SHIELD
by SOURCEREE

What's Inside

National Security Newsletter

April 2021

SOURCEREE

On Earth Day 2021, at Union Station's electric vehicle (EV) rapid charging station, Secretary of Transportation Buttigieg announced the release of the Federal Highway Administration (FHWA) report on the expansion of electric vehicle corridors throughout the United States. The United States has set a goal of installing 500,000 new EV chargers by 2030, building off of EO 14008, "Tackling the Climate Crisis at Home and Abroad," which also includes a goal of greening the US federal government fleet and achieving zero emissions by 2050. For April's SHIELD Newsletter, the Sourceree team is focusing on electric vehicles (EVs) – their increased demand in the federal government, military, and among private consumers will place stress on the EV supply chain, which includes batteries and charging stations. The first article in the newsletter is the FHWA report, which lends insight into the scale of the US plan for EVs in the near future. Next up is a study from the International Council on Clean Transportation, showing a comparison of China, the United States, and Europe's EV market, with China vastly dominating the battery manufacturing and charger supply space. An article from the ARMOR newsletter for the US Army Maneuver Center of Excellence outlines the tactical advantage of an Army EV combat fleet. And finally, with government, military, and private sector fleet modernization, comes increased vulnerability. Bolstering and safeguarding the EV supply environment, while also ensuring US personally identifiable information (PII) and safety is not at risk of cyberattack will be key factors to ensure the widespread adoption of EVs in the United States is both an economic and a national security success.

--Adam Murphy, Sourceree President

Federal Funding is Available For Electric Vehicle Charging Infrastructure On the National Highway System

US Department of Transportation, Federal Highway Administration
22 April 2021

The Federal Highway Administration (FHWA) report first identifies the economic case for electric vehicles (EVs) followed by the ensuing economic benefits. The report then highlights the enormous expansion plan that will increase the demand for Lithium-ion batteries, as well as other items in the EV supply environment.

Select excerpts from the piece:

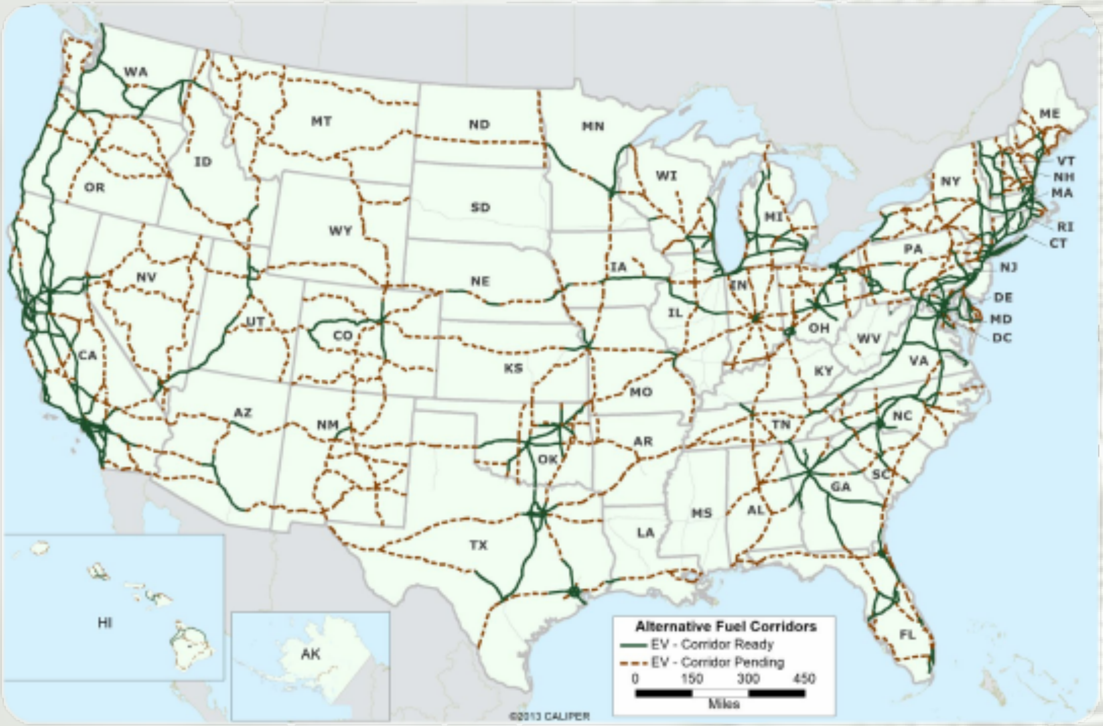
By using electricity rather than gasoline or diesel fuel, EVs have the potential to save consumers money, leaving them with more disposable income to spend in the State and local economy. Also, the electricity rates paid to local electric utilities and generation companies keeps more money in the local economy than money spent on gasoline, which typically flows to oil producers, refiners, and gasoline distributors in other States.

