Les véhicules automatisés face à la menace de nature « cyber »

Association québécoise des transports

Sadio Bâ – 25 octobre 2018 – Montréal

Constat et convictions

- Le numérique est au cœur de l'écosystème automobile.

- Pas de sûreté, pas de confiance dans les nouveaux usages sans cybersécurité.

- Une refonte de l'homologation des véhicules avant la mise en circulation est rendue nécessaire par :
  - l'émergence de la conduite automatisée ;
  - l'intégration du sujet de la cybersécurité dans la délivrance des autorisations.

  La « démonstration de sécurité » ne peut plus reposer uniquement sur une approche basée sur de la conformité.

Sommaire

- La numérisation de l'écosystème automobile
- Les attaques sur des systèmes numériques
- Le cadre réglementaire
- Perspectives et limites du schéma actuel

ACCOMPAGNER
500 interventions
menées en région

SOUTENIR

CONNAÎTRE
& ANTICIPER
59 audits et contrôles
de sécurité

COOPÉRER,
PROMOUVOIR
+120 rencontres internationales

INFLUENCER
& PILOTER

DÉFENDRE
20 opérations majeures de cyber-défense

La numérisation de l’écosystème automobile

Une numérisation inéluctable…

- Trois (r)évolutions majeures dans le secteur de l'automobile :
  - **Motorisation propre** → électrique, hybride, hydrogène…
  - **Automatisation des fonction de conduite** → véhicule autonome
  - **Nouveaux services** → véhicule connecté
- Cette numérisation concerne la fonction première d'une automobile à savoir la **cinématique** mais aussi les **fonctions annexes** (navigation, assistance, infodivertissement…)
- Qui requièrent **toutes** une utilisation **massive** des technologies de l'information et de la communication
- **Augmentation substantielle de la surface d'attaque (cyber)**

…au profit

- une amélioration de la **sécurité routière,** en réduisant le facteur humain (1,25 millions de morts par an et 20 à 50 millions de blessés – chiffres OMS 2018) ;
- une mobilité plus respectueuse de **l'environnement,** en optimisant les circulations et en limitant les émissions polluantes.

