MICHIGAN STATE UNIVERSITY | Center for Anti-Counterfeiting and Product Protection

Counterfeit Parts in the U.S. Department of Defense Supply Chain

Brandon A. Sullivan
Jeremy M. Wilson
A-CAPP Center Backgrounder
April 2016

Counterfeit parts in the U.S. Department of Defense (DOD) supply chain threaten national security by compromising critical military operations and placing the lives of military service members at risk. These counterfeits are difficult to identify and are reported inconsistently when discovered. In an effort to raise awareness and generate discussion, this Backgrounder highlights criminal cases involving counterfeits in the DOD supply chain to illustrate the nature of the risk as it relates to types of counterfeit parts and how they entered the supply chain and then were identified, and the adjudication of individuals involved in the counterfeiting schemes.

Threats to national security resulting from product counterfeiting are a growing concern, particularly when counterfeit parts are installed in weapons, equipment, safety gear, and communications systems used by the U.S. Department of Defense (DOD).

Several attempts have been made to qualify and quantify the risk. Hearings held by the U.S. Senate Committee on Armed Services in 2011 and 2012 identified more than 1800 cases of counterfeit electronic parts and one million individual suspect parts in 2009 and 2010 (U.S. Senate, 2012). A U.S. Department of Commerce (DOC) survey of counterfeit parts in the electronics industry noted an increase in incidents from 3,369 in 2005 to 8,644 in 2008 (U.S. DOC, 2010).

Of course, counterfeiting is not limited to electronics. Various counterfeit parts have been identified involving various weapon systems and other equipment. The Defense Logistics Agency (DLA) cited 19 different counterfeit parts used in over 100 different military systems, including aircraft and missile defense (U.S. Senate, 2012). Other examples include fasteners, titanium used in engine mounts, Kevlar® used in body armor plates, seatbelt clasps, oscillators for navigation systems, and part packaging (U.S. GAO, 2010).

Undoubtedly, the true extent of the risk is far greater. No products are immune from counterfeiting and the vast scale and complexity of the DOD global supply chain opens up various opportunities for their introduction, making those identified likely a lower-bound estimate. These counterfeit products pose a direct threat to military service members and the operations in which they are engaged.

One way of further understanding how counterfeits make their way into the DOD supply chain is to identify what product counterfeiting schemes have been identified, investigated, and charged in criminal courts. This is difficult given the limited access to data. Therefore, our approach to identifying these schemes is to collect open-source information on known cases of product counterfeiting and evaluate several key characteristics of those cases, including how, where, and by whom the schemes are conducted and how they are handled by the legal system. To illustrate how we set out to accomplish this task, we next outline the data collection, searching, and coding criteria for the A-CAPP Center Product Counterfeiting Database (PCD), then describe three criminal cases identified through these efforts.

Product Counterfeiting Database

The PCD assembles information on product counterfeiting using an open-source methodology to gather evidence pertaining to product counterfeiting schemes, offenders, and victims. The database serves as a foundation for developing evidence-based lessons on preventing, detecting, investigating, and responding to product counterfeiting.

To identify these product counterfeiting schemes, we searched the websites of various government agencies and industry organizations that monitor product counterfeiting. From these websites, we reviewed all reports, case studies, press releases, speeches and other documents related to product counterfeiting. We also conducted keyword searches at these websites as well as online databases and news outlets.

After developing an initial list of schemes, we utilized two web-based meta-search engines to capture as much open-source information as possible on each scheme and determine the number of offenders involved. The source of information uncovered originates from court and government records, industry reports, news media, videos, blogs, books, and scholarly accounts. We also uncovered additional schemes during these searches which were then subjected to additional searching and evaluation to determine if they met our inclusion criteria.

Once the schemes were fully searched, we created unique databases for the schemes, offenders, and victims. These databases describe the characteristics and processes associated with the chemistry of these crimes, establishing the basic parameters of the problem (e.g., the number and attributes of suspects and the quantification of harm in terms of seized goods and victims) as well as the response to it (e.g., which agencies identified and investigated the offenses and for what the suspects were charged, convicted, or sentenced). These data provide empirical insights into the counterfeiting of parts and equipment in the DOD supply chain.