As Technology Advances, Consumer Demand for Electric Vehicles Grow

EVs currently represent a small, but rapidly growing portion of new vehicle sales. A variety of factors point to increased EV adoption in the coming years. The tax credits, point of sale rebates, and other incentives offered by the Federal, State, and local governments for the purchase of EVs – as well as the installation of EV chargers – will further encourage more consumers to adopt EVs. Changing Policies:

- Improving Fuel Economy Standards: At President Biden’s direction, the National Highway Traffic Safety Administration (NHTSA) and the Environmental Protection Agency (EPA) are working to increase fuel economy and GHG standards. As standards get tighter, car companies are making more and more electric vehicles, which they can use to comply with the standards. By 2040, more than half of all new cars could be electric.
- Phasing Out Gasoline-Powered Vehicles: Several countries, regions, and cities around the world – and the State of California – have announced plans to require all zero emission vehicles (ZEVs) in the years ahead. Several large automakers, following consumer demand and public policy are committing to bold new goals for all-electric or mostly electric fleets.

Existing and Pending Electric Vehicle Fuel Corridors



▶ FHWA, Alternative Fuel National Corridors map, https://hepgis.fhwa.dot.gov/fhwagis/

Consumers Need to Know They Can Find a Charging Station

One of the primary obstacles to more widespread adoption of EVs is the limited network of EV charging stations, including along highway corridors throughout the National Highway System. According to national survey data, 78 percent of Americans believe that finding an EV charging station is at least moderately difficult. Of drivers who are not planning to buy or lease an EV when they purchase their next vehicle, 48 percent reported concerns about not enough public charging stations. Unlike the existing national network of gas stations, which are estimated to number more than 150,000 as of April 2021, there were only approximately 38,000 publicly-accessible, non-Tesla EV charging stations nationally with approximately 79,000 charging outlets. For drivers taking lengthier trips along the country's Interstates and highways, fast charging is particularly critical, yet there are fewer than 4,000 non-Tesla DC fact charging stations nationally with approximately 7,700 charging outlets.

Building a National EV Charging Network

The eventual National Highway System network of fast charging stations will build on the work already done by FHWA and State partners to designate Alternative Fuel Corridors. The FHWA designates national Alternative Fuel Corridors for electric vehicle charging as well as hydrogen, propane, and natural gas fueling infrastructure based on nominations from State and local officials. The purpose of the program is to add visibility to sections of the National Highway System that can sustain long-distance travel for alternative fuel vehicles. Once FHWA designates these corridors, States may install Alternative Fuel Corridor signs along the designated highway corridor. The FHWA designates EV corridors with public DC fast charging stations as:

- Corridor ready with EV charging stations located no greater than 50 miles apart and no greater than 5 miles off the highway, and
- Corridor pending with some EV charging stations, but not at the right frequency or locations to fully meet the standard of "corridor ready."

The FHWA has designated EV corridors on approximately 58,980 miles of the National Highway System in 48 States plus the District of Columbia, including segments of 106 Interstates along with 104 US highways and State roads. South Dakota and Mississippi are the only two states without an EV corridor designation. The FHWA is working with other Federal, State, and local officials, as well as private industry, to plan and promote both the existing set of corridors and, ultimately, an even more comprehensive national network.

Race to electrify light-duty vehicles in China, the United States, and Europe: A comparison of key EV market development indicators

The International Council on Clean Transportation (ICCT)
Author: Yidan Chu
4 February 2021

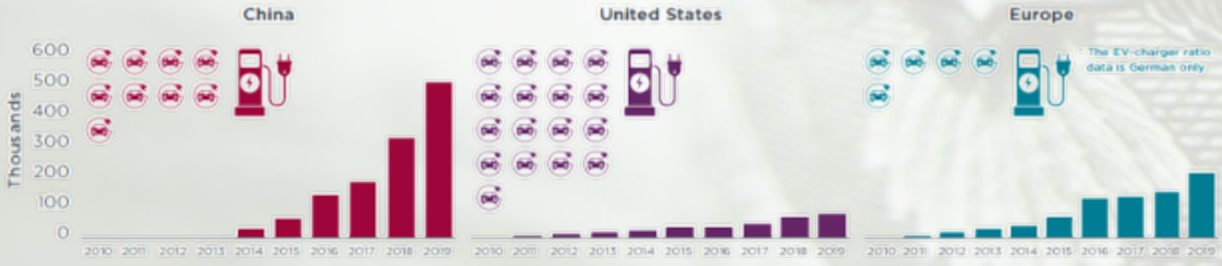
China reached 500,000 electric vehicle (EV) chargers in 2019, the exact amount the United States has set as a goal for 2030. The ICCT report lays out data points for the EV market across China, the United States, and Europe, which are the top three regions for EVs and the EV supply environment. Two critical components of the EV supply environment are highlighted: charging station availability and battery production.

Select excerpts from the piece:

The electric passenger vehicle markets in China, the United States, and Europe have distinct trends. Over the past decade, China has the fastest growth rate and leads in terms of market penetration rate. China is also home to the world's largest stock of electric vehicles, with 4.3 million cumulative electric passenger vehicle sales by August 2020, accounting for 47% of the global total. In contrast, the U.S. market is the slowest growing of the three, with the lowest cumulative sales total and relatively low market penetration. Europe is in the middle in terms of passenger EV stock, market penetration, and industry growth speed. Nonetheless, it is worth noting that in the first eight months of 2020, passenger EV sales in Europe increased significantly and market penetration soared to around 8%.