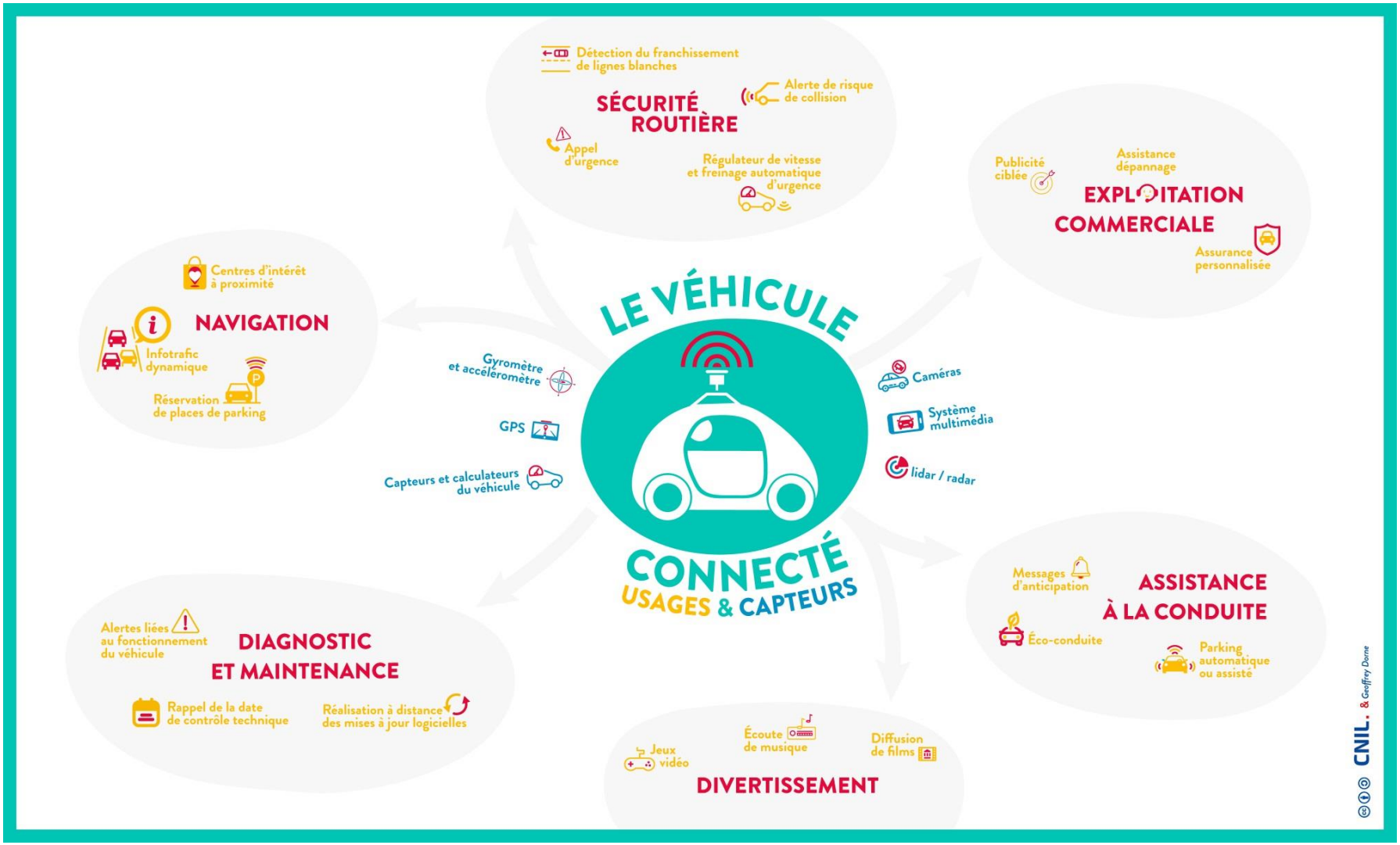
avec un impact

une redistribution de la **chaîne de valeur** parmi les acteurs historiques et des nouveaux entrants, migration de l'industrie vers le service.

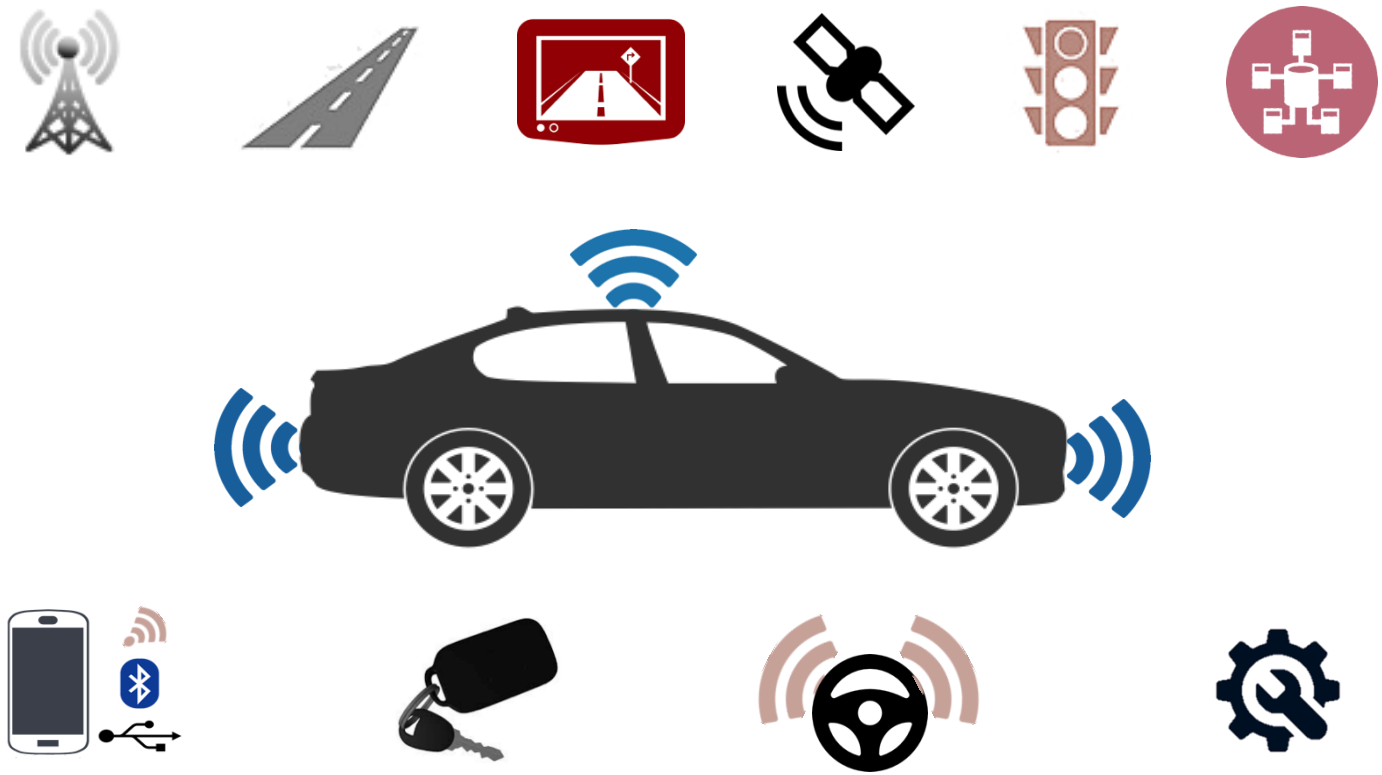
La connexion modifie radicalement le cycle de vie et la nature d'un produit

