March 2016

UNREGULATED E-WASTE EXPORTS FUEL COUNTERFEIT ELECTRONICS THAT UNDERMINE U.S. NATIONAL SECURITY

Restricting Export of Untested, Nonworking Used Electronics from United States Should be Key Element in Comprehensive Strategy

U.S. national security faces a grave threat from counterfeit electronics that have flooded the supply chains of defense contractors, according to a 2012 report by the Senate Armed Services Committee.[1] Many of these counterfeits are used parts – culled from e-waste smuggled into China from the United States and other countries – made to look new and be sold as new.

The committee identified about 1,800 cases of suspected counterfeits in weapons and equipment, including thermal weapons sights delivered to the Army and the control systems for missile systems, military aircraft and helicopters. These counterfeit parts create serious concerns about the reliability of defense systems – and risks for military men and women who must rely on sophisticated electronic equipment. The report notes that with counterfeit chips "there is no way to predict how well they will perform, how long they will last, and the full impact of failure."

"We do not want a $12 million missile defense interceptor's reliability compromised by a $2 counterfeit part," said General Patrick O'Reilly, Director of the U.S. Missile Defense Agency.[2]

For instance, the U.S. Air Force C-130J and C27J military cargo planes are equipped with display units that provide updates on engine status, fuel use, and location, as well as warning messages. Failure could cause the display unit to go blank, lose data, or show a degraded image. The committee found evidence that the units were counterfeit, creating grave risks for military personnel. The committee ultimately traced the units' suspected counterfeit chips to Shenzhen, China.

E-Waste Exports:
The Raw Materials for Counterfeiters

In more than 70 percent of the cases, the committee traced the counterfeit parts to China. The report notes that "much of the material used to make counterfeit electronic parts is electronic waste, or e-waste, shipped from the United States and the rest of the world to China."

> *"Much of the material used to make counterfeit parts is electronic waste, or e-waste, shipped from the United States and the rest of the world to China."*
> *-- Senate Armed Services Committee*

Today there is no national policy regulating e-waste exports to China. *Current U.S. policy actually encourages e-waste exports that help counterfeiters thrive.*

E-waste is shipped from the United States by brokers/exporters. The used electronics are often collected under the guise that they will be responsibly recycled domestically. However, the goods are just "packed and stacked" into shipping containers and exported to developing countries where laws protecting the environment and public health are nonexistent or not enforced. Broker/exporters often claim to provide data erasure, though they typically lack capabilities to reliably do so. As a result, the export of unsanitized data-bearing technology to developing countries is a persistent source of data breaches, identity theft, and cyber crime – including documented cases involving sensitive military issues.

> "Over the past two years alone, more than one million suspect parts have associated with the known supply chain." – DARPA, Feb. 24, 2014

China remains the world's largest importer of e-waste despite a ban it enacted in 2000.[4] An estimated eight million tons of e-waste are imported illegally into China each year, providing a ready supply for counterfeiters. The illicit e-waste trade is among the leading types of transnational organized crime in Asia and the East Pacific – a black market industry valued at $3.75 billion in East Asia alone, according to a 2013 United Nations study.[5]

Smuggled e-waste typically goes through Hong Kong. As China has made some attempts at interdiction, alternate smuggling routes have emerged through Vietnam and North Korea.[6] In January 2014, Chinese authorities arrested smuggling rings when more than 500 agents arrested 54 suspected smugglers.[7] The rings are suspected of importing nearly 80,000 tons of used laptops and computer parts into China.[8] The UN report notes that "the main smuggling methods used for shipping containers of e-waste are concealment and misdeclaration."

E-waste is shipped by truck to China's Guangdong Province, where most counterfeiting activities take place.[9] As described in the Armed Services Committee report, the e-waste is disassembled by hand in backyards and dump sites. The equipment is heated over open fires to loosen and separate components. The parts are then washed in a river or left outside to be cleansed by monsoon rains, and then dried on sidewalks and river banks.

