Counterfeit Prevention Strategies in the Military Supply Chain: Increasing Reliability at a Higher Price

Hans M. Sassenfeld

Capstone: The University of Texas at El Paso

November 14, 2013

Abstract

The reports of counterfeit[1] electronics in the military supply chain by the Commerce Department in 2010 and Senate Arms Services Committee in 2012 spurred major legislative changes that were implemented in the National Defense Authorization Act of 2012. This study in comparing the previous noted reports to new cases reported for 2012 and 2013, found a significant reduction in reported suspect counterfeit case of 50% in just the last year. Improved processes, training, and reporting were all government mandated in 2012 and contributed to the reduction. The study investigates the trends in the military electronics supply chain affected by counterfeiting and assesses the current and future risk to the supply chain. The key findings were increased manufacturing cost and a reduction in suppliers at all levels of the supply chain. These trends will continue and may be exacerbated if recent proposed legislation is passed to extend the definition of counterfeit electronics to that of defective components.

Keywords: Counterfeit, Electronic, Component, Military, and Detection

Research Question

Has the implementation of counterfeit prevention strategies in the U.S. reduced the number of counterfeit incidents and what are the predicted implications and consequences to the viability of component suppliers, manufacturers of military hardware, and current military systems?

Significant reduction in counterfeit cases has direct impact on overall military supply chain

To address the special conditions resulting from the explosion of counterfeit parts the 2012 National Defense Authorization Act (NDAA) was passed. This law pushes the responsibility from the government to the system supplier. So the cost to replace counterfeit parts found in military systems will now be borne by the contractor, not the government. This places a huge burden on the manufacturer of military electronics to prevent counterfeit parts. Failure to do so would now result in billions of dollars in liability to corporations. As a result the manufacturers have implemented many new measures to prevent and detect counterfeit parts, but these are increasing the cost of manufacturing, lengthen the manufacturing time, and putting many small manufacturers and brokers out of business. The long term impacts to weapon systems could be very significant. It is even more alarming that counterfeit parts can be design to introduce weaknesses into military products. These cases need to be evaluated to determine if a concerted effort is underway to subvert major U.S. military systems and if so who is behind these attacks. The main questions the research seeks to answer are whether the number of counterfeit incidents is dropping or is increasing, what is the source, what measures are most effective, and what will be the future impacts on the military electronics supply chain.

Literature review finds little current data on counterfeiting since NDAA became law

The main focus of this research paper is to determine trends, sources, detection methods, and motives associated with counterfeit electronic components. Government published sources provided the majority of assessments in these four areas. In 2010 the Commerce Department released a report that utilized survey information from 387 organizations in five areas of the supply chain to investigate counterfeiting from 2005 through 2008. This was followed in 2011 with Congressional hearings by the U.S. Senate Armed Services Committee (SASC) which included public testimony by various companies and industry experts. Following the hearings the same committee released a detailed report in 2012 that combined the Commerce Department

[1] The word "Counterfeit" in this report is used to refer to both confirmed and suspect counterfeit cases.

findings, an internal GAO audit, public testimony, and internal work by the committee. This report has been widely accepted and quoted by many of the other sources utilized for this research. It is significant in that the report has driven action by Congress and the executive branch to address the findings. The smaller reports and articles reviewed, focus on unique issues associated with counterfeit electronics, but are consistent with the final 2012 report of the Senate committee. The 2013 report by General John Adams, *Remaking American Security*, provides an industry focused study on the issues of American competitiveness of which counterfeiting and intellectual property rights are a significant subset. The article by Burgess, Marcario, Kreisher, and Scully, "Legislation Being Drafted To Address Problem of Counterfeit Military Parts", provides insights into possible legal changes that would have significant impact to the supply chain, if initiated by Congress. No literature was found addressing current trends since the SASC released its report in early 2012.

Background investigation finds rapid growth in counterfeit electronics from 2005 to 2011

The most quoted estimate today of the impact of counterfeit parts comes from the Senate Arms Services Committee with the committee uncovering 1,800 cases of suspect counterfeit parts representing over 1 million parts. The 1800 cases covering the period of 2009 through the 1st quarter of 2011 consist of: 200 from Defense Logistics Agency (DLA), 150 from contractors, and 1,500 from testing houses. (Senate Armed Services Committee - 112th Congress 2012, 12) The bulk of the numbers from the SASC report come from testing houses. Many of these failures would be due to counterfeiting, but some percentage would be due to components that failed up-screen testing. Up-screen testing is done when components are needed that meet higher standards that those published by the manufacturer. So the published number may be inflated, but on the flip side it does not include seizures by Customer and Border Protection (CPB) of counterfeit parts prior to entering the supply chain. The Commerce report used a different method from the SASC by utilizing questionnaires to institutions covering five sectors of the supply chain. Although this methodology was different, the findings also showed rapidly rising incidents of electronics counterfeiting from 2005 through 2008 (U.S. Department of Commerce 2010, 5). Luckily to date, there have been no attributed fatalities due to counterfeiting; although the list of affected systems is extensive and includes: P-8A Poseidon, SH-60B helicopter, thermal night vision sights, missile interceptors, GPS guided artillery shells, Stryker Mobile Gun, and seven different aircraft types (Capaccio 2012, 1). Edwards also found rapid growth in the counterfeit industry (Edwards 2009, 41). McGrath estimates are that between .5% and 5% of the military parts procured today are counterfeit (McGrath 2012, 1). All these reports would indicate either rapid growth in counterfeit components or may just reflect increased detection rates.

Counterfeiting driven by increased cost of military components

In assessing counterfeiting trends it is necessary to evaluate the reasons counterfeit parts are made and their ability to enter and proceed up the supply chain. The most significant reason counterfeit parts are made in the first place is for financial gain. It has been proposed that counterfeit parts could be produced for the intent of caring out a cyber attack. Components modified for cyber attack cannot be ruled out as a motive, although no conclusive literature was identified and no cases were identified in this study. Both motives will be evaluated. As the parts move up the supply chain the profit motive is still the most significant with regards to suppliers and distributors. The need to find replacement parts to support systems operation increases.