- **Maintien en condition de sécurité**
  - Si le processus de mise à jour est maitrisé alors les gains seront énormes pour l'industrie automobile
  - Gestion des configurations
- **Évolution de la couverture fonctionnelle** du produit au cours du temps
  - Gestion des configurations
  - Quid de la validité d'une autorisation de mise en service initiale (homologation)
- **Turbine à données et approche systémique**
  - Statut de la donnée
  - Paradigme holistique (embarqué et débarqué)
  - Multiplicité des parties prenantes

Les nouveaux usages



Véhicules intelligents : Surface d'attaque



Le véhicule étendu

Les attaques sur des systèmes numériques

Cybersécurité ?

- État recherché pour un système (d'information) garantissant la **disponibilité**, **l'intégrité** ou la **confidentialité** des données **stockées**, **traitées** ou **transmises**.

- Elle repose sur des mécanismes incluant entre autres des **règles**, des **produits** ou des **méthodes** pour protéger les personnes et les biens des actes **malveillants**.

- Du **droit**, de la **technique** et de **l'organisation**.

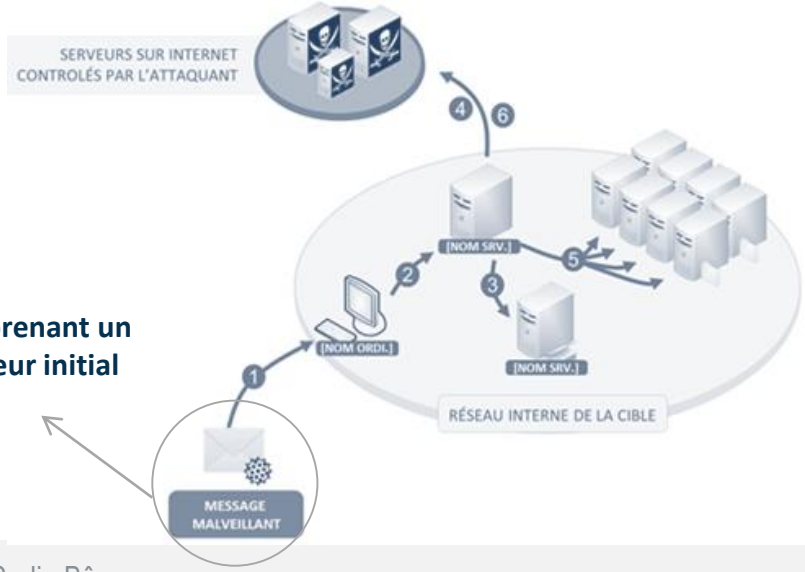
- **Les données personnelles** font l'objet d'une **réglementation spécifique**

Éléments constitutifs d'une menace ?