Charging Infrastructure

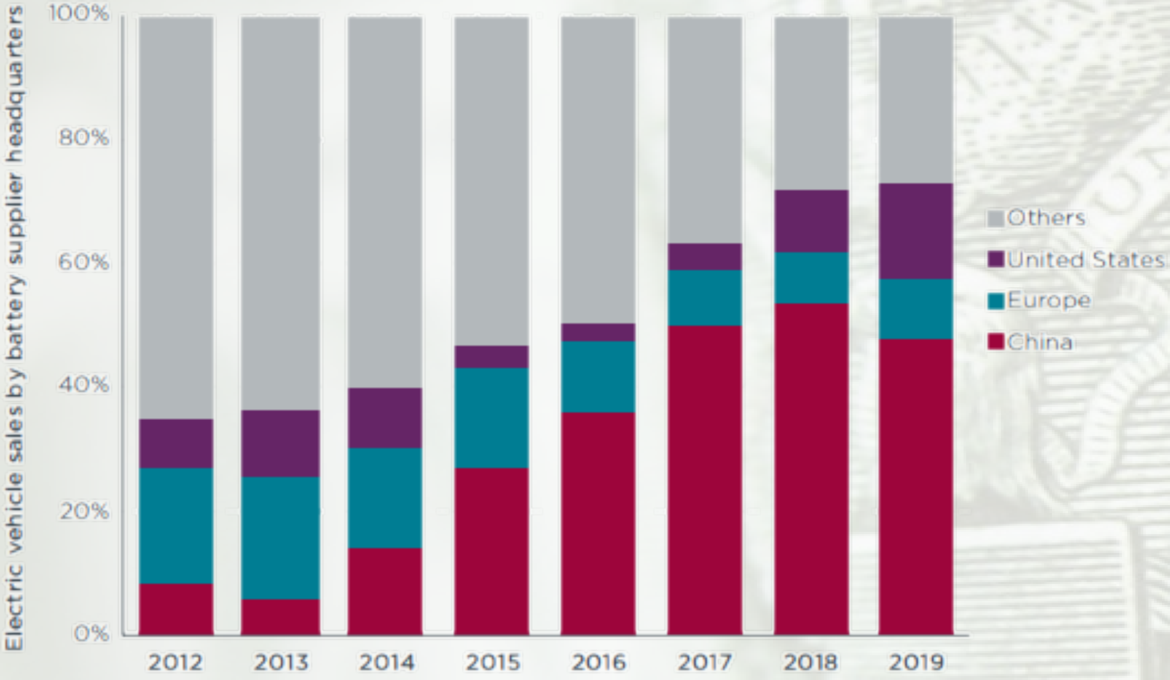
The quantity of public chargers is growing the fastest in China, followed by Europe and then the United States. China has the largest network of public chargers with more than 500,000 chargers by 2019 and accounts for more than 50% of the global total. That is, the number of chargers in China exceeds the number in the United States and Europe combined. However, a large number of chargers does not mean an ideal vehicle-to-charger ratio. While China's passenger electric vehicle-to-public charger ratio (8.5 to 1) is lower than that of the United States (17 to 1), some European countries have even lower EV to public charger ratios (e.g., France: 7 to 1; Germany: 5-1; and the Netherlands: 4-1).



Number of public chargers and vehicle-to-public-charger ratio in 2018[3]

Battery Production

China gradually became the biggest battery producer globally, while the United States' battery production share fluctuated and Europe's share decreased. Based on the vehicle battery supplier's headquarters' location, the share of light-duty EVs fitted with Chinese-made batteries has grown from less than 10% in 2012 to about 50% in 2019. On the other hand, batteries produced from the other two markets currently account for a relatively small share of global sales.



Light-duty electric vehicle sales by battery supplier headquarters[4]

Electric Propulsion: A Game Changer

US Army Maneuver Center of Excellence, ARMOR
Authors: MAJ Ryan Ressler, MAJ Brian Ottestad and Mike Smith
Winter 2021 Edition

This piece in the Winter 2021 Edition of the US Army Maneuver Center of Excellence newsletter outlines the tactical case for electric vehicles (EVs) in the Army fleet, and provides a notional pathway to acquiring EVs for combat use. Key to its success would be a partnership with industry along all parts of the supply chain and to drive innovation.

Select excerpts from the piece:

As the world changes, so must the Army change how it fights. Electric-powered vehicles offer the potential to double the ground forces' operational reach; increase lethality and survivability at the tactical and operational levels; and reduce the Army's logistics burden by half. The rapid and widespread adaptation of vehicle electrification, from hybrids to fully electric vehicles, has begun to alter the full spectrum of the automobile industry and will dramatically revolutionize the way we maintain and sustain vehicles.