Prior to counterfeit awareness by the government and industry, the price for both counterfeit and real parts was driven by the classic supply demand curve. The highest priced components were therefore those that had very high demand and were in low supply. This was the lure for counterfeiters. Counterfeit awareness and legal changes have undoubtedly changed the basic curve but it provides a means to evaluate the underlying drivers of counterfeiting.

Demand for Military Components on the Rise

Military electronics are in high demand due to their overall operating parameters, reliability, and quality. Typically military components and other critical parts have an operational temperature range of between -40 to 85 degrees Celsius as required for military missions that can be required anywhere on the globe (Pecht and Humphrey 2008, 741). The military specifications (Mil-specs) not only dictate the functional parameters of military components, but also the testing required to verify compliance. High demand is also due to the criticality of the components to overall system operation. For example, a C-17 would be grounded if a single electronic fuel sensor failed. The demand for a replacement part to get the aircraft operational and flying again would be very high. The demand for spare parts has also increased due to the extended military missions in Iraq and Afghanistan (U.S. Department of Commerce 2010, 1).

Diminishing Supply Base Reduces Parts Availability

The diminishing supply of military electronics is due to a shift in the number of suppliers. When the B-52 was placed into service over 50 years ago the military was the largest purchaser of electronic components (McHale 2000, 18); (Edwards 2009, 40); (Sandborn 2008, 44). The commercial electronics industry boomed with the introduction of the personal computer in the 80s. The first Apple II computer was built using many Mil-spec components because they were the only ones available at the time. The commercial electronics industry found the quickest way to lower the cost of a component was to reduce the strict requirements of the Mil-Spec system, such as reducing the operating temperature range. This shifted the main manufacturing focus from military to commercial. The bursting of the tech bubble and a shift to off shore manufacturing further reduced the sources of domestically available military suppliers and the components they manufacture. As an example: printed wiring boards (PWBs) that connect all the electronic components together were mainly produced in the U.S. by thousands of commercial and military manufacturers. Today, that number is around 300 with a much smaller subset producing military grade PWBs (Matties 2012). When there are no longer any suppliers of a part, it is then classified as obsolescent. Sandborn points out that military, transportation systems, and aerospace all have high development and implementation cost (Sandborn 2008, 44). He concludes that to offset these cost systems must be in continuous use for 20 plus years to recover their return on investment. To recover this investment product life cycles of 20 to 40 years are common (McHale 2000, 20). With the dwindling supply of sources many components are becoming obsolete long before their designated system life cycle.

Shift to Low Cost Commercial Electronics is Affecting Reliability of Military Electronics

The military electronic supply side took another hit as an unintended consequence of the acquisition reforms implemented in the 1990s. Sean Fernandez was quoted by (McHale 2000, 18) as saying, “When former Secretary of Defense William Perry first issued his commercial-off-the-shelf (COTS) edict in 1994, people jumped on the bandwagon and ordered everything COTS.” The primary focus of the reform was to push for greater use of COTS to reduce the cost of military systems. This hurt the military electronics industry because it reduced the demand for

military grade electronics and injected a whole set of issues directly related to commercial components.

The most damaging was the commercial move to Lead free solder. Solder is a metal compound that has a relatively low melting point and is used to electrically connect components. The European Union first passed laws to limit the use of Lead in electronics manufacturing due to environmental concerns. This standard known as ROHS (Restriction On use of Hazardous Substances) has been applied to the entire commercial market place. Europe's prohibition of Lead forced commercial electronics manufacturers to switch to a pure Tin solder. This change reduced the solder joints flexibility and resulted in more frequent solder fractures and failures. Lead's elimination and use of pure Tin in commercial solder joints is partially responsible for the low 2 to 4 year service life now typical for the commercial electronic market place (Sandborn 2008, 44). Pure Tin can also form crystalline Tin whiskers that can cause catastrophic system failure. This was detected after failure of a Boeing satellite system in orbit that had utilized pure Tin solder (Sandborn 2008, 45). As a result of these failures, military systems can no longer use pure Tin components and manufacturers are less likely to produce both a Lead free and Tin/Lead component (Edwards 2009, 41); (Sandborn 2008, 45). Even newer commercial manufacturing trends such as Gold leaded parts, plastic components, and vented Ball Grid Arrays (BGAs) all provide for lower cost but sacrifice reliability, expected in military components. Commercial production therefore trumps military production.

These two factors: the growth of the commercial market and the push for military systems to use commercial components, have resulted in only 1% of semiconductors today are specifically produced for the military (Adams 2013, 157). Today with such a low market for military and aerospace grade components there is little incentive for manufactures to produce them. According to Sandborn, "The Defense Department spends an estimated $10 billion per year managing and mitigating electronic-part obsolescence." (Sandborn 2008, 44) For a component manufacturer it is more profitable to produce millions of components for an Apple I Pad as opposed to 100 electronic unique components for a B1-B bomber; only 100 B1-Bs were originally built. The electronic suppliers today are more likely to be overseas. Tonelson reported China provided 28% of the commercial electronics used in military hardware and that "share has roughly tripled since 1997" (Tonelson 2012, 1). The end result of high demand and low supply of military electronics is a high cost for these components. Crime detection in law enforcement looks for motive and opportunity, so too in tracking electronic counterfeiters, the motive is profit due to high component prices while offshore manufacturing provides the opportunity.