Un ou plusieurs attaquant(s)

Une ou plusieurs cibles

Un ou plusieurs chemins d'attaque



Comprenant un vecteur initial

Une ou plusieurs finalité(s)

Motivations et profils d'attaquants

LUCRATIVE

Cyber-mercenaires
Officines
Escrocs

IDÉOLOGIQUE

Hacktivistes
Cyber-terroristes
Cyber-patriotes

ÉTATIQUE

Unités spécialisées

LUDIQUE

Adolescents désœuvrés ou non
(script-kiddies)

TECHNIQUE

Hackers chevronnés
Développeurs

PATHOLOGIQUE

Vengeurs
Employés mécontents

Finalités poursuivies

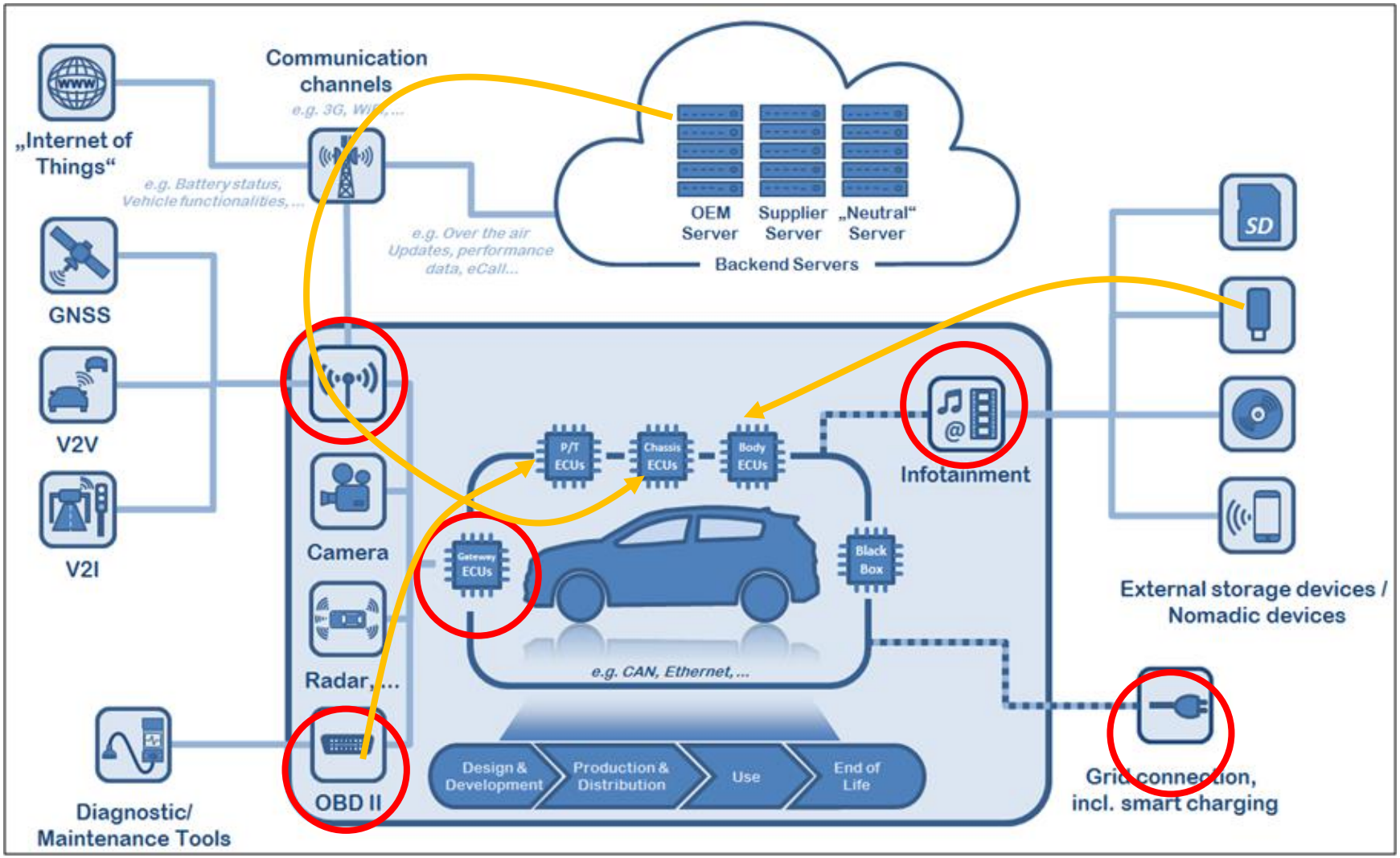
ATTEINTE À L'IMAGE

CYBER CRIMINALITÉ

ESPIONNAGE

SABOTAGE

Cibles et chemins d'attaque



(Nouvelles) Menaces ?
Attaques à distance

- Immobilisation d'une flotte de véhicules ou d'un système de transport à des fins de chantage ;
- Prise de contrôle et utilisation d'un véhicule comme arme par destination ;
- Leurrage d'une intelligence artificielle (signalisation, reconnaissance vocale…) ;
- Système de contrôle du trafic ;
- Système de navigation et de positionnement par satellite ;
- …

La sûreté de fonctionnement et la cybersécurité

- Culturellement deux univers éloignés ;
- Convergence protocolaire ;
- Non prise en compte de la malveillance ;
- Numérisation inéluctable des systèmes et des fonctions.