To date, we have identified a number of schemes that have been indicted in U.S. courts. While we are at the initial stages of the coding process, these three cases provide an overview of the broad scope of the problem, including the different types of parts that have been counterfeited and those who have been criminally charged.

Counterfeit Helicopter Parts

One major criminal case from the early 2000s involved counterfeit helicopter parts. A California man sold flight-critical rubber seals intended for the H-60A (Black Hawk) and H-60 (Sea Hawk) helicopters to the Air Force, Army, Navy, and NASA. He was required by contract to purchase the parts from a DOD-approved Chicago-based supplier, but instead, purchased them from a Taiwanese company for roughly $1 each and mislabeled them, giving the appearance that the parts came from the approved supplier. These substandard quality parts may have failed when installed, placing the lives of U.S. military service members at risk. The perpetrator pled guilty in 2004 and was sentenced to two and half years in prison along with three years of supervised release, and ordered to pay nearly $55,000 in restitution to DOD. A similar scheme occurred from 2005 to 2008 involving counterfeit helicopter parts, where the perpetrator sold microprocessor chips with fake markings to an aerospace contractor.

Counterfeit Integrated Circuits Intended for Nuclear Submarines

As noted above, counterfeit electronics represent a substantial risk. One example of this was the scheme perpetrated by a Massachusetts man who imported thousands of counterfeit integrated circuits (ICs) from China and Hong Kong. From 2007 to 2012 he sold these counterfeits to U.S. customers, one of which was the U.S. Navy, who unknowingly purchased the counterfeits for use in nuclear submarines stationed in Groton, Connecticut. These ICs contained counterfeit marks from major electronics manufacturers, including Motorola,

Xilinx, and National Semiconductor. While he specifically stated the ICs were new products manufactured in Europe, product testing by the U.S. Navy revealed the data code had been altered to hide the fact that they were refurbished and branded with counterfeit marks. The perpetrator pled guilty in 2014 and was sentenced to 37 months in prison. In addition, he was ordered to pay $352,076 in restitution to the 31 companies whose products he counterfeited and forfeit $70,050 in currency and over $35,870 worth of counterfeit ICs. In addition to this case, several others involving counterfeit ICs have been identified in recent years.

Counterfeit Computer Networking Components

Numerous other schemes have involved the sale of counterfeit computer networking components to government agencies, including DOD. The majority of these stem from Operation Network Raider, a collaborative effort between Cisco® and law enforcement by Immigration and Customs Enforcement (ICE), Federal Bureau of Investigation (FBI), and Customs and Border Patrol (CBP) working with the Department of Justice (DOJ) Criminal Division's Computer Crime and Intellectual Property Section, the National Intellectual Property Rights Coordination Center, and numerous U.S. Attorney's Offices. One of these cases involved two Texas men who illegally imported low price network cards from China and later affixed them with counterfeit Cisco® logos and labels to be sold throughout the U.S. Some of these counterfeit parts were sold directly to federal agencies, including the Marine Corps, Air Force, Federal Aviation Administration (FAA), Department of Energy (DOE), Bureau of Prisons (BOP), and FBI, as well as various defense contractors (such as Lockheed Martin), schools, and financial institutions. A similar case also involved a Texas man who purchased counterfeit Cisco® parts from China for sale to the Marine Corps. These counterfeits were intended for use in vital intelligence and security equipment by the Marine Corps at a U.S. military base in Iraq. Both cases resulted in convictions and prison sentences for the perpetrators.

Ongoing Issues and Challenges

These cases point to a number of different ways counterfeits can be introduced into the DOD supply chain. However, these are only a few examples that have been reported to criminal justice authorities and adjudicated. The actual scope of counterfeiting in the DOD supply chain, similar to other types of counterfeiting and crime generally, is likely greater than what is currently known.

Improving the ability to detect and report counterfeits is an important priority to ensure the quality of parts used in military equipment. The 2011-2012 U.S. Senate hearings resulted in a number of recommendations and improvements, including the requirement that all DOD agencies and contractors report counterfeiting incidents. However, establishing reporting requirements has limited effectiveness if other challenges are not addressed. Improvements over past lack of reporting have been made, but substantial shortcomings persist.