China Provides the Right Environment for Counterfeiting and Possible Espionage

One country with the aforementioned motive and opportunity is China. In China the counterfeit parts industry takes scrap electronic boards and black market individuals hold the boards over a fire to remove the components. These are then feed to companies that clean, resurface and print markings identical to original parts (Spiegel 2011, 51). The most common tactic is to take lower performing parts and remark them indicating a higher performance part (Electronics Weekly 2012, 1). These measures use old parts to turn a quick profit. China also possesses the capability to produce new non-counterfeit components, but if these factories run low on legitimate production they can turn to counterfeit components to prevent the factory from becoming idle (Spiegel 2011, 51). New component production houses that choose to counterfeit have the capability to additional circuitry. This adds a new twist in that it is possible to incorporate Trojan or back door hardware that could upon external command initiate a cyber

attack. There is fear that a cyber attack using counterfeit components could be timed or triggered to strike critical infrastructures like communications, banking and even power grids (Cheng and Scissors 2011, 1). While it is possible, it is highly unlikely, as the complexity of each electronic system prevents multi-functionality of components. Input and output requirements of components are strict and further limit the possibility of Trojan code. It would be much more likely that a system would be developed that as a whole could have counter purposes such as cyber warfare.

2012 NDAA Fires First Salvo in U.S. War on Counterfeit Electronics

To address the special conditions resulting for the explosion of counterfeit parts the 2012 National Defense Authorization Act was passed (McGrath 2012, 2). This law pushes the responsibility from the government to the prime contractors supplying the government (Baljko 2013). So the cost to replace counterfeit parts and all associated cost, like loss of an aircraft, will now be borne by the contractor and this liability extends down the entire supply chain (Beidel 2012, 1); (Burgess, et al. 2011, 7). This pushed contractors to implement the government's counterfeit recommendations rapidly to minimize exposure and mitigate risk. The primary change forced contractors to only purchase from Original Equipment Manufacturers (OEMs) and their authorized distributors. These parts must have a certificate of conformance (CoC) stating they meet all specified parameters. Those parts purchases from authorized distributors must also include a chain of custody certificate that is traceable back to the original manufacturer (Electronics Weekly 2012, 2); (Spiegel 2011, 51). These basic precautions have all been implemented by major corporations such as Boeing, Lockheed, and Raytheon. This provides good protection for new parts. Unfortunately, many of the components required today are no longer in production. These cases require additional precautions know as Counterfeit Electronic Part Avoidance (CEPA). The CEPA process requires component engineers evaluate potential component sources and imposes specialized testing to validate the components. This process must be initiated prior to actual purchase of the parts. The CEPA process may require that the proposed parts supplier's facilities be certified and monitored. Even the parts supplied by the government own DLA (Defense Logistics Agency) require CEPA approval and processing.

Detection Methods Provide Final Line of Defense

To support the testing required by the CEPA process and any time a counterfeit is suspected, the industry and testing houses have developed numerous testing methods. Currently there is no single perfect test that will detect 100% of the counterfeit parts. So usually multiple testing methods are employed in an effort to improve detection rates. Table 1 provides a listing of some of the more widely used methods. When counterfeits were first identified in 2008 as an issue, the most common method of detection was high failure rates. Visual detection methods were developed as general awareness of counterfeiting grew. The counterfeiters responded with better blacktopping (process of resurfacing a chip to cover over original markings) and improved marking methods. The inability to visually distinguish counterfeits spurred the investment and growth in the other listed detection methods. Detection methods provide the last chance to catch a counterfeit before they are placed into the manufacturing process. The later in the manufacturing process that a counterfeit is detected, the higher the amount of rework and the associated cost. This is sometimes referred to as the "cost of quality".

Explanation of Counterfeit Test Detection Methods with (Code):

Visual Inspection (V) {Non-Destructive}: Suspect counterfeit parts can be detected by inconsistent markings, uneven lead forming, solder appearance, uneven blacktop, and pin one marking differences.

Resistance to Solvents (B) {Non-Destructive}: The components are swabbed with acetone to see if the markings are easily removed or the swab turns black indicating resurfacing (black topping).

Scanning Electron Microscopy (E) {Destructive}: Electron microscope is used to look microscopically at the surface of the component to detect black topping.

Dynasolve Test (D) {Non-Destructive}: A more aggressive chemical is applied to the component to see if markings or black topping can be removed.

Decapsulation & Die Microscopy (L) {Destructive}: Lid of component is removed and internal die and leads inspected. These are then compared to a know good lot of parts.

X-Ray (X) {Non-Destructive}: X-Ray machine used to look at internal construction of the component and compare to know good lot or to look for inconsistencies between lots.

MFG Specifications Data Sheet (M) {Non-Destructive}: The suspect component's physical and electrical parameters are compared with the published specifications for the part.

X-Ray Fluorescence (XRF) (T) {Non-Destructive}: Equipment test metal components and displays the spectrum associated with the metal compound. Can detect Pure Tin, Tin/Lead, Gold and other metals. These are then compared to see if the finish is per spec.

High Failure Rate (F) {Non-destructive}: Components identified that have a high failure rate in the assembly or during screening test.

Solderability (S) {Non-Destructive}: Steam aging machine used to measure if the finish will produce a sufficient solder joint.

Table 1

No Key Measure of the Number of Counterfeit Incidents, but GIDEP System Gaining

The Government and Industry Data Exchange Program (GIDEP) was started in 1959 to distribute information and component alerts throughout the defense supply chain. The database contains technical information discovered and shared throughout the product lifecycle. One category of alerts provided is "Suspect Counterfeit". The Commerce department reported that only 6 GIDEP reports were issued on "Suspect Counterfeits" in 2008 (U.S. Department of Commerce 2010). So data in the GIDEP database on counterfeits prior to 2008 is very limited. As a result of the Senate Armed Services Committee (SASC) report, the Congress passed and the President signed Section 818 of the National Defense Authorization Act of 2012 on December 31, 2011 (Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law 2012, 7). One of the requirements of NDAA section 818 is mandatory reporting of counterfeit incidents. This lead to the Department of Defense (DoD) on April 26, 2013 issuing instructions mandating reporting of counterfeits using GIDEP at all levels of the defense supply chain (Department of Defense 2013). So today it is the primary source of information on counterfeit electronic components within the supply chain and is available to the industry to help prevent and mitigate

the effects of counterfeits. For this report, GIDEP is the primary data source for current and projected assessments.

