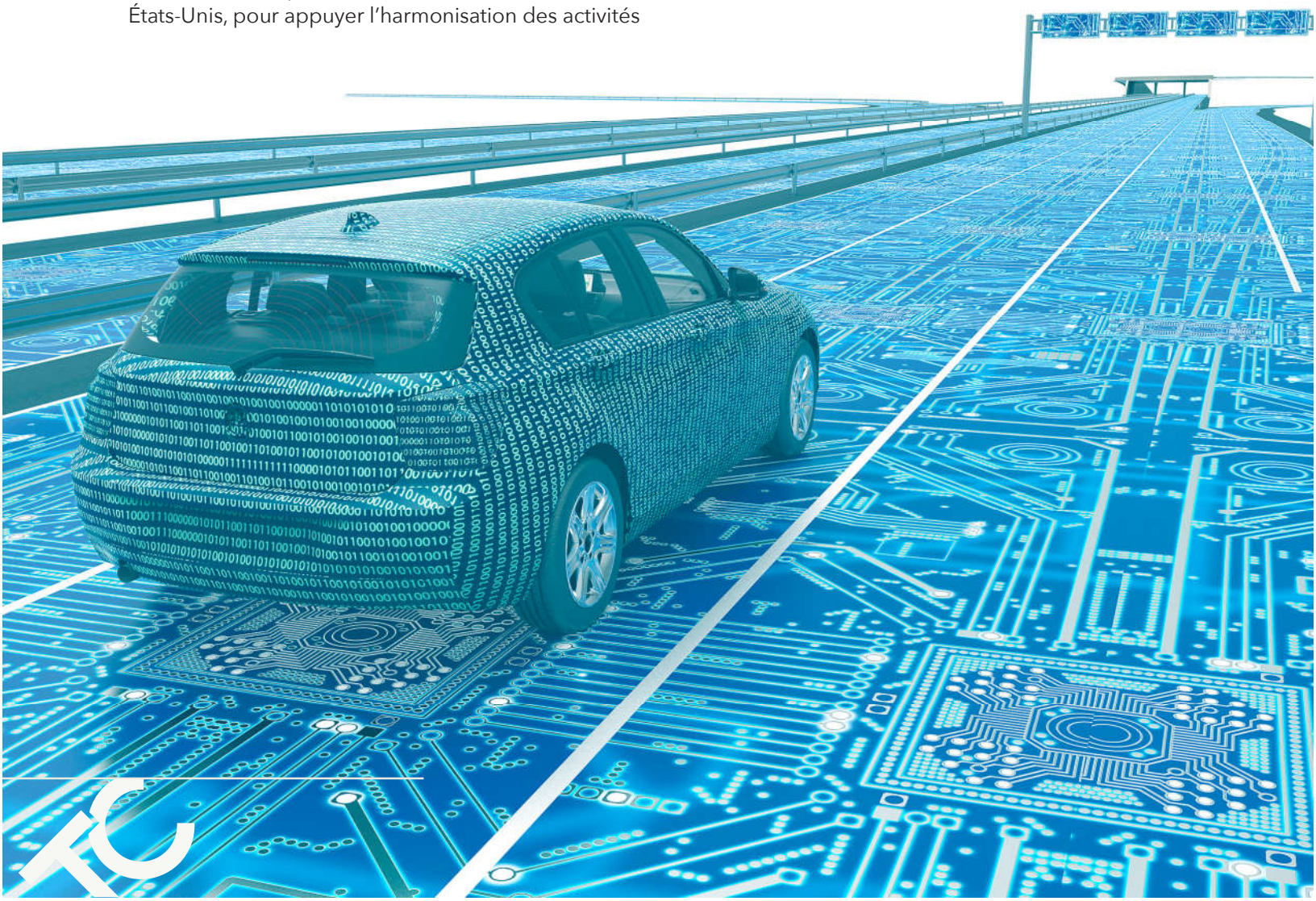
TC travaille activement à relever les nouveaux défis. Dans le contexte de la sécurité routière, TC collabore avec un vaste éventail d'intervenants de tous les ordres de gouvernement, de l'industrie et du milieu universitaire afin de soutenir la recherche et les essais dans le domaine de la cybersécurité. Les programmes de financement, dont le Programme amélioré de paiements de transfert de la Sécurité routière et le Programme de promotion de la connectivité et l'automatisation du système de transports (PCAST) de TC, peuvent être mis à profit pour soutenir la recherche et les essais que réalise le Canada sur les VC/VA, y compris les projets dans le domaine de la cybersécurité. Pour contribuer à améliorer la sécurité et la protection des renseignements personnels dans les communications des véhicules connectés, TC fait la promotion d'un cadre d'un Système de gestion des justificatifs d'identité coordonné à l'échelle nationale qui, à son tour, favorisera des communications plus sûres à partir des véhicules, ainsi que l'interopérabilité

