# STRATÉGIE DE CYBERSÉCURITÉ DES VÉHICULES DE TRANSPORTS CANADA

Transports Canada Transport Canada

Canada

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

TP 15473F

PDF

Cat. No. T46-62/2021F-PDF

ISBN 978-0-660-38865-6



Préparé par Transports Canada.

# Table des matières

# Message du ministre

Je suis heureux de présenter la Stratégie de cybersécurité des véhicules de Transports Canada, qui définit les priorités globales en vue de renforcer la résilience en cybersécurité des véhicules et l'infrastructure de transport routier de soutien au Canada. Ces priorités s'harmonisent avec l'engagement continu de Transports Canada à faire preuve de leadership et à collaborer avec ses partenaires pour promouvoir un écosystème de cybersécurité des véhicules sûr et résilient qui contribue à la sécurité de notre réseau de transport national.

D'un océan à l'autre, le réseau de transport routier du Canada traverse une période de profonds changements technologiques. Les véhicules connectés et automatisés représentent un énorme potentiel pour notre pays et sont capables d'améliorer considérablement la sécurité routière, d'offrir de nouvelles formes de mobilité, de stimuler la croissance économique et de réduire notre impact collectif sur l'environnement. Parallèlement, il est aussi important que nous continuions à surveiller les risques de cybersécurité résultant de l'interconnectivité et de l'automatisation accrues des véhicules et de leur environnement.

Transports Canada a été confronté à un défi déterminant : exploiter le potentiel des nouvelles technologies automobiles, qui représentent la prochaine génération dans le transport routier, tout en veillant à ce que la sécurité demeure la priorité absolue. Cette stratégie est un document de politique fondamental qui appuie l'engagement de Transports Canada à maintenir la sûreté et la sécurité des routes, en étroite collaboration avec les intervenants – l'industrie, les fabricants, le milieu universitaire, le secteur public, les organismes de normalisation et, bien sûr, les Canadiens. Cette stratégie jouera un rôle essentiel en nous aidant à comprendre le paysage complexe des menaces de cybersécurité des véhicules et à définir notre rôle dans l'écosystème numérique.

Je suis également heureux de constater que la stratégie contribue à respecter l'engagement de Transports Canada dans *Transports 2030 – Un plan stratégique pour l'avenir des transports au Canada* afin de soutenir l'utilisation de véhicules connectés et automatisés sur la voie publique pour améliorer la sécurité routière et accroître la mobilité. Notre engagement à relever les défis actuels et émergents en matière de cybersécurité dans le secteur du transport routier soutient également à la *stratégie de transformation du Ministère*.

Finalement, j'aimerais remercier les nombreux partenaires, y compris tous les ordres de gouvernement, les intervenants de l'industrie et du milieu universitaire, qui ont fait part de leurs commentaires et de leur soutien concernant la stratégie. Il est essentiel que les organisations travaillent ensemble pour gérer et atténuer les risques de cybersécurité dans ce secteur en évolution rapide, et il est encourageant de voir les progrès collectifs que nous avons réalisés jusqu'à présent. Je me réjouis à l'idée de poursuive notre collaboration, alors que nous travaillons ensemble pour réaliser les priorités communes qui aideront à assurer la sûreté et la sécurité du réseau de transport du Canada à l'avenir.

**L'honorable Omar Alghabra, C.P., député**
**Ministre des Transports**

# Résumé

Les technologies des véhicules et les infrastructures de soutien évoluent rapidement et ont le potentiel d'améliorer la sécurité routière, d'introduire de nouvelles formes de mobilité et de créer des débouchés économiques. Cette transformation numérique, combinée à un environnement de cybersécurité en constante évolution, crée également de nouveaux défis qui confirment l'importance de renforcer la cyberrésilience dans les réseaux de transport du Canada. Les véhicules connectés et automatisés (VCA) et l'infrastructure qui les prend en charge peuvent être vulnérables aux menaces de cybersécurité, ce qui signifie que la sécurité routière dépend de plus en plus de la résilience des systèmes cyberphysiques interconnectés et complexes au sein des réseaux.

La Stratégie de cybersécurité des véhicules de Transports Canada (TC) [Stratégie] établit des priorités prospectives en matière de cybersécurité des véhicules en vue de renforcer la cyberrésilience du transport routier au Canada. La Stratégie aidera le Ministère à réaliser sa vision de maintenir son rôle de chef de file en assurant la sûreté et la résilience de l'écosystème de cybersécurité automobile.

À l'appui de cette vision, la Stratégie établit trois objectifs primordiaux de cybersécurité pour le transport routier, qui, ensemble, constituent une approche robuste et tournée vers l'avenir pour renforcer la cybersécurité des véhicules au Canada.

- **Objectif 1 : Intégrer les considérations relatives à la cybersécurité des véhicules dans les cadres stratégiques et réglementaires** - TC continuera de publier des politiques et des directives neutres sur le plan technologique en ce qui a trait à la cybersécurité des véhicules, et veillera à ce que les cadres stratégiques et réglementaires demeurent agiles, afin d'appuyer l'évolution continue des besoins de l'industrie et du gouvernement.
- **Objectif 2 : Encourager la sensibilisation et favoriser une approche modernisée et novatrice en matière de cybersécurité des véhicules** - TC continuera d'intensifier la mobilisation des partenaires du gouvernement et de l'industrie; examinera les possibilités de favoriser la compréhension de la cybersécurité des véhicules et des VCA en général chez les consommateurs et de les sensibiliser sur la question; et continuera de faire progresser les initiatives en matière de recherche et d'essais.
- **Objectif 3 : Aborder les enjeux émergents et adjacents dans l'environnement de cybersécurité des véhicules** - La nature complexe et interconnectée de la cybersécurité automobile nécessite la collaboration et la coopération d'un large éventail d'intervenants, et TC continuera d'explorer les possibilités de faire face aux risques de cybersécurité dans l'écosystème plus large de la technologie du transport routier.

La cybersécurité est une responsabilité commune à tous les ordres du gouvernement, au secteur privé et aux citoyens canadiens. TC continuera de s'appuyer sur les travaux en cours avec les intervenants nationaux et internationaux pour diriger une approche coordonnée, prospective et axée sur la sécurité en ce qui a trait à la cybersécurité des véhicules. Les objectifs et les priorités définis dans ce document fournissent une feuille de route stratégique identifiant les domaines clés qui permettront de développer davantage les orientations et les outils politiques, et d'entreprendre la recherche et les tests. Parallèlement, la Stratégie de cybersécurité s'appuie sur la gamme plus large d'outils du gouvernement du Canada pour soutenir l'utilisation de technologies de véhicules sûres et d'infrastructures routières intelligentes, notamment *les Lignes directrices sur la cybersécurité des véhicules au Canada* et *la Stratégie nationale de cybersécurité de Sécurité publique*. Ensemble, ces efforts contribueront à éclairer les prochaines étapes de la cybersécurité des véhicules au Canada et complèteront l'approche plus large du Ministère pour assurer l'introduction sécuritaire des VCA.