Current Assessment Found 50% Reduction in Reported Cases from 2012 to 2013

Based upon GIDEP reports from 2012 and 2013 the number of incidents has dropped by 50%. The process used to determine the reduction was to query the entire GIDEP database filtering for incidents reported in 2012 and 2013 (through the 3rd quarter) that were classified "Suspect Counterfeit". Analysis of the selected GIDEP records shows 107 incidents reported in 2012. This is a large increase in GIDEP reporting from the only 6 reports in 2008 as reported by the commerce department. It reflects a higher level of focus as a result of the NDAA mandate requiring reporting. In reviewing the data for 2013 it was originally thought the number would be higher based upon continued improved reporting, but the actual reports were only 40 for the first three quarters of 2013. This number annualized for a full year would only be 53. This represents a 50% reduction in reported cases. For comparison and validation the SASC report listed 271 GIDEP cases for 2009 and 2010 combined which equates to about 135 per year (Senate Armed Services Committee - 112th Congress 2012, 18). The 2013 annualized case rate of 53 represents a very significant drop.

So what are some of the possible reasons for the reduction? Detailed review of the 2012 cases showed many cases were directly related to parts procured from Hong Dark, a Chinese company and brokered through Global IC a U.S. distributor. The parts were originally procured as far back as 2008, but were being reported in 2012 as a result of increased testing and oversight by L3 Corporation. In 2012 the Air Force Deputy General Counsel issued a suspension of Hong Dark and Global IC Trading Group banning them from directly or indirectly doing business on any federal contract (Department of the Air Force - Office of the Deputy General Counsel 2012). The ban appears to have reduced the cases in 2013 and resulted in a direct reduction in incidents. The successful prosecution of the first counterfeit electronics case in 2011, resulting in a sentence of 38 months for the VisionTech administrator, also has had the effect of reducing counterfeiting (U.S. Department of Justice 2011, 1). Inconsistent reporting might account for some variation in the reported number, but once mandated should have, if anything, inflated the numbers on the high side. One other possible reason is that Customers and Border Patrol (CBP) also where directed to increase interdiction efforts. Their seizures for parts entering the country may account from lower numbers reported in the supply chain.

Review of the 2012 and 2013 GIDEP Data Shows China Still Significant Counterfeit Source

The SASC found that U.S. based companies were the first tier suppliers of counterfeit electronics in 80% of the cases. These distributors/brokers were then asked where they obtained the counterfeit parts and 70% identified China as the second tier. (Senate Armed Services Committee - 112th Congress 2012, 13-14) The commerce department report found similar results with 92% or 140 out of 152 organizations, with counterfeit incidents, reporting the source as China (U.S. Department of Commerce 2010, 177). Although several of the sources polled said, "their answers on where counterfeits originated were based on general information rather than their own experiences." (U.S. Department of Commerce 2010, 16). The GIDEP data analyzed for this report traced 59% back to the U.S. In all cases these were brokers (first tier) and no evidence was provided pointing back to the true source (second tier). This was lower than government reports, but consistent with overall findings. Of the second tier suppliers of counterfeit parts this report found 30% could be definitively traced back to China. See Figure 1.

This is consistent with the first tiers being U.S. based and second tiers from China as reported by SASC. The data did reveal that most reported cases in early 2012 did show that the tier one supplier (U.S. based) was able to identify the second tier supplier (China). With changes to the law placing greater liability burden on the first tier companies, a noticeable change was detected. Fewer distributors like Global IC Trading were open to identification of their tier two sources of counterfeit parts. This of course reduced information on the true sources and inflated the U.S. portion. Identification of the source of the counterfeits was also made more difficult by China's efforts to prevent the U.S. from investigating and cracking down on counterfeiters (Capaccio 2012, 1).