Electric Vehicles' Tactical Advantages

Introducing electric propulsion to the tactical and combat vehicle fleet enables the Army to integrate capabilities that were once thought of as only science fiction. Many of these advantages ascend from electric-drive motors and embedded electric-energy storage and internal-distribution systems. Electrification enhances the tactical aspect of maneuver platforms in three distinct ways:

- First, it enables silent mobility. Silent mobility, a long-desired attribute, will increase lethality and survivability in all formations. Imagine a motorized-cavalry troop fitted with a light reconnaissance vehicle that can conduct its mission set virtually undetected. This – combined with extended range and duration – has a dramatic impact on the overall effectiveness of the future cavalry squadron.
- Second, electrification will extend the duration of silent watch, or the ability to sit in a hide position with all critical systems powered and the engine off. Through increased battery density, power-sharing and the ability to produce and prioritize onboard power, electrified vehicles will far outperform the current fleet in terms of power management.
- Third, electric-powered vehicles will dramatically reduce the thermal signature produced by vehicles, degrading adversarial detection capabilities. Reductions in both visible and acoustic detection will dramatically increase the element of surprise.

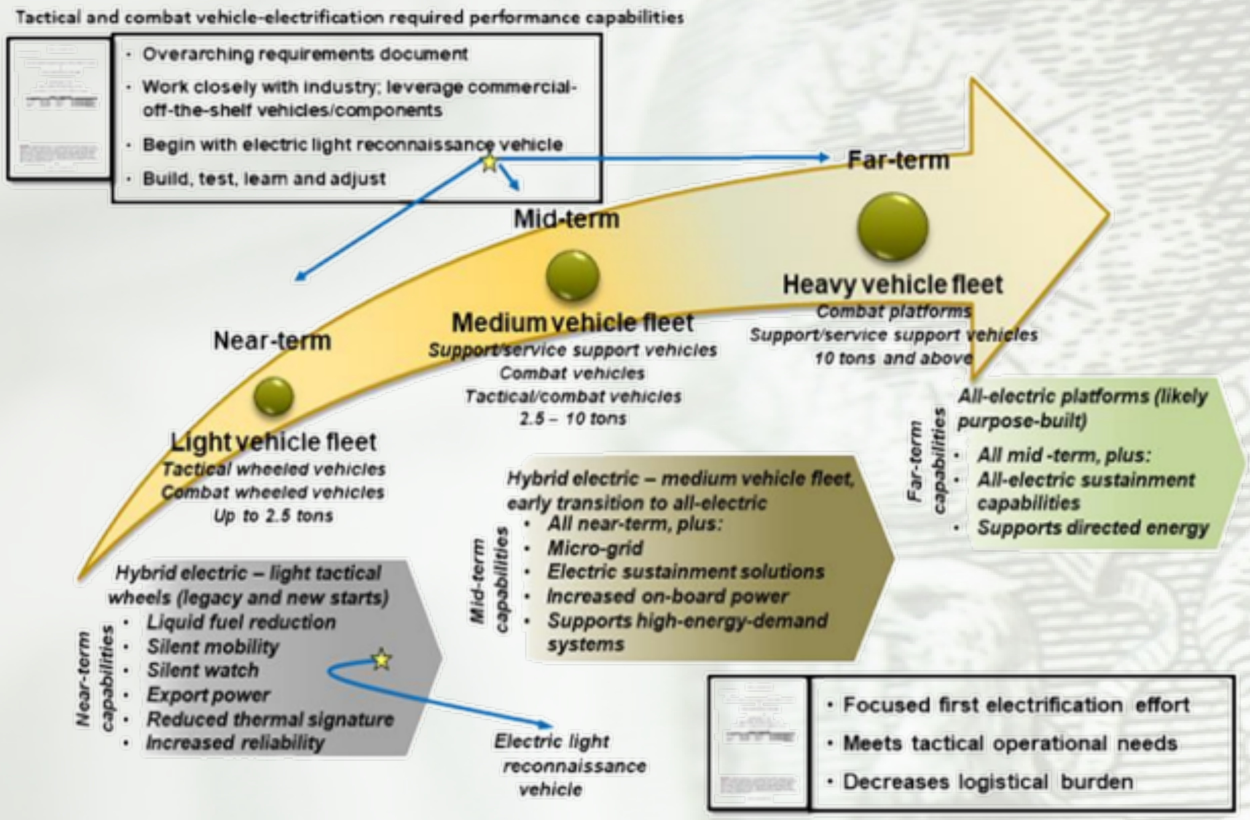

Tactical and combat vehicle-electrification required performance capabilities
Overarching requirements document
Work closely with industry; leverage commercial-off-the-shelf vehicles/components
Begin with electric light reconnaissance vehicle
Build, test, learn and adjust
Far-term
Mid-term
Near-term
Heavy vehicle fleet
Combat platforms
Support/service support vehicles
10 tons and above
Medium vehicle fleet
Support/service support vehicles
Combat vehicles
Tactical/combat vehicles
2.5 – 10 tons
Light vehicle fleet
Tactical wheeled vehicles
Combat wheeled vehicles
Up to 2.5 tons
Far-term capabilities
All-electric platforms (likely purpose-built)
All mid -term, plus:
All-electric sustainment capabilities
Supports directed energy
Mid-term capabilities
Hybrid electric – medium vehicle fleet, early transition to all-electric
All near-term, plus:
Micro-grid
Electric sustainment solutions
Increased on-board power
Supports high-energy-demand systems
Near-term capabilities
Hybrid electric – light tactical wheels (legacy and new starts)
Liquid fuel reduction
Silent mobility
Silent watch
Export power
Reduced thermal signature
Increased reliability
Electric light reconnaissance vehicle
Focused first electrification effort
Meets tactical operational needs
Decreases logistical burden

Figure 5. Possible path to tactical- and combat-vehicle electrification.

