

CAN transceiver in sanctioned military equipment



Some combat drones attacking Ukraine are equipped with CAN transceivers made in U.S.A. (Source: National Police of Ukraine)

CAN technology itself is not subject to a general sanction, but some CAN transceivers have been found in sanctioned military equipment. CAN networks are widely used in military vehicles and combat drones, for example.

Ukrainian authorities have identified various CAN transceivers, particularly from manufacturers like Microchip and Texas Instruments (TI), in Iranian-made Shahed-136 (Geran-2) kamikaze drones as well as Russian-made Lancet and Orlan-10 UAVs (unmanned aerial vehicles). These components, which are common commercial off-the-shelf (COTS) parts used in automotive and industrial applications, are part of ongoing efforts to track and potentially restrict the supply chains of military technology used in conflict zones.

CAN transceivers and controllers have been identified as critical components in military technology, leading to intensified monitoring and sanctions enforcement by global authorities. Authorities have documented CAN components (e.g., Microchip MCP2515 and various Texas Instruments VP230/VP232 transceivers) used in UAVs and missiles like the Russian Kh-69.

Because CAN technology is essential for the communication between flight controllers and sensors in loitering munitions (e.g., Shahed-136/Geran-2, Lancet), these parts are frequently listed in databases used by customs to enforce sanctions against dual-use technology. One of these platforms is [Ukraine War & Sanctions](#) and another one is [War Sanctions](#). Reported are also cases, in which CAN stand-alone protocol controllers by Microchip were utilized in Russian BM-35 kamikaze UAVs.

Texas Instruments strongly opposes the use of their chips in Russian military equipment and the illicit diversion of our parts to Russia. The company said: "Any shipments of TI products into Russia are illicit and unauthorized. It is our policy to comply with export control laws and we

require our customers and distributors to do the same. If there is evidence indicating diversion, we investigate and take action."

Microchip stated, that they do not sell products into countries where their technology is prohibited from sale such as Belarus, Iran, Russia, or sanctioned regions in the Ukraine: "We condemn the illegal use of our products. We take our responsibility as a good corporate citizen seriously, and comply with applicable laws, including export controls and trade sanctions. We take care to maintain supply chain integrity by various methods including screening customers against restricted party lists. Also, we partner with government authorities and law enforcement, as necessary." The company regards the diversion of legally sold products as an industry-wide issue. As a member of Semiconductor Industry Association (SIA), Microchip supports the SIA statement titled [Semiconductor Industry is Committed to Combatting Illicit Chip Diversion](#).

SIA explained that a pathway to illicit diversion is through the "gray market," in which chips are diverted outside of authorized distribution channels into the hands of dealers, brokers, or the open market: "Many of these second- and third-hand resellers are not publicly traded companies, and some operate from jurisdictions where there are laxer local controls and regulations, creating a ripe environment for clandestine procurement networks to operate." According to SIA, some lower-end chips that have been found in Iranian and Russian military equipment were, upon analysis, identified as being produced illegitimately by counterfeiters and re-marked as genuine.

hz