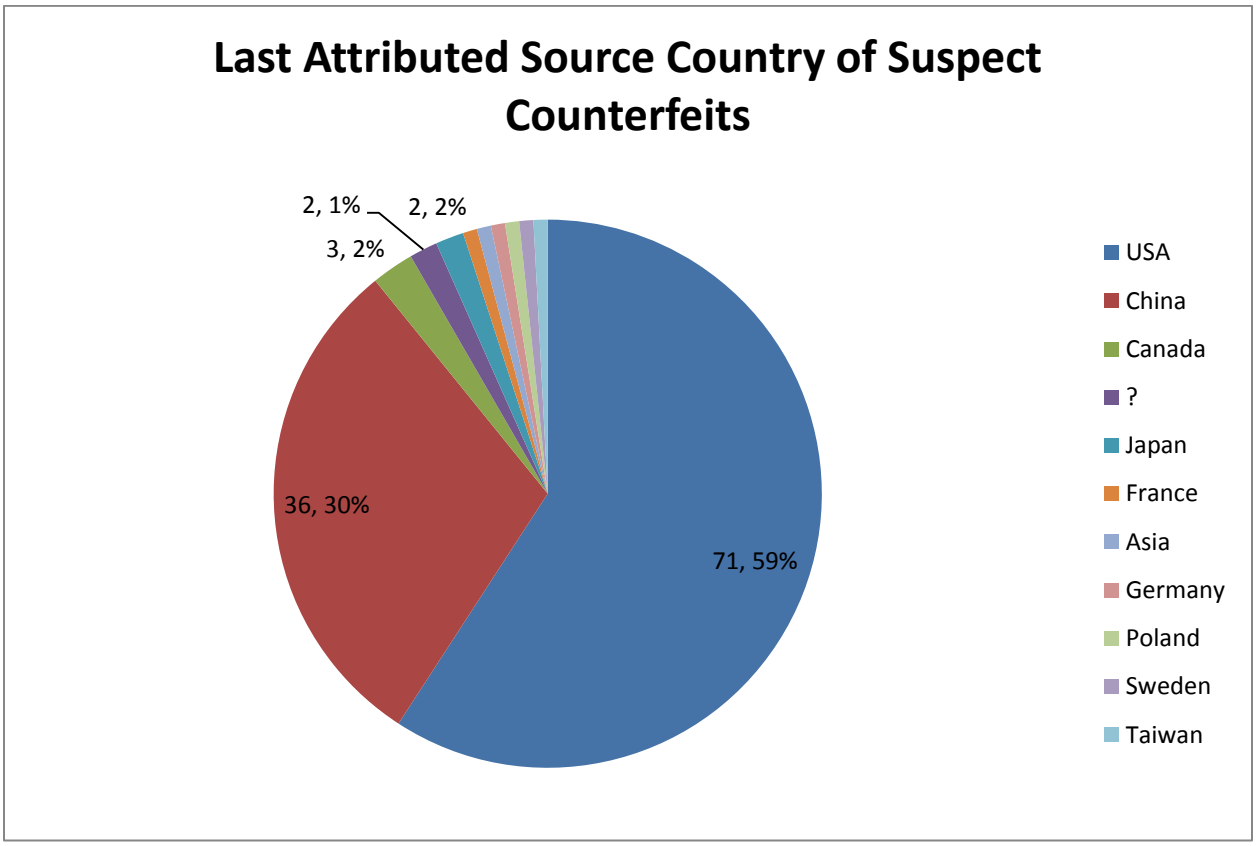

Figure 1

Detailed Analysis Could Find No Cases of Cyber Modifications

The query of the GIDEP "Suspect Counterfeit" data for 2012 and 2013 resulted in 147 records for the two years. These were entered into a spreadsheet with the following fields: GIDEP document number, date reported, title, pages, part number, and manufacturer name. Of the 147 records only 121 had detailed reports made available. Each of the 121 reports were then reviewed in detail to assess if indeed the report did provide sufficient evidence to support the classification of counterfeit, and in only one case was the evidence overwhelming that the component was not counterfeit. The remaining 120 records where then further assessed in detail as to the likely origin of the counterfeit component. Test methods were recorded and the detailed test data reviewed looking for possible added circuitry that would be an indication of cyber modification. This analysis added three nominal variable fields: Motive (Profit/Counterfeit), possible origin, and detection methods (Coded: V,B, E, D, L, X, M, T, F, or S). Of the 120 cases

reviewed in detail none of them exhibited evidence of circuit modification outside the basic functionality of the device. This would make sense as most discrete components serve only simple functions like current limiting and have no access to external stimulus which would be needed for a coordinated attack. Similarly logic components such as central processing units (CPUs) and memory modules do not have the capacity for standalone operation. This study shows that electronic components by themselves do not pose a cyber risk. The risk from cyber attack is greater in whole systems produced overseas such as communications and network equipment. These systems have the capacity for operation in cyber mode and have access to outside stimulus like the internet or wireless access. The GIDEP reports surprisingly showed that all suspect components were destroyed. This is surprising in that no hard evidence now exist that could be used for further study, or by the suspect supplier to prove that the parts were in fact good. It does of course prevent the parts from being reintroduced into the supply chain. While no cyber type devices were identified in the reported cases, there is a possibility that cyber components still exist, but have escaped detection.

2012 & 2013 Case Studies Consistent with Targeted Component Prices

Among the GIDEP cases reviewed for the report are those associated with counterfeiters Hong Dark, Global IC Trading Group, and Vision Tech. The total amount of the sales in each case where costs were identified was between $930 and $12,500 which seems relatively low from a risks verses benefit perspective. This was consistent with the commerce department findings of part values between $.11 and $500 (U.S. Department of Commerce 2010, 12) So counterfeiters made their money through selling of high quantities and multiple parts orders. For example: total annual sales for Vision Tech were estimated at over half a million dollars (U.S. Department of Justice 2011, 1). In about 5 of the 120 cases reviewed for this report the broker or vendor selling the counterfeit components moved out of their facilities and left no forwarding address once they were identified as a counterfeit supplier.

Improvements in detection methods evident from GIDEP Data

NDAA section 818 called for greater testing of existing component stocks and all those acquired from non-OEM or unauthorized distributors. This increased testing was evident in the 2012 and 2013 GIDEP data reviewed. See Figure 2. The most common methods utilized were Visual Inspection and Resistance to Solvents. Of the 120 cases reviewed in this study 77% of the counterfeits were detected by multiple methods. The increased numbers of counterfeit identification tools are also thought to account for some of the reductions in reported cases. Detailed review of the cases showed that in about 6 cases the parts were tested by only one method and were found to be counterfeit, yet it is unlikely they were actually counterfeit (False Positives). These cases could not be confirmed as counterfeit because the company performing the testing destroys all the components once they are suspect. This prevents any further evaluation or testing. It would also hamper prosecution as the evidence is destroyed to prevent distribution.

GIDEP Data Shows Visual Inspection and Resistance to Solvents Main Detection Methods

Figure 2 shows the distribution of detection methods used in the GIDEP data under study. The two main methods accounting for a total of 50% of the detection cases was visual and resistance to solvents. These two methods also require no special equipment and are therefore the lowest cost testing options. One developmental measure proposed by (Beidel 2012, 1) would be for manufactures to embed the equivalent of unique DNA in every chip. This microchip

encoding would allow testing and verification of the parts without verification of chain of custody. This method has been utilized heavily by the government's Defense Logistics Agency (DLA). Another new method of counterfeit preventing reported is the use of a DTEK machine. This proprietary technology looks at the top of the component and compares the microscopic fingerprint to a library of known good components. This technology is non-destructive but does require access to known good parts to be effective. To date the Boeing Company and CBP have implemented this technology in their incoming inspection of purchased parts. Of all the 2012 and 2013 GIDEP reports reviewed for this report, none of the suspect components were detected using either the DTEK equipment or the unique DNA methods. Given the large number of parts screened to the low number of counterfeits, it is too early to tell if this new technology will be of value.