# Introduction

La technologie du transport routier devient de plus en plus sophistiquée avec l'avènement des véhicules connectés et automatisés (VCA)[1] et de l'infrastructure intelligente de transport intelligent (ITI). Ces technologies transforment le réseau de transport du Canada et pourraient améliorer la sécurité routière, en plus d'entraîner des avantages économiques et environnementaux. En même temps, il est essentiel que le gouvernement et les intervenants suivent le rythme du paysage complexe et en évolution de la cybersécurité, afin d'atténuer les menaces et les vulnérabilités potentielles et de réaliser tout le potentiel des nouvelles technologies pour les véhicules.

La Stratégie de cybersécurité de TC définit les objectifs et les priorités qui orienteront le leadership du Ministère et son engagement continu à appuyer les efforts du gouvernement, de l'industrie et du milieu universitaire pour améliorer l'environnement de cybersécurité des véhicules. La Stratégie de cybersécurité s'harmonise avec l'approche plus large de TC pour soutenir l'introduction sûre et sécurisée des VCA, tout en complétant l'approche globale du gouvernement du Canada en matière de cybersécurité.

## Vision pour la Stratégie

Les nouvelles technologies peuvent améliorer la sécurité routière. Il est toutefois important que les processus et les mesures de protection appropriés soient mis en place pour atténuer les menaces à leur intégrité. Reconnaissant que la cybersécurité des véhicules est une responsabilité partagée, et que cette sécurité est liée inextricablement à la sûreté et à la protection des renseignements personnels, il est essentiel de se doter d'une approche axée sur la collaboration pour faire progresser le niveau de cybersécurité du Canada. TC est donc déterminé à continuer de travailler avec les intervenants, y compris tous les ordres du gouvernement, les fabricants, l'industrie et le milieu universitaire, pour établir une approche coordonnée à l'égard de la cybersécurité des véhicules. À cette fin, la Stratégie de cybersécurité a été élaborée pour répondre aux besoins actuels et à moyen terme de l'environnement de cybersécurité des véhicules et, en fin de compte, établir une orientation stratégique permettant de réaliser la vision du Ministère.

Vision : TC continuera de faire preuve de leadership et de collaborer avec ses partenaires pour promouvoir un écosystème de cybersécurité des véhicules sécuritaire et résilient à l'appui de la sécurité de notre réseau national de transport.

Pour réaliser cette vision, le Ministère a défini trois objectifs généraux en matière de cybersécurité des véhicules, lesquels complètent l'approche globale de TC en matière de sûreté et de sécurité des VCA :

1 Les véhicules connectés utilisent différents types de technologie sans fil pour communiquer avec leur environnement. Bien que la technologie puisse différer d'un véhicule à l'autre, la plupart des nouveaux véhicules vendus aujourd'hui ont une version de la connectivité. Un véhicule automatisé utilise une combinaison de capteurs, de contrôleurs, d'ordinateurs de bord et de logiciels pour aider le véhicule à contrôler au moins certaines fonctions de conduite au lieu d'un conducteur humain. De nombreux véhicules actuels disposent déjà de technologies d'assistance à la conduite qui utilisent des niveaux d'automatisation inférieurs allant du niveau 0 à 2 selon le document *Taxonomie et définitions des termes relatifs aux systèmes de conduite automatisés pour véhicules automobiles routiers (J3016_202104)* publié par l'organisation internationale de normalisation SAE International. Cela inclut des fonctionnalités telles que le freinage d'urgence automatique, l'assistance au maintien dans la voie et le régulateur de vitesse adaptatif.

- Intégrer les considérations relatives à la cybersécurité des véhicules dans les cadres stratégiques et réglementaires.
- Encourager la sensibilisation et favoriser une approche modernisée et novatrice en matière de cybersécurité des véhicules.
- Aborder les enjeux émergents et adjacents dans l'environnement de cybersécurité des véhicules.

## Portée de la Stratégie

La Stratégie de cybersécurité s'applique à l'ensemble du cycle de vie des véhicules, depuis la conception et la production jusqu'à la vente, aux réparations et à l'entretien, en passant par le marché secondaire. Bien qu'elle soit principalement axée sur les véhicules légers équipés de fonctions connectées et automatisées, elle peut aussi s'appliquer à d'autres types de véhicules, comme les parcs gouvernementaux, les camions lourds et les véhicules électriques, pour ne nommer que ceux-ci.

Reconnaissant l'interconnectivité inhérente des systèmes cyberphysiques des véhicules, la Stratégie reflète une vision holistique de la cybersécurité qui s'étend au-delà des limites physiques du véhicule. En effet, elle comprend des considérations globales visant l'infrastructure physique et numérique de soutien qui éclairent et facilitent l'exploitation sécuritaire des véhicules, y compris ceux équipés des technologies des VCA.

## Rôles et responsabilités

Au Canada, tous les ordres du gouvernement, le secteur privé et les Canadiens partagent la responsabilité de la sécurité et de la cybersécurité des véhicules automobiles. Les technologies de véhicules de plus en plus complexes et interconnectées soulignent la nécessité pour les intervenants multidisciplinaires nationaux de poursuivre des efforts de collaboration pour assurer la cybersécurité des véhicules et appuyer l'introduction sécuritaire des VCA, qui représentent la prochaine génération dans le secteur du transport routier.

### Gouvernements fédéral, provinciaux et territoriaux et administrations municipales

Le gouvernement fédéral, les gouvernements provinciaux et territoriaux et les administrations municipales partagent la responsabilité de la sûreté et de la sécurité des véhicules automobiles au Canada. Les gouvernements provinciaux et territoriaux surveillent l'application de bon nombre des lois et des règlements qui régissent l'utilisation des véhicules sur la voie publique. Ils ont notamment comme responsabilités le permis de conduire, l'immatriculation des véhicules, l'assurance automobile et la responsabilité civile, les normes d'entretien des véhicules et l'adoption de lois et règlements sur la circulation routière. Les municipalités sont responsables, à divers degrés, de la gestion du transport des passagers, y compris le transport en commun et les taxis, le stationnement, le contrôle de la circulation, et l'adoption et l'application des règlements municipaux. Les municipalités et les gouvernements provinciaux et territoriaux partagent la responsabilité de l'application des lois et règlements sur la circulation routière et de l'adaptation des infrastructures pour soutenir le déploiement de véhicules connectés et automatisés. Certaines responsabilités, comme celles de l'éducation et de la sensibilisation du public, sont partagées entre les trois ordres du gouvernement. TC travaille en étroite collaboration avec les provinces et les territoires pour assurer une approche coordonnée à l'échelle nationale en matière de sécurité routière.

Le ministre des Transports est chargé de l'administration et de l'application de la *Loi sur la sécurité*

*automobile* (LSA). En vertu de la LSA, TC établit des règlements de sécurité régissant l'importation des véhicules automobiles et des équipements de véhicule automobile prescrits ainsi que l'expédition de véhicules automobiles et d'équipements désignés de construction récente au-delà des frontières provinciales et territoriales. Les constructeurs de véhicules ou d'équipement sont responsables d'attester leur conformité aux normes et règlements applicables, et le Ministère mène des activités de surveillance après la commercialisation, comme des inspections de conformité, des tests et des vérifications, pour vérifier la conformité aux exigences fédérales. En outre, les constructeurs sont tenus d'aviser TC lorsqu'ils soupçonnent qu'un défaut de conception ou de construction d'un véhicule ou d'un équipement pourrait mettre en danger la sécurité des personnes ou causer des dommages aux biens ou à l'environnement, y compris tout défaut lié à la sécurité causé par le système cyberphysique du véhicule.