Conclusion

The future is now. Traditional fuel is a high-demand commodity that is difficult to move and distribute on the battlefield. Limitations of fuel-capacity drive operational reach and will impact our influence in future contested environments. Adopting electric-propulsion alternatives while increasing power generation, storage and distribution capabilities will reduce our dependence on traditional fuels; increase the lethality and survivability of units; and enhance the overall effectiveness of the force.

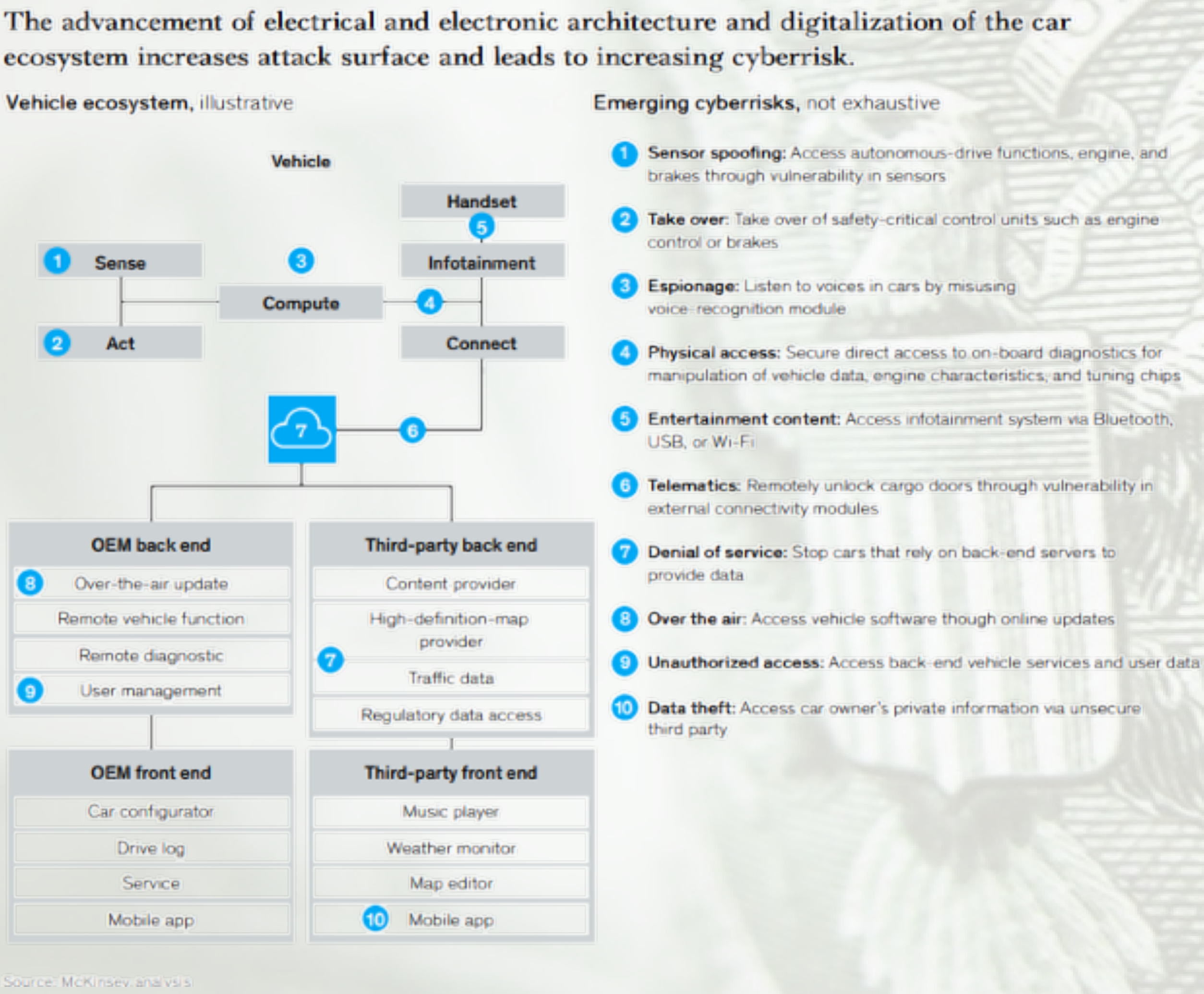
The Army must be an electric-propulsion innovator and continue to strengthen ties with industry regarding propulsion, power and battery technologies. Through the right investments, programs, initiatives and resources, the Army can push these technologies and drive innovation that facilitates continued dominance in the ground domain.

