THE HILL

Counterfeit electronics: Another security threat from China

BY TOM SHARPE - 07/05/15 02:00 PM EDT 6

The Hill's July 2 story "FBI: Chinese malware possibly behind OPM hack" is the latest revelation about cyberattacks from China. Unfortunately, cyberattacks are not the only technology-based security risk coming from China. We must also address the issue of counterfeit electronics.

China is also the primary source of counterfeit electronics that threaten the reliability of military hardware and our critical infrastructure for telecommunications, energy and transportation. A study by the Senate Armed Services Committee found more than 1,800 cases of suspected counterfeits in advanced missile systems, helicopters, submarines and more. Because our company provides counterfeit detection services and parts to Department of Defense agencies, we participated in the study.

Why are counterfeits a problem? Today's defense technologies require sensitive electronic components assembled in ultra-clean room environments; a foreign object smaller than a flake of dandruff can compromise reliability within a single device. The counterfeiting process provides a stark contrast.

On a business trip to China several years ago, I had an unforeseen opportunity to get a first-hand look at the epicenter of the counterfeit manufacturing industry in Guangdong Province. The counterfeiters start with electronic waste (e-waste) — old, discarded computers from the U.S. and other countries — and remove the used electronic components.

E-waste is dismantled by hand in open-air dumps or in backyards. Workers heat components to "reflow" solder attaching them to circuit boards, making it easy to quickly remove with hand tools. After this crude process, parts are washed in rivers and laid out on sidewalks for sorting.

From there, the parts are transported to hundreds of local counterfeiting operations that employ thousands of workers. To hide brand marking and model numbers, parts are sanded or put through an acid wash, then re-coated – a process known as "blacktopping."

This process exposes these highly sensitive chips to moisture, static electricity and other damaging conditions. Acid baths used in some remarking processes can eat away at a microchip's internal parts.

Counterfeiting processes constantly improve, so it is nearly impossible for even a trained eye to detect the better ones without significant testing capabilities. Yet these components can be found everywhere, including highly sophisticated technologies that protect our war fighters and keep critical infrastructure up and running across our country.

Unfortunately, American citizens and businesses are unwittingly complicit in this illicit trade. Because of loopholes in our export policies, much of the e-scrap that counterfeiters use as feedstock comes from our shores. As the Armed Services Committee report found, “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.”

Unethical e-scrap companies and brokers here in the U.S. may promise responsible recycling — then ship broken computers to China in huge volumes. Our discarded, non-working electronics are a cheap source of raw materials. It is a very lucrative trade for the bad guys.

The famous line from Pogo applies to this issue. By allowing unchecked exports of untested, non-working electronics use by counterfeiters, we are undermining our national security. Efforts to prevent fake chips from getting into supply chains have done little to stop the counterfeiters. While prevention and detection measures are important, we believe we must also choke off a huge portion of the counterfeiters’ feedstock: the massive e-waste exports from the U.S.

To accomplish this, Congress must go on the offensive by requiring domestic recycling of untested, nonworking electronics. By keeping these materials in the United States, we will keep them out of the hands of counterfeiters. There already exists a strong core of responsible American recyclers across the country that use highly secure, controlled and scalable recycling processes that can easily get the job done while creating thousands of new jobs simultaneously.

Our trade laws typically prevent exports of materials and services that may be detrimental to our national security and foreign policy. We need Congress to combat counterfeits by requiring amendments to our export policies as an essential step to protecting our military men and women, our national defense and our homeland security.

Sharpe is vice president of SMT Corp., an electronics distributor and counterfeit mitigation laboratory for the defense and aerospace industries