En s'appuyant sur les points forts du solide régime de sécurité des véhicules automobiles du Canada, le Ministère appuie la mise à l'essai et le déploiement des VCA par l'élaboration de directives et d'outils qui établissent des attentes claires en matière de sécurité que les fabricants doivent respecter. Ces efforts sont éclairés par la recherche et les essais, ainsi que par la collaboration continue et le partage d'information avec des partenaires canadiens et internationaux.

Reconnaissant qu'un certain nombre de ministères fédéraux ont des engagements communs à faire progresser la cybersécurité au Canada, TC collabore avec les partenaires des programmes du gouvernement fédéral pour promouvoir une approche cohérente et uniforme en matière de cybersécurité au Canada. Afin d'appuyer un solide programme de cybersécurité des véhicules, TC collabore sur une base régulière avec les ministères fédéraux suivants pour échanger de l'information, cerner les secteurs propices à la collaboration et tirer parti de l'expertise. .

- **Sécurité publique Canada (SP)** assure un leadership national en matière de politique de cybersécurité par le biais de la *Stratégie nationale de cybersécurité du Canada et du plan d'action* connexe, en travaillant avec un éventail d'intervenants pour faire progresser la cybersécurité au pays et à l'étranger. La Stratégie nationale de cybersécurité s'articule autour de trois piliers fondamentaux, soit la sécurité et la résilience, l'innovation en matière de cybersécurité et le leadership et la collaboration qui, collectivement, guident le gouvernement du Canada dans la protection des citoyens et des entreprises contre les cybermenaces.

- **Le Centre de la sécurité des télécommunications (CST)** est l'entité nationale responsable des opérations de cybersécurité, qui sont coordonnées par l'entremise du Centre canadien pour la cybersécurité (CCCS). Le CCCS fournit des renseignements et des conseils opérationnels en matière de cybersécurité au gouvernement, à l'industrie, aux propriétaires et aux exploitants d'infrastructures essentielles et à la population canadienne.

- L**a Gendarmerie royale du Canada (GRC)** coordonne les opérations de lutte contre la cybercriminalité au Canada et collabore avec des partenaires internationaux de lutte contre la cybercriminalité, des efforts facilités par l'Unité nationale de coordination de la lutte contre la cybercriminalité (NC3) et son Centre antifraude du Canada (CAFC).

- **Le ministère de la Défense nationale (MDN)** développe des technologies innovatrices liées au domaine militaire. Recherche et développement pour la défense Canada (RDDC) et son Centre des sciences pour la sécurité (CSS) fournissent aux organisations militaires les outils et la technologie nécessaires pour réagir aux cybermenaces.

- **Le Centre de recherche sur l'automobile et les transports de surface du Conseil national de recherches du Canada (CNRC)** exploite des installations en Ontario et au Québec où des intervenants de tous les échelons de la chaîne d'approvisionnement de l'automobile et de la fabrication peuvent collaborer avec des spécialistes du CNRC et des chercheurs nationaux sur des enjeux communs en matière de transport.

- **Innovation, Sciences et Développement économique Canada (ISDE)** établit et fait respecter les normes techniques et les exigences en matière de licences applicables aux technologies sans fil intégrées dans les véhicules et l'infrastructure routière. ISDE applique également la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui établit les règles de collecte, d'utilisation et de divulgation des renseignements personnels dans le cadre d'activités commerciales (y compris en ce qui concerne la protection de la sécurité). Le Commissariat à la protection de la vie privée est responsable de son application.

## Intervenants

TC collabore avec un large éventail d'intervenants, y compris des fabricants, l'industrie et le milieu universitaire, pour appuyer la recherche, la mise à l'essai et l'élaboration de directives et d'outils en matière de cybersécurité des véhicules. Comme ces intervenants sont responsables de la conception et de la production des systèmes électroniques qui sous-tendent les composants matériels et logiciels d'un véhicule, ils sont bien placés pour appuyer l'évaluation et l'atténuation des risques en matière de cybersécurité. Notamment, TC se réunit sur une base régulière avec des associations de l'industrie automobile, ainsi que d'autres groupes d'intervenants, pour échanger de l'information et des pratiques exemplaires, et se tenir informé des développements en matière de sécurité et de sûreté des véhicules. Cette mobilisation est essentielle au maintien du dialogue sur les principaux enjeux liés à la cybersécurité des véhicules, ce qui aidera à établir une approche coordonnée qui accorde la priorité à la sécurité, à la sûreté et à la protection des renseignements personnels.

Le dialogue continu avec le milieu universitaire est également un élément important de l'établissement d'une approche coordonnée en matière de cybersécurité au Canada. Les collèges et les universités contribuent à la recherche et à l'innovation technologiques, et les découvertes du milieu universitaire peuvent générer des connaissances uniques sur les processus établis, lesquelles permettent de cerner et de relever les défis de la cybersécurité. Le milieu universitaire joue par ailleurs un rôle essentiel dans le recrutement de talents et le développement des compétences, ce qui est essentiel pour répondre aux exigences de cybersécurité d'un secteur de plus en plus numérique.

En outre, TC travaille activement avec la communauté internationale pour élaborer des directives et des normes mondiales pour la sûreté et la sécurité des technologies des véhicules. Cela inclut notamment la participation à des groupes de travail internationaux au sein du Forum mondial de la sécurité routière (groupe de travail 1) et du Forum mondial de l'harmonisation des règlements concernant les véhicules (groupe de travail 29) des Nations Unies ainsi que d'autres organisations de normalisation telles que SAE International et l'Organisation internationale de normalisation (ISO). Les risques qui accompagnent les nouvelles technologies de transport routier n'ont pas de frontières et nécessiteront une approche internationale coordonnée et collaborative. Compte tenu de la nature intégrée du marché nord-américain et de l'importance de la circulation transfrontalière des personnes et des marchandises, TC collabore régulièrement avec le ministère des Transports des États-Unis, y compris la National Highway Traffic Safety Administration (NHTSA), pour établir une approche transfrontalière cohérente et coordonnée. En fin de compte, un engagement soutenu avec des

partenaires internationaux offre la possibilité d'échanger des renseignements et des pratiques exemplaires, d'harmoniser les exigences réglementaires s'il y a lieu et de contribuer à l'établissement d'un consensus international pour la cybersécurité des véhicules.

# Importance de la cybersécurité des véhicules

Les progrès technologiques émergents transforment le secteur du transport routier et peuvent améliorer la sécurité des routes canadiennes. En contrepartie, un développement technologique rapide, y compris des fonctionnalités connectées et automatisées, peut augmenter la « surface d'attaque » du véhicule. Une atteinte à la cybersécurité dans le secteur du transport routier pourrait entraîner des conséquences sur la sécurité et les opérations, comme la compromission de la sécurité des véhicules et des renseignements personnels, le vol de voiture, entre autres. Compte tenu de la complexité de la question et des développements technologiques en cours dans le domaine du transport routier, il est essentiel que les intervenants suivent le rythme de l'évolution de l'environnement cybernétique des véhicules afin de gérer et d'atténuer efficacement les risques liés à la cybersécurité et les vulnérabilités connexes.

