

Toward More Reliable Sourcing: Combatting Counterfeit Electronic Components in the United States Department of Defense Supply Chain

By: Andrew L. Simon
Thesis Advisor: Dr. John Park

Summary: Counterfeit electronic components in military systems raise costs and endanger lives. Because the United States Military requires millions of replacement parts, many of which are no longer manufactured, their entrance into critical supply chains is seemingly inexorable. My work attempts to understand the mechanisms feeding materials to counterfeiters and establishes future research goals as well as corrective steps to better understand and mitigate counterfeit components emanating from Asia.



Andrew holds a J.D., cum laude from New York University School of Law and an A.B., magna cum laude, from Washington University in St. Louis. While an Associate at Skadden, Arps Slate, Meagher & Flom LLP, Andrew advised clients on a range of business and litigation matters. Subsequent to Skadden, Andrew worked with a start-up beverage company and has consulted for several technology and internet start-ups, focusing his efforts primarily on project management, strategic market entry, capital raising, market sizing, financial projections, and scalability.

KEY INSIGHTS

1. Key electronic components manufacturing countries, such as Malaysia, have an abundance components discarded from the manufacturing process. Falling scrap prices provide financial incentives for e-waste recyclers to sell discarded components to counterfeiters rather than engage in materials recovery.
2. Re-aligning the e-waste recyclers' financial incentives with those of legitimate interests through component re-certification programs as well as other recycling projects can help reduce the supply of discarded components available to counterfeiters.
3. Reduced supply of discarded components and increasing availability of legitimately re-certified components can hinder counterfeiters' businesses and improve overall supply chain reliability without relying solely upon costly, time-consuming, and possibly ineffective point-of-receipt inspections.

Introduction & Background

In May 2012, the United States Senate Committee on Armed Services revealed that roughly 1,000,000 counterfeit electronic components made their way into the United States Department of Defense supply chain from 2009-2010 and, worse, that some were installed in critical platforms such as THAAD missile defense systems. Counterfeit electronic components are used parts resold as “new” or are altered to appear as higher-grade items than they actually are. Images 1 & 2 show an integrated circuit that appears to have been counterfeited. At best, counterfeit electronic components are a form of fraud while, at worst, their suppliers are stealing United States taxpayer dollars while simultaneously endangering the lives of U.S. military personnel and ultimately U.S. national security. U.S. Government publications from the last 5-8 years have noted the problem and highlighted the increasing incidence of counterfeit components. Congress and President Obama recently ordered the Department of Defense to eradicate these malignant components from the United States’ critical supply chains by passing the National Defense Authorization Act in January 2013. It is imperative that the U.S. Government now takes proactive steps to implement this mandate. The question, of course, is how.

Presently, many people have offered “fence solutions.” I use the term “fence solution” to refer to any technique designed to keep counterfeits out, usually via screening, rather than approaches that address the problem’s root causes. Most counterfeit electronic components come from Asia, particularly China. But, of course, even counterfeiters must source raw materials to produce their wares. Electronic waste (discarded components

and electronic equipment) is the raw material used by counterfeiters to produce knock-off parts. Therefore, if we can reduce the supply of discarded components presently available to counterfeiters, we can combat counterfeits at their source, rather than on American soil.



Image 1: Part # AD677KR

Source: Erai, Inc. Counterfeits Database



Image 2: Part # AD677KR (Acetone swab removes markings)

Source: Erai, Inc. Counterfeits Database

Research & Analysis

Because there is very little research on the e-waste business as it relates to counterfeit components, I conducted structured interviews over the course of six months to explore the workings and incentives that drive e-waste vendors to sell components to counterfeiters. I interviewed several industry participants and attended talks by others to gain a broad understanding of the business as well as a detailed understanding of how legitimate and illegitimate e-waste transactions work.

I found that integrated circuits (IC) – a type of semiconductor – are usually the most valuable and are therefore highly sought after by counterfeiters. Malaysia produced 164.9 billion integrated circuits from 2008-2012, of which roughly 1.5% (a very conservative estimate) are discarded

as rejected or obsolete. These discards are special though because they are “high quality.” That is, they are unused and therefore will be in better condition, making them more difficult to detect later. Accordingly, such e-waste poses an especially high risk to DoD supply chains.

Relying upon public data, I found that the average Malaysian IC sells in legitimate wholesale ecommerce for RM 0.585 (roughly \$0.19 USD) per piece. Based on my interviews, I estimate that a discarded IC sells for half that (RM0.2925 per piece).

Meanwhile, of the 1.1 million tons of e-waste generated in Malaysia each year, roughly 75% is unaccounted for. This is unsurprising given the falling precious metal concentration in electronic components, a response to rising materials cost, that has led to reduced value in reclaiming metal from e-waste. Many operators in western nations address this problem by charging their clients a fee for e-waste removal. This, however, is not the practice in Asia and, therefore, the situation leaves substantial opportunity for counterfeiters to procure discarded components from e-waste vendors.

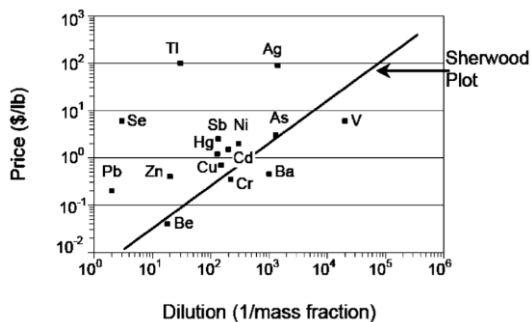


Figure 1: “Sherwood Plot”, a graph that shows the concentration at which virgin ore can be profitably mined. This allows for rapid assessment as to whether a metal is enriched or diluted in a component as compared to its original source.

Source: (Johnson, 2007 – reprinted there with permission of the National Academy of Sciences)

Data uncovered through the interviews reveals that a small e-waste operator can easily earn RM10,000 per month by selling just a few key components to counterfeiters. Meanwhile, a corrupt vendor can earn substantially more, even millions of ringgit, by systematically procuring and selling discarded components. Indeed, based upon publicly available data, the Malaysian market for discarded ICs is likely in the neighborhood of RM 200 million per year. With only about 30 e-waste companies operating in Malaysia, the financial incentive to skip the scrapping and instead sell to counterfeiters is clear.

Solutions

“Fence solutions” can only go so far, to truly solve the counterfeits problem, we must address its root cause: financial incentives. Electronic components, and ICs in particular, have tremendous value in secondary markets where governments and large businesses turn to procure replacement components for legacy systems. So, instead of having an e-waste recycler or other business sell to counterfeiters or suspect parties, we should establish a system where reliable, independent third-parties can certify that discarded, but new, parts are still in fact good parts capable of reliable use in certain applications. Furthermore, we can find other recycling uses for e-waste – something at least one Malaysian vendor is already doing – and, in this way, re-align their financial incentives with those of legitimate interests and thereby reduce the supply of “high quality” discarded electronic components available to counterfeiters.