Various and sometimes inconsistent definitions of what constitutes a counterfeit remain. Defining counterfeiting has been an ongoing issue. Numerous conceptualizations and measurement techniques for determining counterfeits are present across agencies and industries (Wilson, Sullivan, & Hollis, 2016). This problem has not escaped the DOD, as different DOD agencies have used their own definitions for what constitutes a counterfeit (U.S. GAO, 2010). This means that the same agency may identify numerous counterfeits while another who encounters the same or similar counterfeits may not.

Even when a consistent definition can be agreed upon, reporting may not be uniform. Applying these definitions requires expertise in distinguishing counterfeits from genuine products, which may not always be feasible even by industry experts. Counterfeiters are

becoming increasingly sophisticated in creating nearly identical copies. Without intervention, consistently applying definitions and identifying and reporting counterfeits will likely remain a challenge for some time.

A recent U.S. Government Accountability Office (GAO) report (2016) found several issues with DOD's implementation and oversight of these reporting systems. While reporting increased during the U.S. Senate investigation as contractors identified many counterfeits that had not been found earlier, reports dropped off substantially in the years following these hearings. DOD agencies and contractors cited better distributor selection standards, but GAO (2016) noted an amnesty period allowing reporting without naming suppliers also contributed to the short-term increase in reporting. The reluctance to name suppliers stems from concerns over jeopardizing contracts and potential legal actions resulting from damaging supplier reputations. Furthermore, reporting across agencies remains inconsistent (U.S. GAO, 2016). This substantiates GAO recommendations for increased oversight of reporting and clarification of what evidence should be reported as well as improved authenticity testing procedures. Finally, cooperation between agencies and with contractors is essential to effective anti-counterfeiting strategies. Brand owners have consistently cited this as key to their efforts at addressing counterfeiting (Wilson & Sullivan, 2016). Taking advantage of industry expertise and sharing information will go a long way toward establishing the extent of counterfeits in the DOD supply chain and taking constructive steps toward addressing this persistent problem (U.S. GAO, 2010, 2016).

REFERENCES

U.S. DOC. (2010). *Defense Industrial Base Assessment: Counterfeit Electronics.* Washington, DC: U.S. Department of Commerce. Available at: http://www.agmaglobal.org/cms/uploads/BIS%20Survey%20(January%202010%20final).pdf

U.S. GAO. (2010). *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts.* Washington, DC: U.S. Government Accountability Office. Available at: http://www.gao.gov/assets/310/302313.pdf

U.S. GAO. (2016). *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk.* Washington, DC: U.S. Government Accountability Office. Available at: http://www.gao.gov/assets/680/675227.pdf

U.S. Senate. (2012). *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain.* Washington, DC: Committee on Armed Services, U.S. Senate. Available at: https://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf

Wilson, J. M., & Sullivan, B. A. (2016). Brand owner approaches to assessing the risk of product counterfeiting. *Journal of Brand Management.* Online First. doi:10.1057/bm.2016.10

Wilson, J. M., Sullivan, B. A., & Hollis, M. E. (2016). Measuring the "unmeasurable": Approaches to assessing the nature and extent of product counterfeiting. *International Criminal Justice Review.* Online First. doi:10.1177/1057567716644766

The Michigan State University Center for Anti-Counterfeiting and Product Protection (A-CAPP) is the first and preeminent academic body focusing on the complex global issues of anti-counterfeiting and protection of all products, across all industries, and in all markets, and on strategies to effectively detect, deter, and respond to the crime. Linking industry, government, academic, and other stakeholders through interdisciplinary and translational research, education, and outreach, the A-CAPP Center serves as an international hub for evidence-based anti-counterfeit strategy. For more information and opportunities to partner, contact Dr. Jeremy Wilson, Director of the A-CAPP Center, at (517) 432-2204 or jwilson@msu.edu. Additional information can also be found at a-capp.msu.edu.

© 2016 Board of Trustees of Michigan State University. All rights reserved.