## Cybermenaces et répercussions possibles

Comme c'est le cas dans l'écosystème de la cybersécurité des secteurs des infrastructures essentielles, il existe un large éventail d'auteurs de cybermenaces[2] dans l'écosystème des transports, allant d'un attaquant individuel à un adversaire avisé opérant au sein d'un groupe plus vaste. L'ampleur d'une attaque variera en fonction des capacités techniques, de la motivation et des ressources de la personne ou du groupe, et de son accès direct ou distant à sa cible.

La complexité de l'écosystème des transports est accentuée par la transformation des véhicules en systèmes cyberphysiques qui sont non seulement équipés de systèmes électroniques internes, mais qui sont maintenant aussi connectés à des dispositifs externes et à des interfaces de communication réseau. Bien que cette combinaison puisse améliorer l'automatisation, la sécurité et les fonctions de commodité, elle augmente également les points d'accès qui peuvent être exploités pour des cyberattaques. Des mesures de cybersécurité adéquates peuvent atténuer le risque de manipulation de composants du véhicule à partir de points d'accès, notamment :

- les interfaces réseau physiques permettant à des sources externes de se connecter aux réseaux du véhicule, y compris les supports CD/DVD, les systèmes d'infodivertissement, les ports des systèmes de diagnostic de bord (OBD) et les ports de bus série universel (USB)
- les interfaces sans fil et les fonctions de connectivité qui permettent au véhicule d'envoyer et de recevoir des données au moyen d'un réseau d'interfaces sans fil qui fournissent une connectivité à courte ou à longue portée, comme la communication dédiée à courte distance (CDCD), les communications cellulaires, les dispositifs Bluetooth, le Wi-Fi, les fréquences radio qui prennent

2 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. L'universalisation d'Internet a fait en sorte que ces auteurs de menace peuvent compromettre, peu importe où ils se trouvent dans le monde, la sécurité des systèmes d'information au Canada. Centre canadien pour la cybersécurité. *Cybermenace et auteurs de cybermenaces*. https://www.cyber.gc.ca/sites/default/files/publications/itsg33-ann2-fra.pdf. Consulté le 8 avril 2021.

en charge diverses fonctions comme les systèmes de surveillance de la pression des pneus (SSPN) et les systèmes d'entrée et de démarrage sans clé

- les interfaces avec le système télématique, qui intègrent les télécommunications et l'informatique pour des applications intelligentes dans les véhicules, et stockent des renseignements personnels.

Il est essentiel que tous les intervenants – du gouvernement à l'industrie, en passant par les fabricants et les fournisseurs de services – comprennent le contexte des menaces liées aux véhicules et accordent la priorité à des concepts de cybersécurité robustes et aux pratiques exemplaires (comme la gestion des risques, la protection de l'ensemble de l'écosystème des véhicules, la gestion des vulnérabilités, la surveillance des incidents et l'intervention en cas d'incident, et l'amélioration continue) pour maintenir efficacement la sûreté, la sécurité et la confidentialité globales de l'écosystème du transport routier[3].

## Objectifs et priorités en matière de cybersécurité des véhicules

TC et l'ensemble des intervenants ont déjà établi une base solide pour la cybersécurité des véhicules. Le Ministère continuera de tirer parti de ce travail en axant ses travaux sur les objectifs suivants et les priorités correspondantes au cours des prochaines années, tout en recherchant les possibilités de collaboration continue avec les intervenants. Ensemble, ces efforts aideront à orienter les prochaines étapes à l'appui de la résilience en matière de cybersécurité des véhicules.

3 Pour plus d'informations sur les concepts de cybersécurité et les meilleures pratiques, reportez-vous aux *Lignes directrices sur la cybersécurité des véhicules de Transports Canada*, au *Cadre et outil d'évaluation de la cybersécurité des véhicules* de TC, et d'autres normes internationales telles que le projet de norme internationale 21434 de l'ISO/SAE : *Véhicules routiers – Ingénierie de la cybersécurité*.

# Objectif 1

## Intégrer les considérations relatives à la cybersécurité des véhicules dans les cadres stratégiques et réglementaires

Les VCA et les technologies d'infrastructure connexes se développent rapidement. Ainsi, en mars 2018, la *Loi sur la sécurité automobile* a été modifiée afin de renforcer les pouvoirs d'application et de mise en conformité du ministre des Transports dans le domaine de la sécurité routière et d'offrir une plus grande souplesse pour suivre le rythme des technologies émergentes dans l'industrie automobile. Pour compléter ces principales modifications législatives, TC continuera de publier des politiques et des directives neutres sur le plan technologique en ce qui a trait à la cybersécurité des véhicules, et veillera à ce que les cadres stratégiques et réglementaires demeurent agiles, afin d'appuyer l'évolution continue des besoins de l'industrie et du gouvernement.

- Priorité 1.1 : Orientation, outils et politiques non réglementaires
- Priorité 1.2 : Modernisation des cadres stratégiques et réglementaires
- Priorité 1.3 : Alignement avec les normes et les exigences internationales

## Priorité 1.1 : Orientation, outils et politiques non réglementaires

TC a axé ses efforts sur l'élaboration de directives et d'outils non réglementaires afin d'appuyer les efforts de l'industrie et d'éclairer la voie à suivre en ce qui a trait aux VCA. Notamment, en mai 2020, TC a publié les *Lignes directrices sur la cybersécurité des véhicules au Canada*, qui fournissent un ensemble de principes directeurs neutres sur le plan technologique pour aider l'industrie à renforcer la cyberrésilience des véhicules. Ces lignes directrices proposent des pratiques exemplaires sur la gestion des risques liés à la cybersécurité et la protection de l'ensemble de l'écosystème des véhicules au moyen de mesures de protection, ainsi que sur la façon de détecter et de surveiller les événements liés à la cybersécurité des véhicules, d'y réagir et de s'en rétablir.

En s'appuyant sur la publication de ces lignes directrices, TC continue d'examiner de nouvelles possibilités d'entreprendre des recherches et d'élaborer des politiques et d'autres outils pour appuyer la cybersécurité dans l'ensemble de la chaîne d'approvisionnement des véhicules. À titre d'exemple, TC a mis au point le *Cadre et outil d'évaluation de la cybersécurité des véhicules au Canada* qui permettra aux fabricants et aux fournisseurs d'évaluer et de mieux comprendre leur niveau en matière de cybersécurité. De plus, TC a donné un mandat d'élaboration d'outils, de lignes directrices et d'activités de formation pour aider les autorités routières (p. ex., les propriétaires/exploitants d'infrastructures) à améliorer la cybersécurité des systèmes d'infrastructure de transport routier (p. ex., les systèmes de gestion de la circulation).

## Priorité 1.2 : Modernisation des cadres stratégiques et réglementaires

La *Loi sur la sécurité automobile* est le fondement d'un environnement réglementaire souple et agile pour la sécurité routière qui encourage l'innovation dans le secteur des VCA et favorise une souplesse accrue. En plus d'élaborer des directives et des outils complémentaires pour accompagner le cadre de réglementation, le Ministère continuera d'examiner les cadres de réglementation et stratégiques existants pour s'assurer qu'ils demeurent souples et agiles afin de pouvoir suivre le rythme de l'émergence de nouvelles technologies. Cette souplesse permettra à TC d'être préparé aux nouveaux développements dans le domaine de la cybersécurité des véhicules, à leur évaluation et leur adoption par l'industrie, et à leur intégration dans les politiques, les exigences et les cadres de réglementation du gouvernement.