partout en Amérique du Nord. Le Canada dispose également a attribué et harmonisé le spectre à large bande de part et d'autre de la frontière, permettant ainsi les premiers essais et projets pilotes transfrontaliers. De plus, des investissements récents dans les bancs d'essai 5G ont ouvert la voie à l'innovation.

TC est déterminé à continuer de collaborer avec des partenaires internationaux dignes de confiance et à soutenir l'élaboration de normes et de cadres harmonisés en matière de cybersécurité des véhicules. Parallèlement, le Canada continuera d'harmoniser ses efforts avec ceux des États-Unis, afin de définir des initiatives conjointes permettant de renforcer la collaboration transfrontalière dans le domaine de la cybersécurité des VC/VA. Compte tenu de la nature intégrée du marché de l'automobile et des réseaux de transport nord-américain, notamment la circulation et les échanges commerciaux transfrontaliers, ces efforts favoriseront l'interopérabilité des technologies pour VC/VA à la frontière. TC continuera de contribuer à l'élaboration de normes internationales en matière de sûreté et de sécurité des VC/VA et à exercer un leadership mondial dans ce secteur qui évolue rapidement.

CONCLUSION

Les *Lignes directrices sur la cybersécurité des véhicules au Canada* représentent une étape importante de la promotion de la cybersécurité des véhicules au Canada et établissent une base solide pour les futures possibilités de collaboration. TC est déterminé à réaliser son engagement qui consiste à poursuivre les efforts auprès des intervenants afin de surveiller les tendances et les progrès dans le domaine de la sécurité des véhicules et de tirer parti de la série actuelle de directives et d'outils pour appuyer les priorités futures en matière de cybersécurité des véhicules. Cela comprend le travail continu avec les partenaires internationaux, dont les États-Unis, pour appuyer l'harmonisation des activités de cybersécurité des véhicules, le cas échéant. De manière globale, ces efforts auront pour effet de consolider la position sur le plan de la cybersécurité des véhicules alors que nous nous efforçons de paver la voie à l'adoption sûre et sécuritaire des VC/VA au Canada.



ANNEXE I : GLOSSAIRE[15]

Attaque : Tentative d'accéder de façon non autorisée à des renseignements professionnels ou personnels, aux cybersystèmes ou aux réseaux à des fins (habituellement) criminelles. Une attaque réussie peut entraîner une faille de la sécurité ou être classée de façon générique, comme un «incident».

Auteur d'une menace : Les auteurs de cybermenaces sont des États, des groupes ou des personnes qui cherchent à tirer avantage des vulnérabilités, d'une sensibilisation insuffisante à la cybersécurité et des progrès technologiques pour obtenir un accès non autorisé aux systèmes d'information ou encore porter préjudice aux données, aux dispositifs, aux systèmes et aux réseaux des victimes.

Bluetooth : Protocole sans fil qui permet aux appareils dotés de la fonction Bluetooth de communiquer entre eux à courte distance (par exemple, 30 pieds).

Bus de réseau local contrôlé (CANbus) : Principal protocole du réseau de communication en série utilisé pour la communication entre les véhicules.

