



House Select Committee on China

Trojan Horse: China's Auto Threat to America – Applied Intuition QFR Responses

Representative Gus Bilirakis – FL-12

- 1. China is investing heavily in innovative technologies like autonomous vehicles, and if the United States does not implement smart policies to help foster and advance next-generation automotive technology, we are going to cede that market to China. Do you think it's important for Congress to legislate a federal regulatory framework that supports the testing and deployment of AVs at scale in the U.S.? What are the stakes if we fail to do so?**

A consistent national framework would mitigate the current patchwork of state rules that deters investment and slows the safe scaling of autonomous vehicle (AV) deployments. There are key economic and strategic interests at stake in relation to AV technologies: AV leadership drives high-value manufacturing, provides high-paying jobs, and furthers the development of the software-defined architecture that underpins dual-use autonomy for both the commercial and defense sectors. If we fail to provide a clear pathway for the scaled deployment of AV technology, we risk losing to the PRC, not only American leadership in AV technologies, but also: (1) U.S. influence over the technological standards that will guide the further development of AVs; (2) our ability to attract, build, and maintain talent in the AV workforce; and (3) production capabilities for key AV-related technologies.

Representative Haley Stevens – MI-11

- 1. Do you agree that Chinese counterfeit products are a public safety threat?**

Yes. Counterfeit automotive components can fail unpredictably, undermine product integrity, and create cybersecurity risks. This is especially concerning as vehicles become more connected, autonomous, and software-defined platforms.

- 2. Should Congress avoid passing measures that would inhibit OEMs from curtailing these dangerous products?**

Congress should enact policies that allow vehicle manufacturers and Original Equipment Manufacturers (OEMs) to detect and report counterfeit or compromised components. Policymakers can consider strengthening the abilities of OEMs to take action against counterfeit parts by supporting information-sharing and aligning

enforcement across federal agencies (CBP, DOT/NHTSA, and Commerce) to detect and report high-risk connected vehicle components.

Representative Jill N. Tokuda – HI-02

1. What should Congress put into a “CHIPS 2.0” to successfully decouple ourselves from PRC dominance in the market?

Any “CHIPS 2.0” legislation should be designed around the reality that cars are rapidly becoming software-defined platforms, and that autonomy depends on a tightly integrated stack of compute, sensors, networking, and safety-critical software. That means Congress should not only expand U.S. and allied semiconductor capacity but also target the supporting technologies that enable software-defined vehicles at scale, including automotive-grade compute, networking, and the secure hardware needed for over-the-air updates and in-vehicle cybersecurity. Beyond semiconductors, “CHIPS 2.0” could reinforce trusted supply chains for autonomy-critical components like LiDAR, radar, and cameras, as well as the specialized materials and manufacturing inputs that could become production bottlenecks. Finally, Congress should pair these investments with standards and incentives that strengthen the software side of the automotive technology stack. For instance, Congress should aim to secure update integrity and large-scale validation and testing infrastructure, so American and allied companies can deploy software-defined and autonomous capabilities faster, more safely, and without new dependencies on PRC technology.

2. What is your assessment of how the PRC could leverage their growth in autonomy and self-driving automobiles for defense purposes? And how might this threaten U.S. leadership in artificial intelligence?

Autonomy is inherently a dual-use technology. Large-scale commercial deployment produces three clear military-relevant advantages: (1) massive real-world data for perception and decision-making software; (2) rapid iteration of sensors, compute, and software validation tools at commercial speed and scale; and (3) the ability to translate supply-chain dominance of components like LiDAR into a broader autonomy advantage. Under the PRC’s civil-military fusion strategy, these commercial gains could accelerate PLA capabilities in unmanned vehicle operations in both uncontested and contested environments. If the PRC were to gain a decisive advantage over data, software, and critical autonomy components, they could accelerate AI capability in the physical world and gain a strategic advantage over the United States.

3. What would you recommend to policymakers to ensure we build an innovative and effective U.S. and allied industrial base for AI-powered autonomous systems for the military that is also good value for taxpayers, especially given the challenges of cost overruns from legacy defense contractors?

To build an innovative and effective U.S. and allied industrial base for AI-powered defense autonomy that is also good value for taxpayers, Congress should prioritize buying and adapting proven commercial autonomy software, simulation, and validation tooling, and harden it for military conditions, rather than repeatedly funding bespoke, one-off systems. Policymakers should require modular, software-defined architectures and open interfaces so the Department can continually upgrade components over time and avoid vendor lock-in, while maintaining real competition for new capabilities. Funding should emphasize virtual testing, high-quality data collection, and continuous software updates so capabilities improve on a modern software cycle, not on multi-year paperwork-driven timelines.