En 2019, le gouvernement du Canada a publié la *Feuille de route de l'Examen de la réglementation du secteur des transports*, qui établit le plan de TC visant à éliminer les obstacles réglementaires à l'innovation et à l'investissement dans le secteur des transports, y compris les VCA. En s'appuyant sur ces travaux, TC a publié la *Feuille de route de l'examen réglementaire sur les normes internationales*, qui cerne les occasions où le Canada pourrait jouer un rôle de leadership accru dans l'élaboration des normes internationales, y compris celles visant les VCA et d'autres technologies nouvelles pour les véhicules. À l'avenir, TC continuera de participer activement à ce processus d'examen de la réglementation mené à l'échelle du gouvernement, notamment en déterminant les possibilités d'intégrer des aspects relatifs à la cybersécurité des véhicules.

TC continuera également de collaborer avec d'autres ministères fédéraux responsables pour faire progresser les initiatives complémentaires de cybersécurité des véhicules. Par exemple, dans le cadre de l'approche nationale du Canada en matière de cybersécurité, le Ministère continuera de surveiller les initiatives dirigées par SP, comme la Stratégie nationale de cybersécurité du Canada et le plan d'action connexe, afin de déterminer les occasions d'y intégrer la cybersécurité des véhicules. En outre, TC continuera de collaborer avec SP dans le cadre de l'initiative des cybersystèmes essentiels[4], afin de veiller à ce que les cybersystèmes essentiels du secteur du

4 Pour renforcer et protéger la cybersécurité des infrastructures essentielles du Canada, le gouvernement a l'intention de proposer une nouvelle loi et d'apporter les modifications nécessaires à la législation fédérale existante

transport routier demeurent sécuritaires et fiables et soient protégés contre les menaces et les vulnérabilités en matière de cybersécurité.

## Priorité 1.3 : Alignement avec les normes et les exigences internationales

TC participe activement à des efforts internationaux plus vastes pour appuyer l'élaboration de normes de sécurité mondiales pour les nouvelles caractéristiques des véhicules ayant des avantages prouvés sur le plan de la sécurité. Dans le cadre de ces travaux, TC participe à des réunions et surveille les travaux de l'équipe spéciale internationale pour la cybersécurité et les questions de sûreté des transmissions sans fil, qui relève du Groupe de travail des véhicules automatisés/autonomes et connectés du Forum mondial de l'harmonisation des règlements concernant les véhicules de la Commission économique pour l'Europe des Nations Unies (groupe de travail 29).

En janvier 2021, le nouveau règlement sur la cybersécurité élaboré par l'équipe spéciale pour la cybersécurité et les questions de sûreté des transmissions sans fil est entré en vigueur. Le règlement des Nations Unies sur la cybersécurité vise à fournir un cadre aux pays dotés d'un système réglementaire d'homologation des types de véhicules[5] afin de s'assurer que les risques liés à la cybersécurité sont cernés et gérés dès la conception des véhicules, ainsi que surveillés et évalués sur une base régulière. Actuellement, l'équipe spéciale élabore des lignes directrices sur les exigences techniques pour les parties contractantes à l'Accord de 1998, dont le Canada est signataire. Les lignes directrices fourniront des conseils sur la cybersécurité et les processus de mise à jour des logiciels pour le véhicule, y compris sur les aspects de la gouvernance et du cycle de vie.

En même temps, TC surveille les efforts d'autres organismes de normalisation qui travaillent à l'élaboration d'exigences en matière de cybersécurité des véhicules. Par exemple, l'ISO et SAE International ont élaboré le projet de norme internationale 21434 : *Véhicules routiers – Ingénierie de la cybersécurité*. Les normes peuvent servir de référence aux fabricants et aux fournisseurs de véhicules pour veiller à ce que les risques liés à la cybersécurité soient gérés de façon efficace et efficiente. Elles sont étroitement liées à la norme ISO 5112, *Véhicules routiers – Lignes directrices pour l'audit de l'ingénierie de la cybersécurité*[6].

À l'avenir, TC continuera de surveiller les résultats des travaux de l'équipe spéciale pour la cybersécurité et les questions de sûreté des transmissions sans fil, ainsi que l'élaboration de la norme ISO/SAE 21434, et examinera l'orientation proposée dans le contexte des travaux en cours pour renforcer le niveau de cybersécurité des véhicules du Canada. De plus, TC continuera de collaborer avec ses homologues aux États-Unis. Étant donné le régime d'autocertification commun aux deux pays, qui est unique dans la communauté internationale, il est important que le Canada et les États-Unis travaillent ensemble pour présenter une perspective commune et assurer l'harmonisation de leurs approches, dans la mesure du possible.

afin d'introduire un nouveau cadre pour les cybersystèmes essentiels. Pour obtenir plus de renseignements, veuillez consulter la page suivante : Canada. *Investir dans la classe moyenne*. https://www.budget.gc.ca/2019/docs/plan/budget-2019-fr.pdf. Consulté le 12 avril 2021.

5 Il est important de noter que le règlement a été élaboré dans le contexte d'un système d'homologation de type, qui diffère du cadre d'autocertification canadien, qui exige que les fabricants respectent les normes de sécurité rigoureuses énoncées dans le règlement.

6 La norme ISO/DPAS 5112, Véhicules routiers – Lignes directrices pour l'audit de l'ingénierie de la cybersécurité, est une ligne directrice pour l'audit de la cybersécurité des véhicules en cours d'élaboration. Pour obtenir plus de renseignements, consultez la page suivante : https://www.iso.org/standard/80840.html. Consulté le 12 avril 2021.

# Objectif 2

## Encourager la sensibilisation et favoriser une approche modernisée et novatrice en matière de cybersécurité des véhicules

TC travaille en étroite collaboration avec les intervenants nationaux du transport routier pour collaborer à des initiatives, échanger de l'information et des mises à jour, et travailler à l'atteinte d'objectifs communs. Pour effectuer ce travail, le Ministère intensifiera la mobilisation des partenaires du gouvernement et de l'industrie; examinera les possibilités d'appuyer la compréhension et la sensibilisation des consommateurs à l'égard de la cybersécurité des véhicules, et des VCA en général; et continuera de faire progresser les initiatives en matière de recherche et d'essais.

- Priorité 2.1 : Participation active aux forums fédéraux-provinciaux-territoriaux et de l'industrie
- Priorité 2.2 : Recherche, mise à l'essai et validation
- Priorité 2.3 : Sensibilisation et éducation du public sur la cybersécurité des véhicules
- Priorité 2.4 : Planification et préparation

## Priorité 2.1 : Participation active aux forums fédéraux-provinciaux-territoriaux et de l'industrie

Une collaboration sans précédent entre le secteur de la cybersécurité, l'industrie automobile et les gouvernements est nécessaire pour bien gérer les responsabilités et les défis communs associés à la cybersécurité des systèmes automobiles.

