

# Technologies for Counterfeit/Clone Mitigation

---

Kerry Bernstein

US Government Consultant

[Kerry.bernstein.ctr@mail.mil](mailto:Kerry.bernstein.ctr@mail.mil)

703-746-1426

DHS/GMU Workshop

21 August, 2020



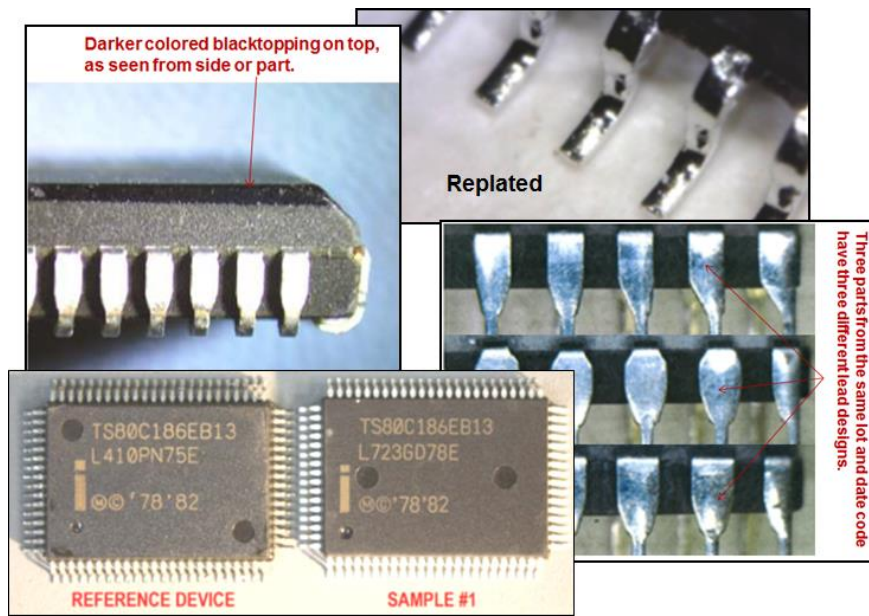


# Electronic Counterfeits vs Clones

## Counterfeits

*Still the original part from OEM:*

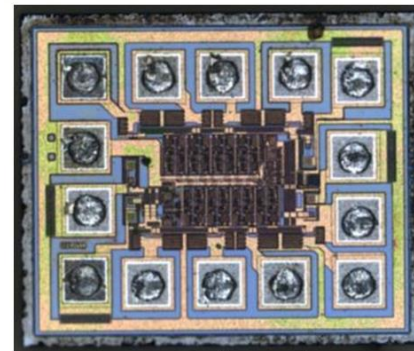
- Recycled used components
- OEM's fab test failures sold on black market.
- Unlicensed fab overproduction



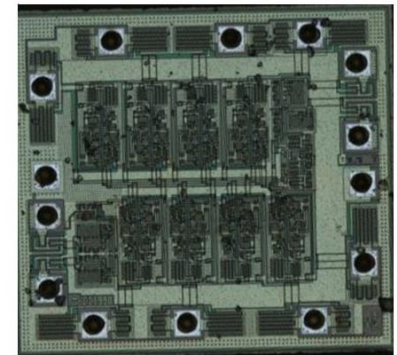
## Clones

*A completely different part:*

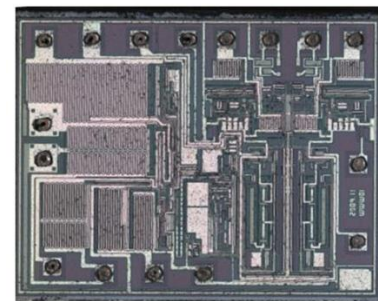
- Copies fabbed in foreign plant
- New design of reverse-engineered components using stolen IP, potentially with altered function