Communication dédiée à courte distance (CDCD) : Les systèmes de CDCD comprennent des liens sans fil sur de courtes distances servant à transférer les données entre des véhicules et des appareils en bordure de la route, d'autres véhicules et des appareils portables.

Confidentialité : Propriété de l'information qui n'est pas divulguée aux utilisateurs, aux procédés ou aux appareils, à moins que ceux-ci ne soient autorisés à accéder à l'information.

Contrôles de sécurité : Mesure de protection ou contremesure prescrite pour un système ou une organisation conçue dans le but de protéger la confidentialité, l'intégrité et la disponibilité de son information, ainsi que pour répondre à un ensemble d'exigences définies en matière de sécurité.

Cyberrésilience : Capacité de s'adapter à des conditions changeantes, à se préparer à faire face à une perturbation, à résister à cette perturbation et à se remettre rapidement d'une perturbation.

15 Toutes les définitions qu'on retrouve dans ce glossaire ont été consultées en décembre 2019 et proviennent des documents de source suivants : Transports Canada; Innovation, Sciences et Développement économique Canada; Glossaire du Centre canadien pour la cybersécurité https://cyber.gc.ca/fr/glossaire et page Web sur la cybermenace et auteurs de cybermenaces https://cyber.gc.ca/fr/orientation/cybermenace-et-auteurs-de-cybermenaces; Principes fondamentaux de cybersécurité à l'intention du milieu des infrastructures essentielles du Canada de Sécurité publique Canada https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-fr.aspx; Glossaire des termes communs dans le domaine de la cybersécurité de National Initiative For Cybersecurity Careers And Studies https://niccs.us-cert.gov/about-niccs/glossary#T; Glossaire de National Institute of Standards and Technology https://csrc.nist.gov/glossary; le rapport sur Paver la voie : Technologie et le futur du véhicule automatisé https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_ AutomatedVehicles_f.pdf; le page Web sur « Origin Equipment Manufacturer » de Sunpower Electronics Ltd https://www.sunpower-uk.com/glossary/what-is-an-original-equipment-manufacturer-oem/; Glossaire de la conduite autonome d'Intel https://newsroom.intel.com/ wp-content/uploads/sites/11/2017/05/ Autonomous-Driving-Glossary. pdf; Les « Cybersecurity Best Practices for Modern Vehicles » de NHTSA https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/sae2017chatipoglu_0.pdf; Les « Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA » d'UNECE https://www.unece.org/fileadmin/DAM/trans/doc/ 2018/wp29grva/GRVA-01-17.pdf.

Défense en profondeur : Mesure de sécurité des TI consistant à établir de multiples couches de protection pour assurer l'intégrité de l'information. Ces couches de protection sont généralement constituées de logiciels antivirus, de logiciels anti-espions, de coupe-feu, de mots de passe hiérarchiques, de mesures de détection des intrusions et de données biométriques.

Disponibilité : Le fait d'être accessible et utilisable sur demande.

Évaluation de la menace et des risques : Processus qui consiste à identifier les biens d'un système et la manière dont ces systèmes peuvent être compromis, et ce, tout en évaluant le niveau de risque que les menaces présentent pour les biens et à recommander ensuite des mesures de sécurité pour atténuer ces menaces.

Exploitation à distance : Exploitation d'une machine qui est victime (c'est-à-dire un véhicule ou le système d'un véhicule) en acheminant des commandes spécialement formulées à partir d'un réseau éloigné et vers un service utilisé sur cette machine dans le but de la manipuler et d'y avoir ainsi accès ou pour obtenir de l'information.

Fabricant d'équipement d'origine (FÉO) : Le FÉO concerne un produit que la société achète en vue de le réutiliser ou de l'intégrer à un autre produit en utilisant la marque du revendeur.

Infodivertissement du véhicule : Ensemble de matériel et de logiciel de divertissement à l'intérieur d'un véhicule, comme les systèmes de navigation, la radio, les lecteurs vidéo et le Wi-Fi.