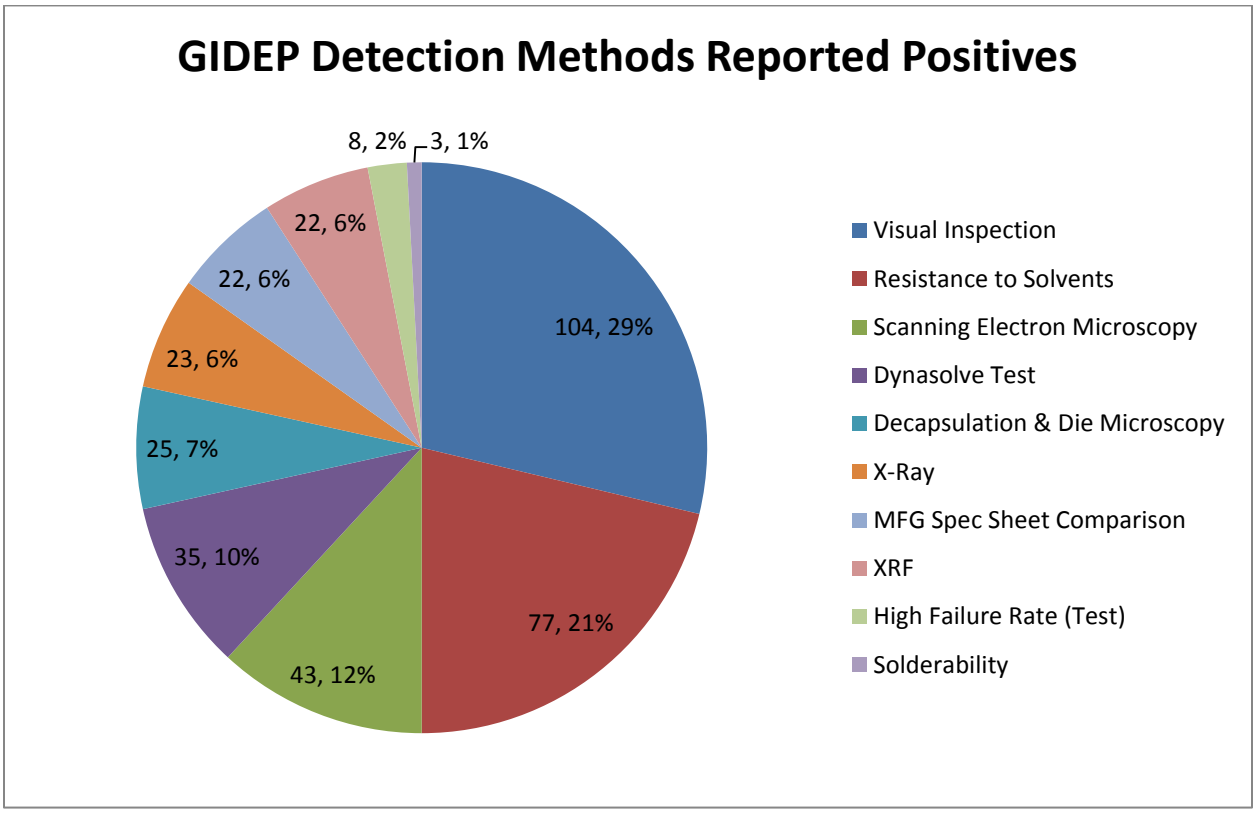

Figure 2

Military System Reliability Improving Along with Parts Obsolescence

Counterfeit electronics do affect overall military systems reliability and operational readiness. One DoD official in John Reed's article "*Fake Parts are Seeping Into Military Aircraft Maintenance Depots*" is quoted as estimating a "5 to 15 percent annual decrease in weapon systems reliability." (U.S. Department of Commerce 2010, 140) It is assessed that the 50% reduction trend in counterfeit cases identified in this study will continue. Fewer counterfeit parts in the overall supply chain should improve overall system reliability. It is proposed that parts obsolescence will increase as the commercial market continues to grow in relation to the military market. Previously identified issues like pure Tin components, plastic parts, and vented BGAs will pose increasing challenges for parts selection and availability. Decreased parts availability

will increase procurement cycle times and cost while increasing overall system down times. This can be mitigated by analysis and storage of spare part stocks.

Predictive Analysis - Reduction in Parts Brokers and Decreased Military Supply Base

On major concern is reduction in parts brokers and un-authorized distributors driven by the 2012 NDAA mandates. The 2012 NDAA mandates purchase from OEMs and authorized distributors effectively closing the door to brokers and independent distributors. The Commerce Department report recommended against using brokers and distributors, "The most widely suggested best practice to avoid purchasing counterfeits is to buy parts directly from OCMs and authorized distributors, rather than from parts brokers, independent distributors, or the grey market." (U.S. Department of Commerce 2010) Brokers and distributors can be utilized, but it requires additional and costly CEPA (Counterfeit Electronic Parts and Avoidance). The American Bar Associations' Task Force on Counterfeit Parts also identified the risk to the supply chain and proposes that, "…(OEMs, dealers/distributors, brokers, etc.), will find it no longer attractive, or economically feasible, to participate in the defense electronics supply chain." (Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law 2012, 12). Some companies provide commercial off the shelf products, but they now specifically exclude sales and support to military customers because they do not want to incur the liability associated with large military systems. According to the Commerce department the two major sources of counterfeit components are brokers and independent distributors, 84% and 42% respectively (U.S. Department of Commerce 2010, 115). So it follows that as counterfeit prevention rises, those part sources will start to dry up. All these indicators point to continued reduction in the number of military part suppliers.