TC travaille en étroite collaboration avec d'autres ministères fédéraux par l'entremise d'un certain nombre de groupes de travail interministériels et avec les gouvernements provinciaux et territoriaux par l'entremise du Conseil canadien des administrateurs en transport motorisé (CCATM). Le CCATM coordonne toutes les questions relatives à l'administration, à la réglementation et au contrôle des transports routiers et de la sécurité routière, et compte parmi ses membres des représentants de tous les gouvernements provinciaux et territoriaux et du gouvernement fédéral où TC joue un rôle de leadership clé. De plus, TC participe activement aux travaux du groupe de travail du CCATM sur les VCA et a tiré parti de ce forum pour contribuer à de multiples initiatives stratégiques, y compris sur la cybersécurité des véhicules, et mener des consultations à cet égard.

En outre, TC collabore de façon régulière avec des partenaires de l'industrie, ce qui lui permet d'échanger de l'information, de se tenir informé des nouveaux enjeux et de mener des consultations sur les initiatives en matière de cybersécurité des véhicules. Par exemple, TC participe à des forums de partage de l'information de l'industrie, comme le Centre de partage et d'analyse de l'information sur l'automobile (Auto-ISAC), dont les membres comprennent des fabricants d'équipement d'origine de véhicules légers et lourds, des fournisseurs et des entreprises de véhicules commerciaux. Auto-ISAC favorise une approche mondiale robuste, fondée sur les risques, pour la cybersécurité du transport routier et partage des renseignements sur la cybersécurité, y compris les vulnérabilités et les flux de menaces pour faciliter la prévention des cyberincidents, l'atténuation et l'intervention. TC participe également à un programme régulier de réunions avec des associations de l'industrie automobile et d'autres groupes d'intervenants au Canada pour effectuer des consultations sur les développements en matière de sécurité et de sûreté des véhicules, y compris les questions liées à la cybersécurité des véhicules.

TC continuera d'établir de solides partenariats avec tous les ordres du gouvernement et les intervenants de l'industrie nationale, y compris les fabricants d'équipement, les fournisseurs, les universitaires et les experts en cybersécurité, afin de produire et d'échanger des données sur les vulnérabilités émergentes, des analyses des risques et des stratégies d'atténuation et de rétablissement dans le domaine de la cybersécurité.

## Priorité 2.2 : Recherche, mise à l'essai et validation

Partout au Canada, tous les ordres du gouvernement, le secteur privé et le milieu universitaire tirent parti de la géographie unique, des conditions météorologiques variables et de la diversité des routes du Canada pour entreprendre des recherches sur les nouvelles technologies automobiles, y compris les essais rigoureux et la validation nécessaires pour bien comprendre les capacités et les vulnérabilités de ces technologies avant leur intégration dans le réseau de transport routier. La cybersécurité est un enjeu fondamental qui doit être abordé, étant donné la nature connectée et interdépendante des technologies émergentes des véhicules.

À l'échelle du gouvernement fédéral, TC et d'autres ministères mènent leurs propres activités d'essai pour cerner les risques pour la sécurité et la sûreté, ainsi que les pratiques exemplaires. Par exemple, le Centre d'essais pour véhicules automobiles (CEVA) de TC à Blainville, au Québec, est une installation de calibre mondial pour l'essai de véhicules et d'équipement. Se concentrant sur les tests de sécurité et l'évaluation liés à son mandat, le CEVA examine et évalue les technologies des VCA, y compris les systèmes avancés d'aide à la conduite (ADAS), les applications des véhicules

connectés et les réseaux coopératifs de camions circulant en peloton afin d'appuyer l'élaboration de normes et de règlements futurs.

Le Ministère va aussi suivre les travaux du Centre de recherche sur l'automobile et les transports de surface du Conseil national de recherches du Canada, qui mène des recherches et des essais liés aux technologies de pointe pour les véhicules (p. ex. en examinant les vulnérabilités liées à la cybersécurité des fonctions connectées, la cartographie et la connectivité pour la conduite automatisée). TC continuera d'explorer les occasions de collaborer avec les partenaires du programme pour faire progresser les efforts de recherche et de tests.

En outre, TC a établi des programmes de financement pour encourager l'intégration sécuritaire des VCA, y compris des projets visant à faire progresser la cybersécurité des véhicules. Par exemple, TC a mis en œuvre le Programme amélioré de paiements de transfert de la sécurité routière (PAPTSR), qui investit dans des projets qui font la promotion de la sécurité routière, y compris dans la conception, la mise à l'essai et l'intégration de solutions novatrices pour les VCA et d'autres technologies d'amélioration de la sécurité. Ces activités de programmation permettent au Canada d'être mieux préparé à l'utilisation plus générale des VCA sur ses routes et au développement de l'infrastructure numérique de soutien. De plus, TC a également mis en œuvre le Programme de promotion de la connectivité et de l'automatisation du système de transports (PCAST) afin d'aider les administrations canadiennes à se préparer à l'éventail de questions techniques, réglementaires et stratégiques qui émergeront à la suite de l'introduction des VCA, y compris l'état de préparation et la cyberrésilience de l'infrastructure. Le programme appuie la recherche et les tests, ainsi que l'élaboration de codes, de normes et de documents d'orientation. Le programme appuie également les activités de renforcement des capacités et de partage de connaissances en matière de cybersécurité, y compris l'accroissement de la capacité et du niveau des propriétaires et des exploitants d'infrastructure de transport au Canada. Le programme a distribué des subventions et des contributions à plusieurs projets d'essai et d'évaluation des VCA.

Dans le cadre de ses efforts prospectifs, TC examinera les possibilités de renforcer la recherche et les essais actuels sur la cybersécurité des véhicules, et déterminera de nouvelles approches et de nouveaux domaines pour mettre à l'essai et évaluer la cybersécurité des technologies de transport routier (p. ex. l'intrusion, la prévention et la détection des incidents, la mise au point de logiciels et de matériel, la mise à jour et l'entretien de produits, la chaîne d'approvisionnement, etc.), dans le but d'appuyer l'introduction sécuritaire de technologies nouvelles et émergentes au Canada.

## Priorité 2.3 : Sensibilisation et éducation du public sur la cybersécurité des véhicules

Une recherche sur l'opinion publique menée par TC indique que la sensibilisation des consommateurs à la fonctionnalité des VCA est essentielle à son acceptation et à son adoption en toute sécurité. De nos jours, les consommateurs de véhicule mentionnent que les capacités des systèmes avancés d'aide à la conduite, comme l'aide au maintien de la trajectoire et la régulation de vitesse adaptative, ne sont pas universellement comprises. Afin de sensibiliser la population et de fournir des renseignements factuels sur les VCA, TC a mis en ligne une présence Web consacrée aux VCA, qui comprend des considérations liées à la cybersécurité des véhicules.

TC reconnaît qu'il est essentiel d'éduquer les consommateurs sur les pratiques cybersécuritaires pour assurer la sécurité et la sûreté de tous les usagers de la route, ainsi que l'intégrité des systèmes et des fonctionnalités numériques d'un véhicule. Cette question devient particulièrement importante, car les véhicules automobiles sont équipés de faibles niveaux d'automatisation, et seront éventuellement équipés de fonctions plus automatisées qui dépendent de l'échange d'information numérique pour fonctionner, et qui exigent l'installation de mises à jour logicielles dans le cadre de l'entretien normal des véhicules.