La sûreté de fonctionnement est directement tributaire de la cybersécurité.

Le cadre législatif et réglementaire

La Loi de Programmation Militaire (LPM)

Entrée en vigueur en 2016, cette réglementation contient des dispositions pour renforcer le niveau de sécurité informatique des Opérateurs d'Importance Vitale (OIV)


Energie


Alimentation


Finance


Public


Télécoms


Santé


Industrie


Défense


Transport


Eau


Espace & Recherche


Justice

Règles de sécurité

Contrôles de sécurité

Notification des incidents

Crise Majeure

Directive SRI (*NIS*)

- **6 juillet 2016** : Adoption de la Directive sur la sécurité des réseaux et des systèmes d'information

→ Transposée dans le droit français le 15 mai 2018

- Désignation des opérateurs de services essentiels (OSE) avant le 9 novembre 2018. **Les acteurs industriels en sont exclus**.

- **4 axes** :

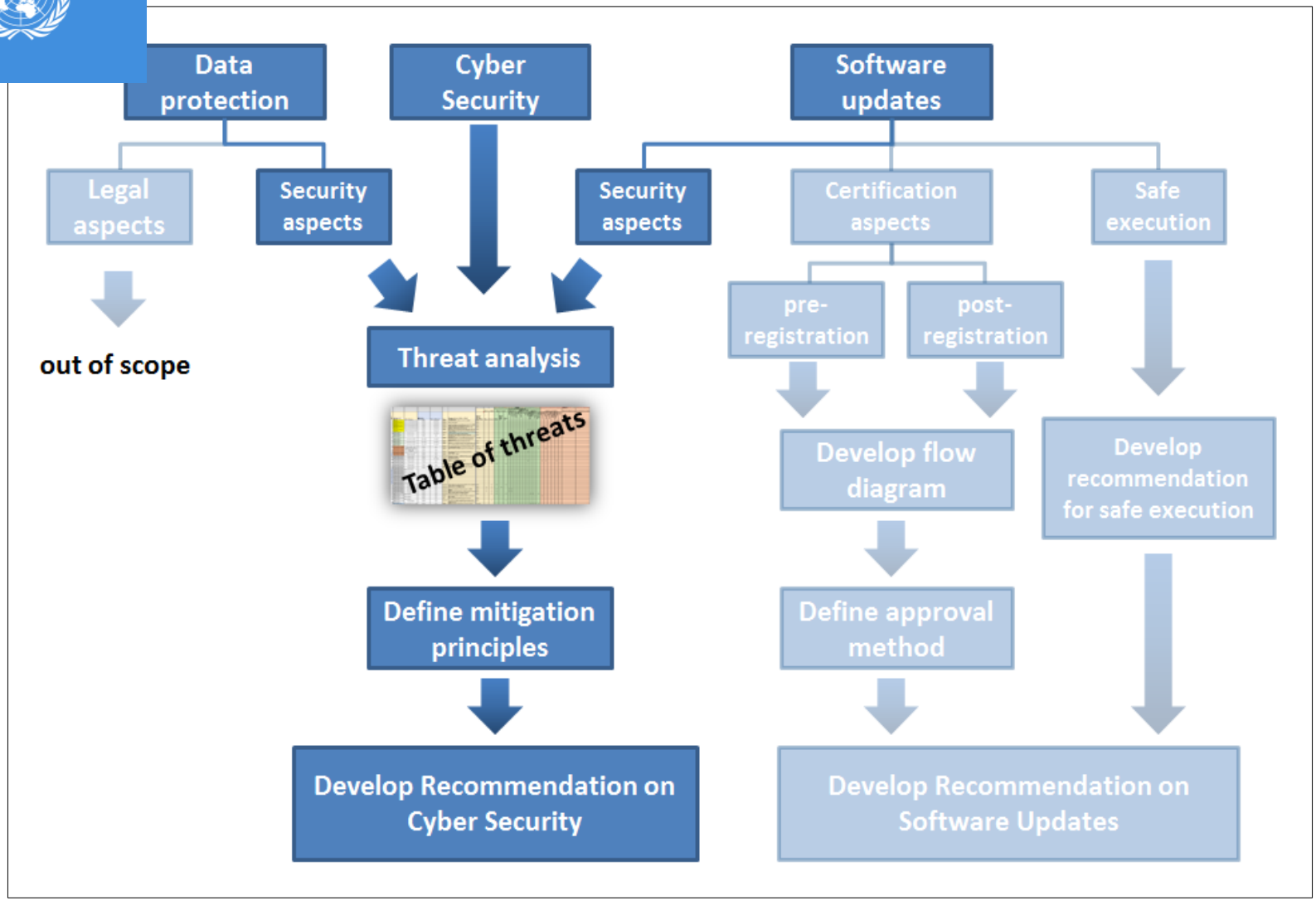
- Renforcement des capacités nationales de cyber sécurité des Etats membres
- Mise en place d'une coopération entre EM
- Instauration d'un cadre réglementaire destiné à renforcer la cyber sécurité des opérateurs de services qui sont essentiels au fonctionnement de l'économie et de la société
- Instauration d'un cadre réglementaire destiné à renforcer la cyber sécurité des fournisseurs de service numérique