The final blow to brokers may come from the growth in 4PL (4 tier Parts Logistics) suppliers. These suppliers work with large defense contractors to manage their supply chain. The 4PL does the procurement, inspection, warehousing, and kitting of all component parts. The defense contractor is then issued a complete kit of parts. This eliminates these functions in the defense prime contractor. The 4PL must still comply with all laws concerning counterfeit parts, but they are large enough to have procedures, training, and equipment to handle the task. This also somewhat mitigates the liability of the prime contractor. Major 4PL suppliers including distributors like Arrow, Avnet, and TTI now provide supply chain services to help clients deal with parts obsolescence (McHale 2000, 18&20). These systems have been proven to be cost effective when compared with other methods that address parts issues one at a time (McHale 2000, 18&20). They do have a negative effect in that they further reduce the number of companies in the supply chain and push out primarily the brokers and small distributors. Ultimately, the reduced number of suppliers will drive military parts shortages, resulting in higher demand and cost.

Higher Parts Cost Will Drive Higher Cost Throughout the Supply Chain – U.S. Gov. Pays

The NDAA of 2012 imposed significant additional requirements on the entire defense supply chain. With ultimate liability of system failures resting on any company creating or utilizing counterfeit components the companies will have to pass this increased liability on to its customers and the government or at least budget management reserve to cover the liability. In addition the cost associated with rework of counterfeit parts and the associated corrective and preventative actions (RCCA) are all considered unallowable cost (Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar

Association Section of Public Contract Law 2012, 8). Unallowable cost cannot be charged to the government contract and must be paid by the contractor directly out of profit. The cost to implementing a compliant counterfeit prevention system may be reimbursed by the government, but the specifics have not yet been defined. (Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law 2012, 10) A compliant system is costly and consists of training, documenting procedures, testing, process controls, and reporting requirements. The testing methods used to detect counterfeit electronic components have expanded and the cost of the equipment. A DTEK system license for example runs about $20,000 per year. Real time x-ray equipment can easily cost in the range of $300,000. The depreciation of these assets will be spread over all the government contracts. Costs are also higher to report counterfeit and suspect counterfeit electronics. Reporting has been mandated, but the costs are just now being assessed on each weapons system. These costs are more easily borne by larger corporations, and smaller brokers and distributors will find it hard to comply further driving their exodus from the supply chain. Ultimately all costs will be passed on and will increase the total system price to the government.

Some of these costs haven't hit the top line yet. While it is hard to assess, there is some indication that companies have not yet built the counterfeit prevent cost into their proposals. For example: one extremely costly measure is to purchase the original manufacturing dies and to have the parts manufactured by companies specializing in obsolete remanufacturing (McHale 2000, 20) (Edwards 2009, 41). This type of cost will significantly increase as commercial parts either do not comply or no longer exist.

Proposed Legislation if Enacted Would Directly Reduce Military Supplier Profitability

There is a proposal before Congress to identify as counterfeit any component that has a high failure rate. In fact, the definition of what constitutes counterfeit goods is still somewhat in question. The 2012 NDAA does not provide a clear legal definition of counterfeit (Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law 2012, 14). The following is the definition provided by the Department of Commerce:

- "is an unauthorized copy;
- does not conform to original OCM design, model, and/or performance standards;
- is not produced by the OCM or is produced by unauthorized contractors;
- is an off-specification, defective, or used OCM product sold as "new" or working ; or
- has incorrect or false markings and/or documentation." (U.S. Department of Commerce 2010, 3)

Bullet four includes defective components in the list of counterfeit components. This is an issue as defective components impact manufacturing cost by as much as 12%. This includes the material and labor cost to replace the defective component and the subsequent retesting. Congress currently is evaluating whether defective components should be included in the definition and should be treated as such. If this were to become law the cost at all levels of production would be high since it is common for components to have a certain amount of normal mortality usually between 1% and 5%. Classifying normal failures as counterfeit would result in fewer parts, increased false positive reporting, and most certainly higher cost. These costs would initially hit a company's profit line, only to be eventually budgeted into future proposals. Other ramifications would be increased cost of acquiring the parts and a forced 100% testing of all components prior to use. This would add significantly to the cost of the overall system and

would do little to improve reliability as most systems are functionally tested prior to use. Marginal design failures would also potentially trigger counterfeit prevention measure resulting in complete removal of all suspect components due to a few off nominal failures. It is recommended that component failure issues be segregated from issues dealing with counterfeit goods made by other than the original equipment manufacturers (OEM).

Assessed Vulnerability to Cyber Attack is Low but Recommend Continued Vigilance

Based on zero reported cases and no findings in the data reviewed, it is assessed that the vulnerability to cyber attack from China or any other country through counterfeit electronic component parts is extremely low. Components especially complex components like CPUs and memory should still be tested using de-lidding to look for differences in die structure that might indicate malicious code. It is also recommended that at least a small number of counterfeit components be retained after detection for the purposes of further investigation and prosecution of the counterfeiters.

Summary of Findings Shows Significant Drop in Counterfeiting and Increased Cost

The number of counterfeit cases is dropping due to changes driven by the 2012 NDAA. The drop in reported GIDEP cases of 50% is significant as better reporting is also now in place. China continues to be the most likely source of counterfeit electronics. Improved testing methods have provided greater visibility to counterfeit components and many new methods are on the horizon. It is also significant that no indication was found to indicate that components have been counterfeited with the intention to commit cyber attacks. This still requires close scrutiny because it is hard to detect such a device and the implications of a successful attack would be grave. The mandated and voluntary changes implemented by the industry to prevent counterfeit electronics will improve system quality and reliability, but unfortunately at a cost. The cost of the new processes, training, equipment, and potential liability will all have to be passed on to the government through higher prices. These increases especially liability will drive many smaller brokers and vendors from the military arena. This move away from military manufacturing to commercial was the main historic driver of the growth in part obsolescence and higher component prices. This trend will continue and issues such as Lead free, plastic parts, vented BGAs, and other commercial driven processes will limit and complicate the procurement of military electronics. It is also assessed that if Congress mandates that all component failures be treated as a counterfeit, then the cost of this increased reporting and handling will add as much as 12% to the cost of manufacturing. The total price tag for military systems and platforms will be affected as all these higher cost flow up. The final assessment is that military and civilian leadership will find it increasingly difficult to balance lower defense budgets and mandated sequestration cuts to the increasing cost of military systems thus requiring careful consideration and selection of military systems to match national security goals.