Intégrité : Le fait que des renseignements, un système d'information ou un composant d'un système n'ont pas été modifiés ou détruits de manière non autorisée.

Intelligence artificielle : Sous-domaine de l'informatique ayant trait au développement de programmes informatiques aptes à résoudre des problèmes, à apprendre, à comprendre des langages, à interpréter des scènes visuelles, bref, à se comporter de façon à reproduire les facultés cognitives de l'intelligence humaine.

LIDAR : Laser pulsé qui mesure des distances variables. Dans les VA, le LIDAR rebondit sur les objets qui se trouvent à proximité (comme les piétons et les autres véhicules) pour les mapper ensuite en trois dimensions de manière à ce que le VA connaisse sa position par rapport à ces objets.

Menace : Circonstance ou événement qui a ou qui révèle la possibilité d'exploiter les vulnérabilités et d'influencer négativement (en provoquant des conséquences défavorables) sur les opérations ou les biens d'une organisation (y compris l'information et les systèmes informatiques), les individus, d'autres organisations ou la société.

Micrologiciel : Programmes informatiques et données stockés sur le matériel, qui empêchent de procéder à l'écriture ou à la modification dynamique des programmes et des données pendant l'exécution des programmes.

Mises à jour par la voie des airs : Toute méthode de transfert des données sans fil plutôt que par câble ou au moyen d'une autre connexion locale.

Modificateurs de véhicules : Entreprises modifiant les véhicules entre le moment où ils sont certifiés complets ou le moment où la production finale est terminée et certifiée, et la première vente au détail, conformément à l'article 9, Véhicule modifié, du Règlement sur la sécurité des véhicules automobiles.

Moindre privilège : Principe qui consiste à n'accorder à un individu que les privilèges nécessaires afin qu'il puisse réaliser les tâches autorisées. Ce principe limite les dommages pouvant résulter d'un accident, d'une erreur ou de l'utilisation non autorisée d'un système d'information.

Risque : Exposition à un résultat négatif advenant qu'une menace se concrétise.

Surface d'attaque : Manières dont un adversaire peut s'infiltrer dans un système et causer possiblement des dommages.

Système cyberphysique : Système constitué de réseaux sophistiqués de composants physiques et computationnels en interaction.

Technologie de l'information : Tout équipement, système ou sous-système interconnecté qui sert à effectuer l'acquisition, l'entreposage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, la commutation, l'échange, la transmission, ou la réception automatisés de données ou d'information par l'organisme de direction.

Technologie opérationnelle : Matériel et logiciels qui détectent ou provoquent un changement par la surveillance et/ou le contrôle direct des dispositifs physiques, des processus et des événements dans l'entreprise ».

Télématique : Intégration des télécommunications et de l'informatique aux applications intelligentes à l'intérieur des véhicules, comme la gestion d'un parc de véhicules.

Unité de contrôle électronique (UCÉ) : Unité intégrée au véhicule qui contrôle un ou plusieurs systèmes électriques, comme le module de commande du moteur ou l'interface homme-machine.

Véhicule automatisé (VA) : Un VA utilise une combinaison de capteurs, de contrôleurs et d'ordinateurs de bord ainsi qu'un logiciel avancé. Cela permet au véhicule de commander au moins certaines fonctions de conduite à la place d'un conducteur humain (par exemple, la direction, le freinage et l'accélération, la vérification et la surveillance de l'environnement de conduite).

Véhicule connecté : Les véhicules connectés communiquent avec leurs environs à l'aide d'un certain nombre de technologies sans fil telles que la communication dédiée à courte distance (CDCD), la technologie cellulaire de cinquième génération, le Wi-Fi, la technologie Bluetooth ou des satellites. Selon les caractéristiques installées, un véhicule branché peut communiquer avec : ses occupants, par exemple, par l'entremise de leurs appareils mobiles; avec d'autres véhicules et usagers de la route (de véhicule à véhicule (V à V); avec l'infrastructure de transport environnante, comme les routes et les feux de circulation (de véhicule à infrastructure - V à I); avec des applications en ligne et d'autres entités (véhicule à tout - V à T).