Un cadre réglementaire insuffisant et mal adapté

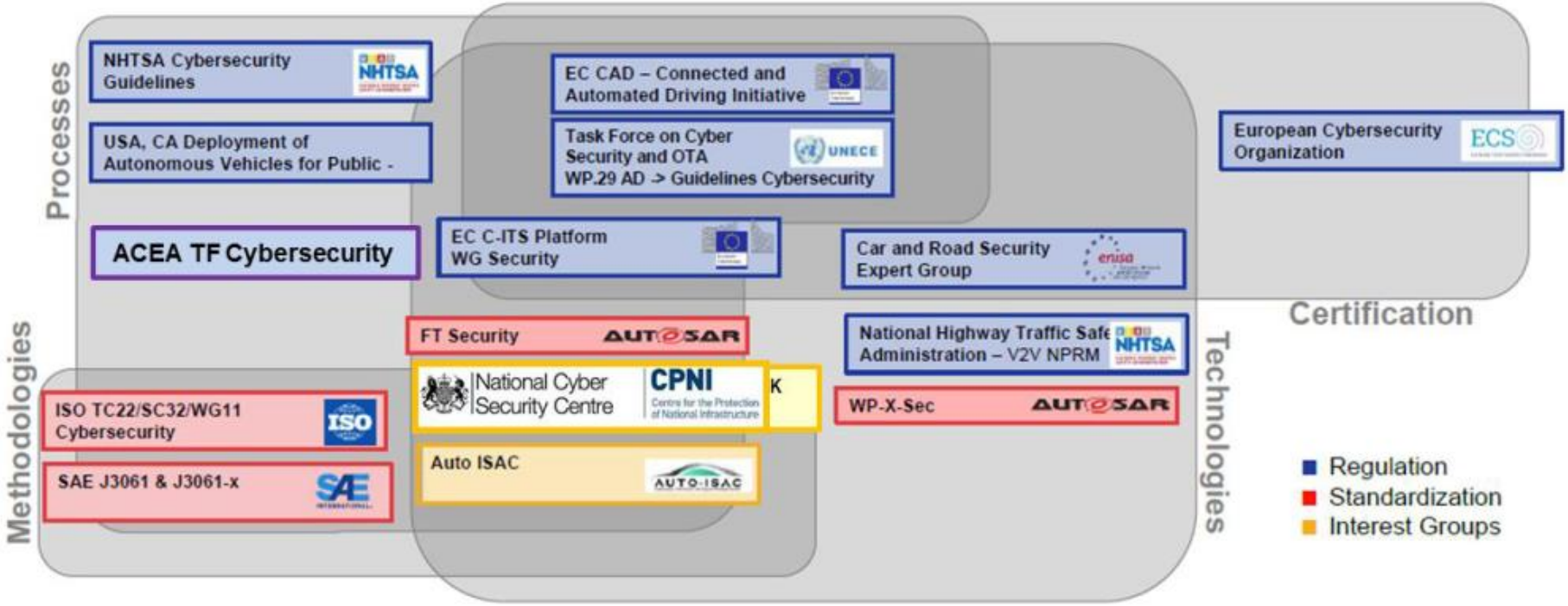
- LPM et SRI (*NIS*) sont axées sur les **infrastructures critiques** et concernent les opérateurs d'importance vitale et les opérateurs de services essentiel, **pas les produits.**

