Trucks play a very role important role in driving the nation's economy, moving more than 70% of all the freights transported in the US by weight. Any event that grounds all trucks even for a few days, have severe consequences, including food shortages, hospitals exhausting their oxygen supplies, and gas stations running out of fuel. While we have not yet faced such a situation, the way modern heavy vehicles are designed, this increasingly looks like a distinct possibility. Modern day trucks are equipped with numerous sensors, embedded controllers, communication networks, and electro-mechanical systems that work in tandem to improve their performance, efficiency, safety, connectivity, and user-experience. However, they also bring up serious cyber threats to the truck's operation. This talk discusses cyber security vulnerabilities our group has identified that span across all modern day heavy vehicles and allow a hacker to access the embedded controller network of a truck to cause different types of attacks. We present some approaches for detecting attacks in real-time and show how we can distinguish them from safety-critical events. We have developed reporting tools and techniques that can aid the heavy vehicle drivers in near real-time to make informed decisions in the event of a cyber attack. We also discuss how we can achieve cyber-resiliency and conclude by discussing some of our future research directions in heavy vehicle security.