Vulnérabilité : Faille ou faiblesse dans la conception ou la mise en œuvre d'un système informatique ou son environnement qu'on pourrait exploiter afin de nuire aux biens ou aux opérations d'une organisation.

WiFi : Terme générique qui définit le réseau local sans fil et qui est conforme au protocole IEEE 802.11.

ANNEXE 2 : PRATIQUES EXEMPLAIRES EN MATIÈRE DE CYBERSÉCURITÉ DES VÉHICULES – DOCUMENTS DE RÉFÉRENCE

- Automotive Information Sharing and Analysis Centre (Auto-ISAC). 2019. Automotive Cyberse-curity Best Practices – Key Cybersecurity Functions [en anglais seulement].
- Chennakeshu, Sandeep. Blackberry. Décembre 2017. Cybersecurity for Automobiles: Black-Berry's 7-Pillar Recommendation [en anglais seulement].
- European Automobile Manufacturers Association's (ACEA). 2017. Principles of Automobile Cyber Security [en anglais seulement].
- European Union Agency for Cybersecurity (ENISA). Novembre 2019. Good Practices for Security of Smart Cars [en anglais seulement].
- ISO 27001 : Technologies de l'information – Techniques de sécurité – Systèmes de manage-ment de la sécurité de l'information – Exigences.
- ISO 27035 : Gestion des incidents de sécurité de l'information.
- ISO/SAE 21434 : Véhicules routiers – Ingénierie de la cybersécurité. (À venir)
- ISO/IEC 29147:2018 : Technologies de l'information – Techniques de sécurité – Divulgation de vulnérabilité. https://www.iso.org/fr/standard/72311.html.
- ISO/IEC 30111:2019 : Technologies de l'information – Techniques de sécurité – Processus de traitement de la vulnérabilité. https://www.iso.org/fr/standard/69725.html.
- National Motor Freight Traffic Association. RFP templates: Appendix II Cyber Security Requi-rements. https://github.com/nmfta-repo/nmfta-rfp_templates [en anglais seulement].
- National Institute of Standards and Technology. NIST Special Publication 800-53 : Security and Privacy Controls for Federal Information Systems and Organizations [en anglais seulement].
- National Institute of Standards and Technology. 16 avril 2018. Framework for Improving Critical Infrastructure Cybersecurity V1.1 [en anglais seulement].
- PAS 1885:2018. The fundamental principles of automotive cyber security. Specification [en anglais seulement].
- PAS 11281:2018. Connected automotive ecosystems. Impact of security on safety. Code of practice [en anglais seulement].
- SAE. Janvier 2016. J3061 : Cybersecurity Guidebook for Cyber-Physical Systems [en anglais seulement].
- SAE. J3101 : Requirements for Hardware Protected Security for Ground Vehicle Applications (en cours d'élaboration) [en anglais seulement].
- SAE. Juin 2018. J3138 : Diagnostic Link Connector Security [en anglais seulement].
- Transports Canada. Juin 2018. Essais des véhicules hautement automatisés au Canada : Lignes directrices à l'intention des organismes d'essais.

> Transports Canada. Février 2019. Cadre de sécurité du Canada pour les véhicules automatisés et connectés.

> Transports Canada. Février 2019. Évaluation de la sécurité des systèmes de conduite automatisés au Canada.

> CEE-ONU GRVA Groupe spécial de la cybersécurité et des questions de sûreté des transmis-sions sans fil. Proposition de recommandation sur la cybersécurité. https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02f.pdf.

> Department for Transport (DfT) du Royaume-Uni et Centre for the Protection of National In-frastructure (CPNI). Octobre 2016. The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles [en anglais seulement].

> National Highway Traffic Safety Administration (NHTSA) des États-Unis. 2016. Cybersecurity Best Practices for Modern Vehicles [en anglais seulement].