The Race for Cybersecurity: Protecting the Connected Car in a New Era of Regulation

McKinsey & Company
Authors: Johannes Deichmann, Benjamin Klein, Gundbert Scherf, and Rupert Stützle
October 2019

A widespread vulnerability to risk accompanies the improvements made by an entirely modern fleet for the federal government and military and increased standards and incentives for private consumers to adopt electric vehicles (EVs). McKinsey & Company identifies multiple avenues of where a connected car is open to cyberattack.

Select excerpts from the piece:



The advancement of electrical and electronic architecture and digitalization of the car ecosystem increases attack surface and leads to increasing cyberrisk.

Vehicle ecosystem, illustrative

Emerging cyberrisks, not exhaustive

1. **Sensor spoofing:** Access autonomous-drive functions, engine, and brakes through vulnerability in sensors
2. **Take over:** Take over of safety-critical control units such as engine control or brakes
3. **Espionage:** Listen to voices in cars by misusing voice-recognition module
4. **Physical access:** Secure direct access to on-board diagnostics for manipulation of vehicle data, engine characteristics, and tuning chips
5. **Entertainment content:** Access infotainment system via Bluetooth, USB, or Wi-Fi
6. **Telematics:** Remotely unlock cargo doors through vulnerability in external connectivity modules
7. **Denial of service:** Stop cars that rely on back-end servers to provide data
8. **Over the air:** Access vehicle software though online updates
9. **Unauthorized access:** Access back-end vehicle services and user data
10. **Data theft:** Access car owner's private information via unsecure third party

Source: McKinsey analysis

Cybersecurity becomes a core product and value-chain issue

Cybersecurity has risen in importance as the automotive industry undergoes a transformation driven by new personal-mobility concepts, autonomous driving, vehicle electrification, and car connectivity. In fact, it has become a core consideration, given the digitization of in-car systems, the propagation of software, and the creation of new, fully digital mobility services. These services include arrays of car apps, online offerings, vehicle features that customers can buy and unlock online, and charging stations for e-vehicles that "talk" to on-board electronics. Today's cars have up to 150 electronic control units; by 2030, many observers expect them to have roughly 300 million lines of software code. By way of comparison, today's cars have about 100 million lines of code. To put that into perspective, a passenger aircraft has an estimated 15 million lines of code, a modern fighter jet about 25 million, and a mass-market PC operating system close to 40 million. This overabundance of complex software code results from both the legacy of designing electronics systems in specific ways for the past 35 years and the growing requirements and increasing complexity of systems in connected and autonomous cars. It generates ample opportunity for cyberattacks—not only in the car but also along the entire value chain.

The cybersecurity playing field tilts in favor of attackers

To be sure, the economics of car cybersecurity are inherently unfair: with the right state-of-the1art tools, attacks are relatively affordable, low1effort affairs. Mounting a coherent defense for the complex value chain and its products, on the other hand, requires increasingly higher effort and investment. So far, this reality tilts the playing field in favor of the attackers. Examples abound across the industry. For example, white-hat hackers took control of the infotainment system in an electric1vehicle model. They exploited a vulnerability in the in-car web browser during a hacking contest, causing the electric-vehicle maker to release a software update to mitigate the problem. In another white-hat hack, a Chinese security company found 14 vulnerabilities in the vehicles of a European premium-car maker in 2018. Another global automaker recalled approximately 1.4 million cars in 2015 in one of the first cases involving automotive cybersecurity risks. The impact of the recall was significant, with a potential cost for the OEM of almost $600 million, based on our calculations.