Forum mondial pour l'harmonisation de la réglementation des véhicules (WP.29)

- Définit le cadre technique de réception par type des véhicules (homologation).
- Pour accroitre la cybersécurité des futurs véhicules et donc introduire des exigences SSI dans la réglementation, il faut s'appuyer sur le WP29.
- Attention toutefois, toute la dimension « numérique » d'un véhicule, n'est pas couverte par le WP29 (système d'infodivertissement, certains systèmes d'aide à la conduite, système de navigation…).
- Les exigences de nature « cyber » dans la **réglementation** technique (WP.29) relatives à la réception par type des véhicules à moteur ne concerneraient **que la phase de production du véhicule** (via la délivrance par les autorités nationales d'un certificat de conformité).


Data protection
Cyber Security
Software updates
Legal aspects
Security aspects
Security aspects
Certification aspects
Safe execution
out of scope
Threat analysis
pre-registration
post-registration
Table of threats
Develop flow diagram
Develop recommendation for safe execution
Define mitigation principles
Define approval method
Develop Recommendation on Cyber Security
Develop Recommendation on Software Updates

Un foisonnement d'initiatives



Perspectives et limites du schéma actuel

Cadre français
pour favoriser les expérimentations

- Un cadre réglementaire est en vigueur depuis le 18 avril 2018, autorisant les **expérimentations** sur les voies publiques de véhicules à délégation de conduite.
- Pour la première fois le dossier d'instruction de la demande d'autorisation contient un volet de **cybersécurité** (questionnaire, analyse des risques, audits de sécurité, plan d'amélioration continue, incidents « cyber »…)

Approche française *(présentée le 14 mai 2018)*

Il n'y aura pas de confiance dans les nouveaux usages du véhicule automatisé et autonome sans la prise en compte de la cyber-sécurité. En outre la singularité du risque numérique ne doit pas conduire à le traiter de manière singulière. De ce fait, il est suggéré :

- par le biais du WP.29, de ***modifier la réglementation technique pour introduire des exigences de nature « cyber », intervenant dès la conception des nouveaux véhicules*** ;
- de faire converger les approches normatives relatives à la sûreté de fonctionnement avec celles relatives à la cyber-sécurité ;
- de peser sur la récente proposition de la Commission européenne relative à un **schéma européen de certification** en matière de cyber-sécurité qui permettra d'offrir un cadre d'évaluation du niveau de sécurité des produits et des systèmes ;
- de mettre en place, idéalement au niveau européen, une ***structure d'échange dédiée au secteur automobile sur l'état de la menace et les réponses*** à apporter aux cyber-attaques ;
- de développer la **culture en matière de cyber-sécurité** auprès de l'ensemble des acteurs des filières.

Trois pistes principales non exclusives l'une de l'autre

échéance fin 2019

> Réglementaire *(forum mondial pour l'harmonisation de la réglementation des véhicules) ;*

Le développement des systèmes de conduite hautement automatisés appelle à préparer une ***nouvelle approche de validation par les autorités publiques***. L'homologation « classique » des véhicules fondée sur les performances basiques des organes (ex : direction, freinage, éclairage) n'est en effet plus adaptée au développement du véhicule autonome. L'interaction du véhicule avec son environnement de circulation devient le barycentre de la validation, et non plus le véhicule lui-même.

> Normatif *(ISO/SAE 21434)* qui couvrirait le **cycle de production** et le **cycle de vie** ;

> Évaluation et certification *(schéma de certification européen de cybersécurité).*

Constat et convictions

- Le numérique est au cœur de l'écosystème automobile.

- Pas de sûreté, pas de confiance dans les nouveaux usages sans cybersécurité.

- Une refonte de l'homologation des véhicules avant la mise en circulation est rendue nécessaire par :
  - l'émergence de la conduite automatisée ;
  - l'intégration du sujet de la cybersécurité dans la délivrance des autorisations.

  La « démonstration de sécurité » ne peut plus reposer uniquement sur une approche basée sur de la conformité.

… Est-ce que cela était vraiment mieux avant ?

MERCI

sadio.ba@ssi.gouv.fr