En s'appuyant sur la publication des *Lignes directrices sur la cybersécurité des véhicules au Canada* de TC, qui proposent des pratiques exemplaires à l'industrie, le Ministère s'efforcera d'accroître sa présence Web actuelle traitant des VCA afin d'inclure des renseignements supplémentaires sur la cybersécurité des véhicules à l'intention des consommateurs, de maintenir la sécurité et la protection des renseignements personnels et de prévenir le vol. En prenant d'autres mesures, TC continuera d'examiner des possibilités nouvelles et novatrices de mobiliser la population et de la sensibiliser aux questions de cybersécurité des véhicules, ce qui pourrait comprendre la recherche sur l'opinion publique, la mobilisation ciblée et la démystification de la fonctionnalité des systèmes de véhicules.

De plus, selon une étude de marché, le marché mondial de la cybersécurité des systèmes automobiles était évalué à 1,9 milliard de dollars américains en 2020 et devrait atteindre 4,0 milliards de dollars américains d'ici 2025[7]. Cette croissance représente une occasion exceptionnelle pour l'économie canadienne, parce qu'il y a une demande importante dans l'industrie pour de nouveaux travailleurs hautement qualifiés capables de travailler dans les nombreuses disciplines liées à la cybersécurité des véhicules, y compris des ingénieurs, des analystes de la sécurité, des vérificateurs et plus encore. TC a financé l'élaboration d'un rapport sur le développement du cybertalent pour les administrations routières canadiennes[8], qui donne un aperçu d'une approche globale pour relever les défis liés au développement des talents et des compétences en matière de cybersécurité dans le secteur du transport routier. TC continuera à surveiller les efforts dans l'ensemble des ministères fédéraux pour constituer l'effectif de cybersécurité de l'avenir et combler les lacunes en matière de talents dans le domaine de la cybersécurité.

## Priorité 2.4 : Planification et préparation

Le secteur du transport routier doit être adéquatement préparé à gérer les incidents de cybersécurité qui touchent les usagers de la route et le réseau de transport routier. À l'appui de ces travaux, TC continuera d'élargir sa collaboration avec d'autres ministères fédéraux responsables, ainsi qu'avec les collectivités du transport routier et de la cybersécurité, afin d'assurer une approche coordonnée pour ce qui est des activités de préparation et d'intervention en cas d'incident.

Cette approche comprend la collaboration avec d'autres ministères fédéraux responsables, comme le Centre de la sécurité des télécommunications (CST) et son Centre canadien pour la cybersécurité. Le Centre pour la cybersécurité dirige la réponse du gouvernement aux événements de cybersécurité et travaille de pair avec les secteurs privé et public afin de fournir un soutien pour les enjeux cybernétiques complexes. TC maintiendra sa collaboration avec le Centre de la sécurité des télécommunications afin de tenir compte des points de vue des intervenants du transport routier, et continuer de participer aux travaux d'Auto-ISAC, pour pouvoir observer les pratiques exemplaires en matière de gestion des incidents qu'utilisent les experts de l'industrie dans les situations réelles de vie.

TC continuera également de participer à des exercices de simulation sur la cybersécurité à l'échelle nationale et internationale, en soulevant les considérations relatives à la cybersécurité des véhicules lorsque cela est pertinent, et en tirant parti des pratiques exemplaires et des leçons apprises pour orienter les activités de cybersécurité des véhicules futures.

---

7 Markets and Markets. *Marché de la cybersécurité automobile par forme (dans le véhicule, services en nuage externes), sécurité (point de terminaison, application, réseau sans fil), application (infodivertissement, groupe motopropulseur, ADAS et sécurité), type de véhicule, type de VE et région – Prévisions mondiales jusqu'en 2025*. Octobre 2020 "https://www.marketsandmarkets.com/Market-Reports/cyber-security-automotive-industry-market-170885898.html. Consulté le 12 avril 2021.

8 Ye, Z., Donaldson, K., Davidson, R. *Developing Cyber Talent for Canadian Road Authorities. Conseil des technologies de l'information et des communications (CTIC).* 2017. https://www.ictc-ctic.ca/wp-content/uploads/2019/05/ICTC_Cyber-Talent-Transport_May28-2019.pdf. Consulté le 12 avril 2021.

# Objectif 3

## Aborder les enjeux émergents et adjacents dans l'environnement de la cybersécurité des systèmes automobiles

Les priorités suivantes représentent l'éventail des activités que TC pourrait envisager pour mettre en œuvre une approche modernisée, novatrice et souple en matière de cybersécurité des véhicules. Chaque priorité répond aux besoins en matière de cybersécurité pour divers types de technologies de transport routier, ainsi qu'à l'approche recommandée pour répondre à ces besoins. La nature complexe et interconnectée de la cybersécurité des véhicules exige la collaboration et la coopération d'un large éventail d'intervenants. Voici une liste non exhaustive des priorités qui pourraient être prises en compte dans le cadre de cet objectif.

- Priorité 3.1 : Protection de la vie privée et gestion des renseignements personnels
- Priorité 3.2 : Sécurité de l'infrastructure numérique
- Priorité 3.3 : Sécurité de la chaîne d'approvisionnement
- Priorité 3.4 : Considérations relatives au marché secondaire
- Priorité 3.5 : Véhicules à usage spécial et véhicules électriques

## Priorité 3.1 : Protection de la vie privée et gestion des renseignements personnels

La protection de la vie privée est inextricablement liée à la cybersécurité des véhicules et à la sécurité routière. Étant donné que les véhicules automobiles sont équipés de systèmes interconnectés qui communiquent entre eux à l'intérieur d'un véhicule, entre les véhicules et avec les usagers de la route et les systèmes de l'infrastructure routière, une quantité importante de renseignements personnels sont générés sur le rendement des véhicules et leurs occupants et peuvent être utilisés à des fins de recherche et à des fins commerciales. Par conséquent, des politiques sur la gestion des risques liés à la protection de la vie privée et sur la gestion responsable des renseignements personnels devraient être envisagées de concert avec la cybersécurité tout au long du cycle de vie d'un véhicule.

La collecte et le stockage des renseignements personnels doivent être conformes aux lois applicables, y compris la loi fédérale sur la protection de la vie privée pour le secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). La LPRPDE définit des règles pour la collecte, l'utilisation et la divulgation de renseignements personnels dans le cadre d'activités commerciales. C'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 très semblables 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 applicables.

Le Commissariat à la protection de la vie privée (CPVP) veille au respect de la LPRPDE, tandis que ses homologues provinciaux font respecter les lois semblables des provinces. ISDE est responsable de l'administration de la LPRPDE, y compris de l'élaboration des politiques liées à la Loi. ISDE dirige notamment l'élaboration et la mise en œuvre du projet de *Loi sur la protection de la vie privée des consommateurs*, qui, s'il était approuvé, représenterait l'approche du Canada pour moderniser la LPRPDE, et le régime fédéral actuel de protection de la vie privée pour régir la collecte, l'utilisation et la divulgation des renseignements personnels dans le cadre des activités commerciales au Canada.

TC continuera de collaborer avec ISDE pour fournir le contexte important relatif au secteur du transport routier, s'il y a lieu. Plus précisément, TC continuera d'examiner la relation interconnectée entre la cybersécurité des véhicules, la protection de la vie privée et la sécurité routière, afin d'appuyer ISDE et le CPVP.