Large factories employing 10,000 to 15,000 people are set up for counterfeiting, according to the Senate report:

> "Parts may be sanded down to remove the existing part number and other marks that indicate a part's quality in performance. In a process known as 'black topping,' the tops of the parts may be recoated to hide sanding marks. State-of-the-art printing equipment may be used to put false markings on the parts. Once they have been through the counterfeiting process, the parts are packaged and shipped to Shenzhen… or other cities to be sold in markets or over the Internet. From there, the parts enter the U.S. defense supply chain where they can compromise performance and reliability, endanger the safety of military personnel and open vulnerabilities in U.S. defenses."

Based on the Armed Services Committee's work, anti-counterfeiting measures were included in the 2012 National Defense Authorization Act. The measures were designed to address weaknesses in the defense supply chain and promote counterfeit avoidance practices.

However, serious problems continue. According to a Feb. 24, 2014 news release by the Defense Advanced Research Projects Agency (DARPA), "Used and non-authentic counterfeit electronic components are widespread throughout the defense supply chain; over the past two years alone, more than one million suspect parts have been associated with the known supply chain."[10]

E-Waste Export Restrictions: The Missing Piece of a Comprehensive Strategy

While improving supply chains and detecting counterfeit microchips are critical, to date there has been little focus on attacking the problem at its source – by reducing the flow of raw materials culled from e-waste.

The Secure E-Waste Export and Recycling Act (SEERA) is a bill to control the export of electronic waste (e-waste) in order to ensure that such waste does not become the source of counterfeit goods that may reenter military and civilian electronics supply chains in the United States. SEERA would amend existing Export Administration Regulations by designating non-working/non-tested used electronic items (based on a list of common electronic products or fragments of products that contain circuitry) as "Electronic Waste" which cannot be exported outside of the U.S. unless certain specific conditions are met.

SEERA is consistent with historic U.S. practices of restricting exports that pose a threat to national security.

This approach would stop the flow of e-waste from the United States that is undermining our national security. SEERA will require domestic recycling of all untested, nonworking electronics. By keeping these materials in the United States, we will keep them out the hands of counterfeiters and data thieves. Under SEERA, export of tested, working equipment will continue and is expected to grow, creating up to 42,000 good-paying jobs for Americans.[11]

The United States has historically restricted export of products and information that pose a threat to national security. SEERA is consistent with this approach. Given the role of e-waste in fueling counterfeit electronics and creating security threats, it is simply common sense to regulate exports of these materials.

About the Coalition for American Electronics Recycling

The Coalition for American Electronics Recycling is the voice of the emerging e-waste recycling industry on Capitol Hill. Since its formation in November 2011 with a handful of members, CAER now includes more than 130 companies and supporting members operating more than 280 facilities in 35 states and Puerto Rico and the District of Columbia. Visit the CAER website for a complete member list.

Sources:

1 "Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain," Committee on Armed Services, United States Senate, May 21, 2012. Download available here.

2 Armed Services Committee report, page i

3 "Did IAF's 'US-made' C-130J Super Hercules that crashed have fake Chinese parts?" Times of India, March 30, 2014.

4 "Eight Million Tons of Illegal E-waste Is Smuggled Into China Each Year," Smithsonian, Feb. 28, 2014.

5 "Transnational Organized Crime in East Asia and the Pacific: A Threat Assessment," United Nations Office on Drugs and Crime, April 2013.

6 "Did North Korea Recycle Your Laptop?" Bloomberg.com, March 6, 2014.

7 "Why China is still the dumping ground for the world's electronic refuse," Quartz, Feb. 27, 2014

8 "E-waste bust in China has U.S. connections," E-Scrap News, March 7, 2014.

9 Armed Services Committee report, page 5 – 6

10 Tiny, Cheap, Foolproof: Seeking new component to counter counterfeit electronics," DARPA news release, Feb. 24, 2014.

11 "Jobs Through Electronics Recycling," DSM Environmental Services, Inc. for the Coalition for American Electronics Recycling, January 2013.

12 "China loses trade dispute over rare earth exports," Reuters, March 26, 2014.