Future Research Should Link CPB Efforts

One area of future research would be to evaluate Customs and Border Protection's (CPB's) data on interdiction of counterfeit electronics components entering the country. This may represent a significant factor in the apparent reduction in counterfeit cases as found in this report. The data provided by CPB would also help in identifying with some certainty the source of counterfeit electronics. CPB was contacted, but at the time of this writing, the specific data requested was not available.

Credits

I would like to thank Dr. Valero for his encouragement and editing of the final product of this report. Recognition is also given to Christina Wang for her assistance with the Boeing counterfeit prevention process and knowledge of the GIDEP system. Finally I would like to thank my wife, Eva Sassenfeld, for her editing skills on this and all my papers.

Appendix A

Government-Industry Data Exchange Program (GIDEP)

– Controlled Data Distribution Requirements

While this report utilizes as its primary source GIDEP data, only summary data has been provided and the database generated of specific GIDEP reports has not been provided in this report. Release of the spreadsheet with detailed data would require approval of the GIDEP program manager. The following specifics were taken from GIDEP Publication 1:

> "1.3.3 Limitation of Data. Data and documents downloaded from GIDEP are controlled distribution and shall not be shared with companies outside the continental United States and Canada. Distribution of GIDEP data is controlled under the Foreign Technology Transfer Act.
>
> Access to the GIDEP databases and sharing of program data is restricted to United States and Canadian governments and government contractors, as prescribed in the GIDEP Operations Manual, and a Memorandum of Agreement. Access by other nationals and foreign contractors operating outside Canada and the United States requires approval of the US Department of State and the DoD Office of Technology Transfer.
>
> Requests for exceptions to the restriction will be sent to the Program Manager, Office of the Deputy Undersecretary of Defense, Supply Chain Integration, with a copy to the GIDEP Operations Center. The Program Manager will process the request for exception to the restrictions and directly advise the requester of the approval or rejection of the request." (GIDEP 2008)

Examples of redacted GIDEP reports are available in the Commerce Department Report. (U.S. Department of Commerce 2010)

Bibliography

Adams, Brigadier General John. "Remaking American Security - Supply Chain Vulnerabilities & National Security Risks Across the U.S. Defense Industrial Base." Alliance for American Manufacturing, 2013, 336.

Baljko, Jennifer. "The anti-counterfeit movement: Is it really a movement yet?" *Electronic Design News* (Canon Communications), May 2013: 22-24.

Beidel, Eric. "Plant Dna May Protect Military Supply Chain." *National Defense*, March 2012: 38-39.

Burgess, R. R., J. C. Marcario, O. Kreisher, and M. Scully. "Legislation Being Drafted To Address Problem of Counterfeit Military Parts." *Sea Power*, 2011: 6-9.

Capaccio, T. "China Top Source of Counterfeit U.S. Military Electronics." *Bloomberg.* May 22, 2012.

Cheng, Dean, and Derek Scissors. "China and Cybersecurity: Trojan Chips and U.S.-Chinese Relations." *The Heritage Foundation.* May 5, 2011. http://www.heritage.org/research/reports/2011/05/china-and-cyber-security-trojan-chips-and-us-chinese-relations (accessed September 15, 2013).

Department of Defense. "Instruction Number 4140.67." April 26, 2013.

Department of the Air Force - Office of the Deputy General Counsel. "Memorandum in support of the suspension of: Hong Dark..." *Eaton.* January 13, 2012. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&cad=rja&ved=0CDAQFjAB&url=http%3A%2F%2Fwww.eaton.com%2Fecm%2Fidcplg%3FIdcService%3DGET_FILE%26allowInterrupt%3D1%26RevisionSelectionMethod%3DLatestReleased%26noSaveAs%3D0%26Rendition%3DP (accessed November 2, 2013).

Edwards, C. C. "Past the sell-by date." *Engineering & Technology (17509637)* 4, no. 14 (2009): 40-41.

Electronics Weekly. Reed Business Information Ltd., June 27, 2012.

GIDEP. "Publication 1." *GIDEP.* April 2008. http://www.gidep.org/about/opmanual/appen-e.pdf (accessed November 3, 2013).

Matties, Barry. "The China Trap." *SMT Magazine*, April 2012: 88-93.

McGrath, Dylan. "Counterfeit chip reports maintain record pace." *Electronic Engineering Times*, October 2012: 10.

McHale, J. "Design engineers look to electronics distributors for value-added COTS." *Military & Aerospace Electronics*, December 1, 2000: 18.

Pecht, M. G., and D. Humphrey. "Addressing Obsolescence—The Uprating Option." *IEEE Transactions On Components & Packaging Technologies*, 2008: 741-745.

Sandborn, P. "Trapped on Technology's Trailing Edge." *IEEE Spectrum*, 2008: 43-58.

Senate Armed Services Committee - 112th Congress. *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain.* Committee on Armed Services - United States Senate, U.S. Government Printing Office, 2012, 74.

Spiegel, R. "Counterfeiting continues to grow, but the industry fights back." *Electronic Design News*, 2011: 51.

Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law. "White Paper regarding Department of Defense Implementation of Section 818 of the 2012 National Defense Authorization Act for Fiscal Year 2012." 2012, 43.

Tonelson, Alan. "Economic Watch: U.S. must stop using China's fake military parts." *The Washington Times*, May 30, 2012: 10.

U.S. Department of Commerce. *Defense Industrial Base Assessment: Counterfeit Electronics.* Bureau of Industry and Security, 2010, 243.

U.S. Department of Justice. "Administrator of VisionTech Components, LLC Sentenced To 38 Months in Prison For Her Role in Sales of Counterfeit Integrated Circuits Destined to U.S. Military and Other Industries." *Press Release.* District of Columbia, October 25, 2011.