The automotive industry lacks a standard approach for dealing with cybersecurity

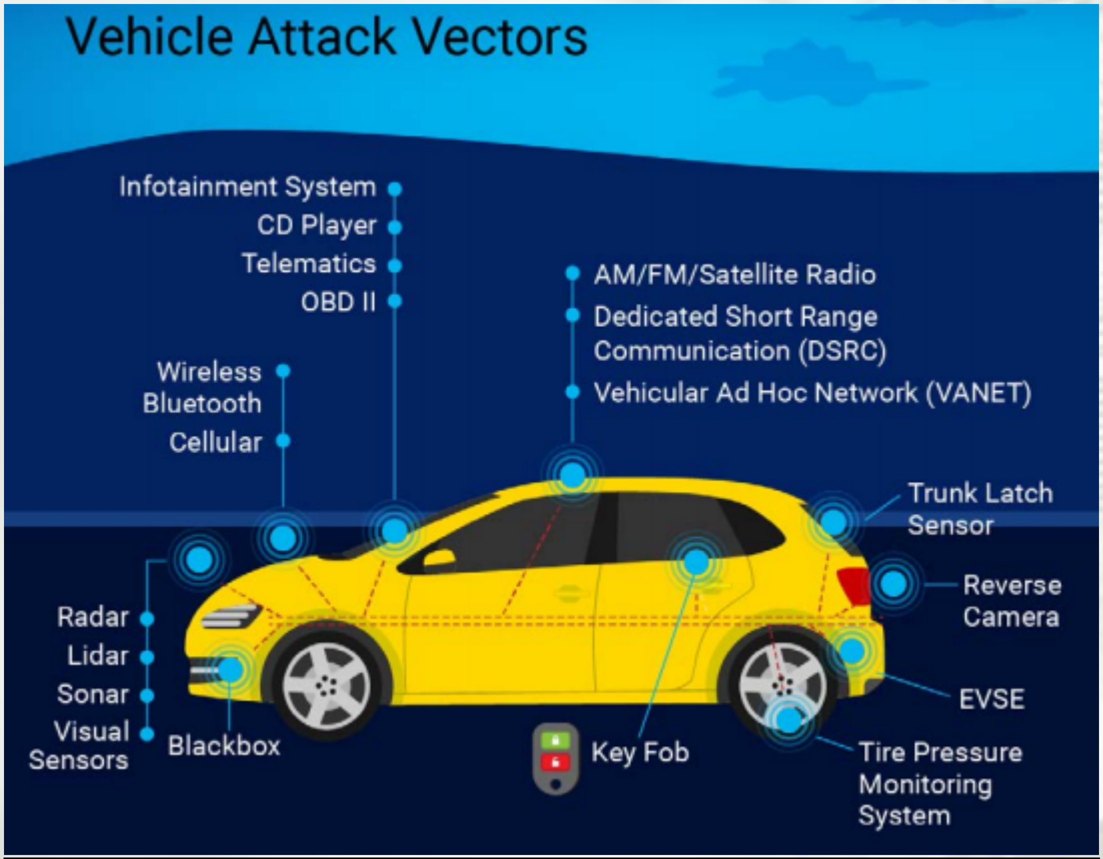
For an industry used to breaking down complex challenges and standardizing responses, cybersecurity remains an unstandardized anomaly. Thus far, automotive suppliers have a hard time dealing with the varying requirements of their OEM customers. Consequently, they try to balance the use of common security requirements that go into their core products against those via the software adjustments made for individual OEMs. However, current supplier relationships and contractual arrangements often do not allow OEMs to test the end-to-end cybersecurity of a vehicle platform or technology stack made up of parts sourced from various suppliers. That can make it difficult for both suppliers and OEMs to work together to achieve effective cybersecurity during automotive software development and testing

Vehicle Cybersecurity Threats and Mitigation Approaches

National Renewable Energy Laboratory
Authors: Cabell Hodge; Konrad Hauck; Shivam Gupta; and Jesse Bennett
August 2019

A widespread vulnerability to risk accompanies the improvements made by an entirely modern fleet for the federal government and military and increased standards and incentives for private consumers to adopt electric vehicles (EVs). This piece by the National Renewable Energy Laboratory lays out the risk of compromise to the telematics systems standard on modern vehicles as well as to elements in the EV supply environment.

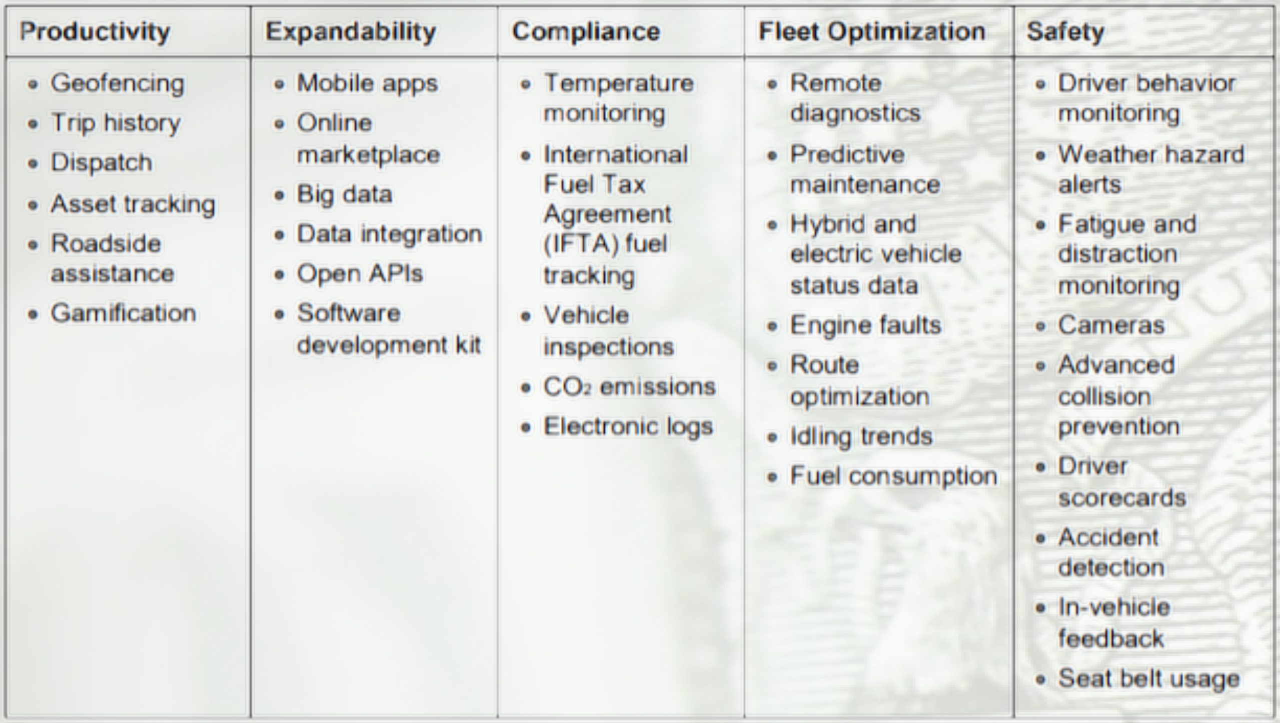
Select excerpts from the piece:



In 2015, vehicle cybersecurity pioneers Charlie Miller and Chris Valasek shut down a Jeep's acceleration on the highway and disabled its brakes in a parking lot (Valasek and Miller 2015). 1 Their initial experiments relied on hardwiring computers directly to the car, but they developed the capability to send messages remotely, revealing a troubling access point. A few years later, Tencent Keen Security Lab researchers discovered vulnerabilities in BMWs that allowed them to access the infotainment systems, the telematics control unit, the unified diagnostics services, and the CAN bus via Bluetooth or a cellular connection (Tencent Keen Security Lab 2018). Bluetooth pairing allows drivers—and potentially hackers—to connect cellular phones to vehicles, take control of infotainment systems, or crash the systems (Mäkilä, Taimisto, and Vuontisjärvi 2011).

Telematics

Table 1. Five Categories of Vehicle Telematics Services



Productivity	Expandability	Compliance	Fleet Optimization	Safety
• Geofencing • Trip history • Dispatch • Asset tracking • Roadside assistance • Gamification	• Mobile apps • Online marketplace • Big data • Data integration • Open APIs • Software development kit	• Temperature monitoring • International Fuel Tax Agreement (IFTA) fuel tracking • Vehicle inspections • CO_2 emissions • Electronic logs	• Remote diagnostics • Predictive maintenance • Hybrid and electric vehicle status data • Engine faults • Route optimization • Idling trends • Fuel consumption	• Driver behavior monitoring • Weather hazard alerts • Fatigue and distraction monitoring • Cameras • Advanced collision prevention • Driver scorecards • Accident detection • In-vehicle feedback • Seat belt usage

The most vulnerable hacking opportunity for telematics is access to the data collected by the system. Collecting data from telematics is possible without write access or bridging different networks. It still requires hacking the telematics network and is inherently a remote risk.

However, the most threatening method for controlling a vehicle through telematics would be to reflash the firmware remotely, which could give a malicious actor insight, control, and ability to manipulate functions of the vehicle as they desire. Research has shown the ability to reflash aftermarket telematics firmware (Foster et al. 2015) and incorporate malicious code into OEM telematics (Li et al. 2019) when critical security measures were not instituted. These failures included using the same cryptographic key for every telematics device, a lack of strong authentication procedures, lack of encryption, and an unsecured update server. With multi-factor authentication, it is difficult for adversaries to access firmware administrative control to reflash firmware updates, even if using another device that is compatible with the device in the car.

Research by the DOT Volpe National Transportation Systems Center identified a risk associated with the ability to send OTA short message service (SMS) messages to query and configure information about the vehicle's status if the attacker knows the personally identifiable information (PII) related to the vehicle. This attack would take moderately lengthy open source intelligence gathering on the part of the attacker and would have to specifically target a particular individual. This presented a greater risk using 2G and 3G networks; 4G-LTE allows messages sent between the car and server to be encrypted and authenticated, making interception, replay, or other intrusions difficult to execute.

Electric Vehicles and Electric Vehicle Supply Equipment

Plug-in electric vehicles (EVs) fuel in a different manner than conventional vehicles and communicate in the process with the electric vehicle supply equipment (EVSE) that charge them. Different types of EVSE have varying levels of communication capabilities. While some communication is essential to establish a connection and greater capabilities provide additional benefits such as power demand management and billing options, they also expose EVs to cybersecurity threats.

All EVs require EVSE to recharge the traction battery. EVSE units provide a source of power to refuel EVs, and must also incorporate communication to ensure energy is supplied appropriately. Table 2 displays the most common EVSE types used in federal fleets and the communication networks they use.

In addition to physical access, EVSE units sometimes coordinate and share information with a vendor through a remote management service. Access to this management service typically requires valid credentials; however, in certain scenarios, an attacker could gain access to these credentials and expose the charging system to multiple vulnerabilities from a remote location.

Although wireless communication between an EVSE and management service provides useful benefits, such as wireless firmware updates as well as customer verification and payment processing, these features also expose the system to remote hacks. This exposure leaves valuable data, such as customer information or firmware, stored on file transfer protocol (FTP) or database servers, exposed to theft or modification. Personal data stored on a database or used by a web server may be acquired through the use of either standardized query language (SQL) injections or cross-site scripting (XSS). Additionally, malicious firmware may be uploaded to unsecure FTP sites and potentially compromise the operation of the EVSE.

Protected by

SHIELD

by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

SHIELD VISION

Software platform for on-demand supply chain risk assessments and financial intelligence

SHIELD SQUAD

Analytical Support

SHIELD INTEL

Business intelligence reports on critical suppliers