## Priorité 3.2 : Sécurité de l'infrastructure numérique

Les véhicules connectés présentent le potentiel d'améliorer la sécurité et l'efficacité du transport routier en permettant la communication entre les véhicules et les infrastructures intelligentes (p. ex. les feux de circulation, les passages à niveau, les panneaux de signalisation, etc.) et d'autres usagers de la route (p. ex. les piétons, les motocyclistes et les cyclistes). La communication sécurisée entre les véhicules et l'infrastructure routière connectée est essentielle pour assurer un réseau de transport routier sécuritaire.

Afin d'aider les provinces, les territoires et les municipalités à comprendre et améliorer le niveau de cybersécurité de leur infrastructure routière et de leurs réseaux de transport intelligents, TC élaborera, dans le cadre du PCAST, une suite d'outils d'évaluation des risques de cybersécurité, des documents d'orientation et offrira un soutien technique qui seront très bien adaptés à leurs besoins fonctionnels

TC contribue également à la promotion de l'élaboration d'un cadre national pour les Systèmes de

gestion des certificats de sécurité (SGCS). Le SGJS contribuera à assurer la sécurité et la fiabilité des communications des véhicules connectés en intégrant des principes de protection de la vie privée dès la conception et en permettant la communication sans révéler de renseignements personnels sur le véhicule ou le conducteur. TC est membre observateur de SCMS Manager LLC et participe au groupe de travail sur l'interopérabilité transfrontalière qui vise à promouvoir une interopérabilité multi-instance et multi-fournisseur à l'échelle de l'Amérique du Nord.

TC dirige également des travaux pour mieux comprendre les exigences en matière d'infrastructure de positionnement, de navigation et de synchronisation (PNS) pour les systèmes de transport de prochaine génération afin d'aider les véhicules à naviguer en toute sécurité sur les routes canadiennes. Les résultats appuieront une stratégie pangouvernementale pour l'investissement dans l'infrastructure de PNS canadien et du système mondial de navigation par satellite (GNSS) par l'intermédiaire du Conseil du positionnement, de la navigation et de la synchronisation (CPNS), un groupe multilatéral dont ISDE est l'hôte pour coordonner les efforts sur les sujets liés au PNS dans une approche pangouvernementale. Ce groupe étudie également la sécurité des systèmes GNSS, en particulier dans le contexte des applications critiques pour la sécurité, comme le transport.

## Priorité 3.3 : Sécurité de la chaîne d'approvisionnement

Le maintien d'un niveau global de cybersécurité tout au long du cycle de vie des véhicules est déterminé par les mesures de sécurité mises en œuvre dans la chaîne d'approvisionnement. La chaîne d'approvisionnement des véhicules est longue et complexe, et encore compliquée par l'émergence de fonctionnalités connectées et automatisées dans les véhicules. Outre les fournisseurs d'équipements automobiles traditionnels, la chaîne d'approvisionnement comprend désormais de nouveaux fournisseurs de technologies qui fournissent des logiciels, des micrologiciels et des composants matériels. 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. Étant donné que les véhicules automobiles peuvent rester en service pendant des décennies, les intervenants doivent s'assurer que les composants électroniques sont cybersécurisés avant qu'ils ne soient intégrés dans un système, et qu'ils restent pris en charge pour répondre aux menaces et aux vulnérabilités en constante évolution. TC continuera de surveiller les problèmes potentiels de sûreté et de sécurité liés à la chaîne d'approvisionnement des véhicules et fournira des conseils et du soutien, le cas échéant.

## Priorité 3.4 : Considérations relatives au marché secondaire

Reconnaissant que le véhicule moyen reste utilisé pendant plus de dix ans, une approche basée sur le cycle de vie de la sécurité doit s'étendre au secteur du marché secondaire. Les véhicules sont de plus en plus connectés à des appareils externes et à une infrastructure numérique, que ce soit pour des fonctionnalités pratiques, des exigences opérationnelles ou des systèmes de gestion de parc de véhicules, et ils nécessiteront un entretien et des réparations réguliers pour fonctionner en toute sécurité. En outre, les mises à jour par transmission sans fil sont susceptibles de devenir de plus en plus standard pour garantir que les logiciels restent à jour.

Les vendeurs, les fournisseurs et les techniciens de service dans les secteurs du marché secondaire (p. ex., les fabricants d'appareils automobiles, les services de diagnostic et de réparation, les fournisseurs de services tiers, etc.) devraient continuer de s'assurer que leurs opérations et leurs produits répondent aux menaces et aux vulnérabilités émergentes dans l'écosystème des véhicules. Bien que les gouvernements provinciaux et territoriaux soient responsables de la réglementation et des stratégies d'application de la loi en ce qui a trait à l'entretien, à l'utilisation de l'équipement des véhicules automobiles et à l'installation de l'équipement du marché secondaire, TC fournira le soutien nécessaire afin de mieux comprendre les risques et de déterminer les possibilités de renforcer la cybersécurité globale des véhicules au Canada.

## Priorité 3.5 : Véhicules à usage spécial et véhicules électriques

The vehicle ecosystem is comprised of many vehicle types, ranging from light duty vehicles to government fleets, first responder vehicles, passenger (e.g. rentals) and commercial (e.g. heavy-duty trucks) fleets as well as electric vehicles and their associated infrastructure. Recognizing that special purpose vehicles may have distinctive safety and security components and may be used to transport different types of cargo, including dangerous goods, different vehicle types will require individual risk assessments that consider the likelihood and impact of a cyber security incident.

For example, many commercial motor vehicle operators are making use of fleet management systems which connect with a vehicle's electronic control module and can record, store and transmit data such as but not limited to vehicle status, position, speed, fuel economy, cargo identification and driver working hours. While these systems can be used to optimise fleet movements, reduce environmental impact, reduce driver fatigue and increase road safety, this connectivity could present cyber security vulnerabilities. TC is monitoring and engaging with stakeholders to assess and address emerging cyber security risks in this space, in order to support the safe and secure use of these systems.

Moving forward, TC will continue to monitor advances in the technology supporting special vehicles, including potential implications for cyber security vulnerabilities, and will work with stakeholders as appropriate to better understand mitigate emerging threats.

# Conclusion

La complexité et l'interdépendance croissantes des véhicules et de l'infrastructure de soutien révèlent l'importance de donner la priorité à la gestion des risques en matière de cybersécurité dans tous les aspects de l'écosystème des véhicules. Pour maintenir la confiance des Canadiens envers la sécurité et la sûreté de leurs véhicules, et la protection de leurs renseignements personnels, il incombe à tous les intervenants – le gouvernement, l'industrie, les fabricants et les fournisseurs – de promouvoir l'échange d'information, la recherche et la mise à l'essai, et l'élaboration de lignes directrices à l'appui de la cyberrésilience des véhicules.

La Stratégie sur la cybersécurité de Transports Canada s'appuie sur le régime flexible de sécurité des véhicules automobiles du Ministère et sur une série de lignes directrices et d'outils complémentaires pour encadrer l'utilisation de technologies de sécurité des véhicules. Elle tient compte des concepts fondamentaux de la cybersécurité dans sa vision, ses objectifs et ses priorités. TC continuera de travailler avec les intervenants pour surveiller les tendances et les progrès en matière de sécurité des véhicules, et utilisera la feuille de route prospective de la Stratégie de cybersécurité pour se donner l'élan et renforcer encore davantage le niveau de cybersécurité des véhicules au Canada.