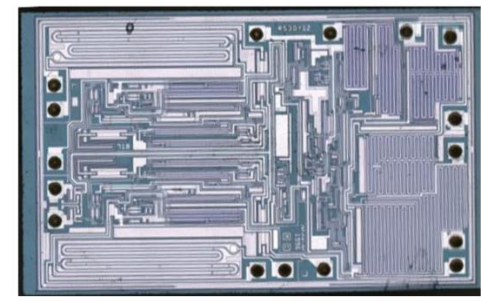
Suspect



Good



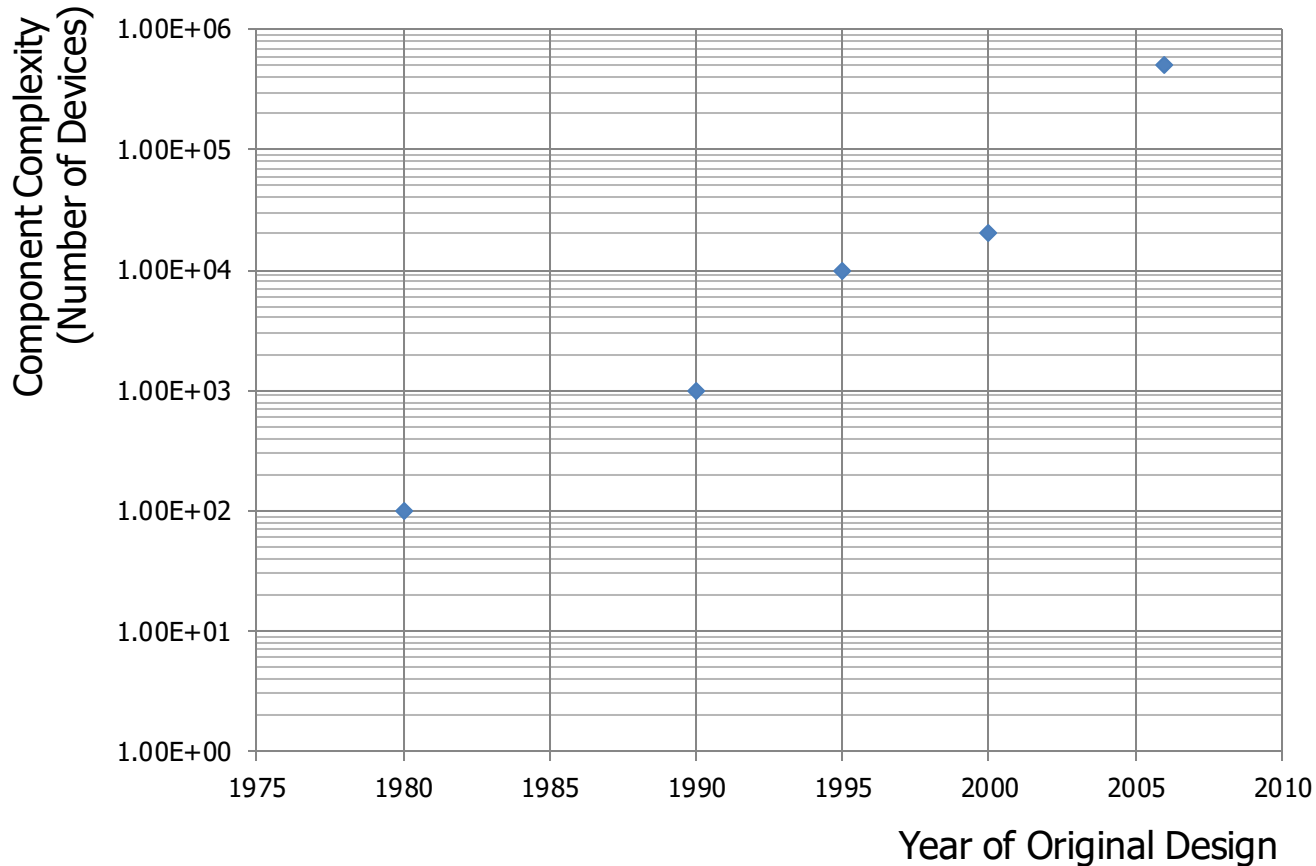
Suspect



Good



# Growing National Security Exposure

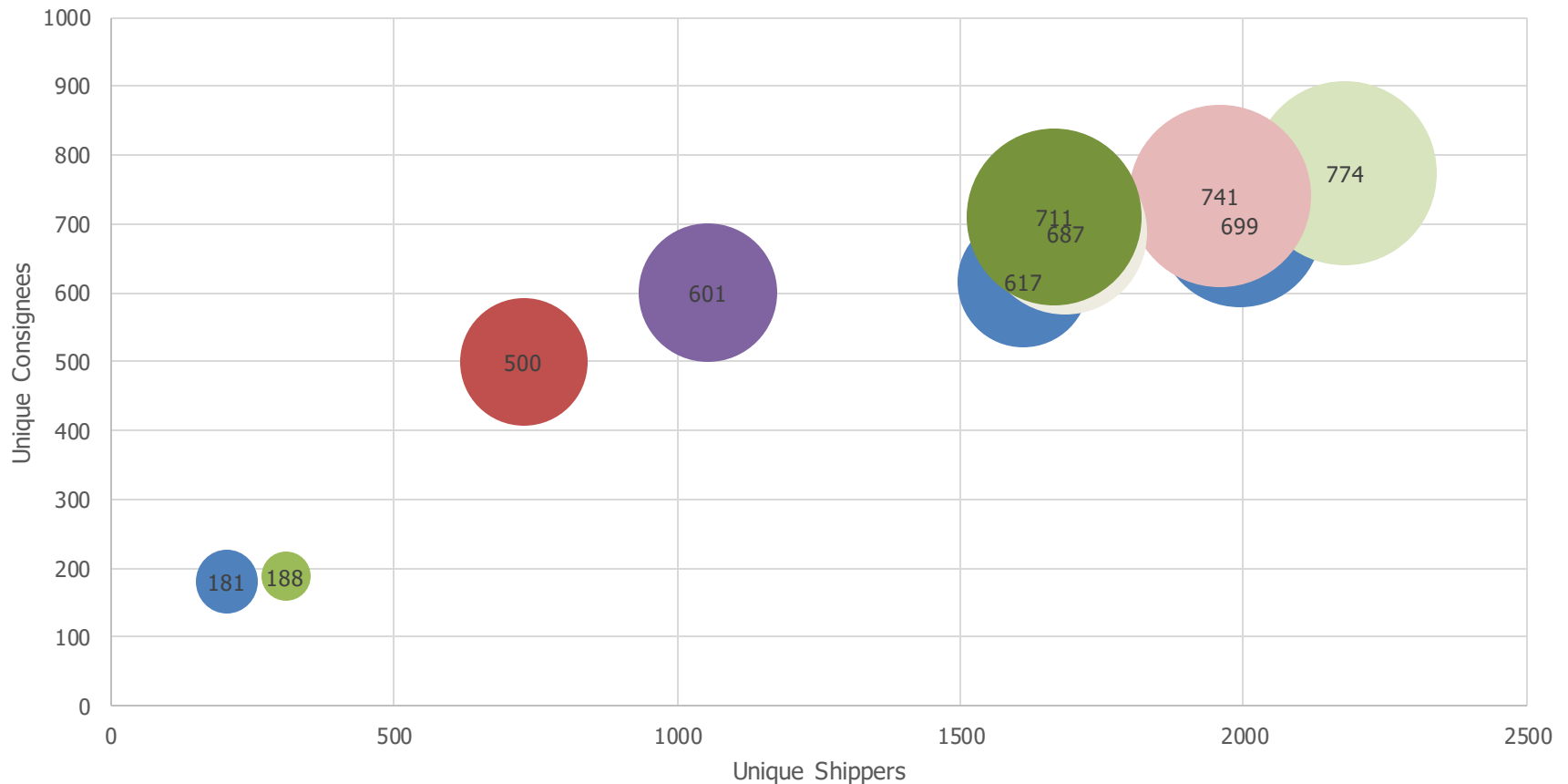


- Plot of selected counterfeit parts discovered in the DoD supply chain over past 2 years
- Evidence of growing capability in counterfeiting more complex components

Distribution A, Approved for Unlimited Distribution



# CBP Data for Specific Shipments\*

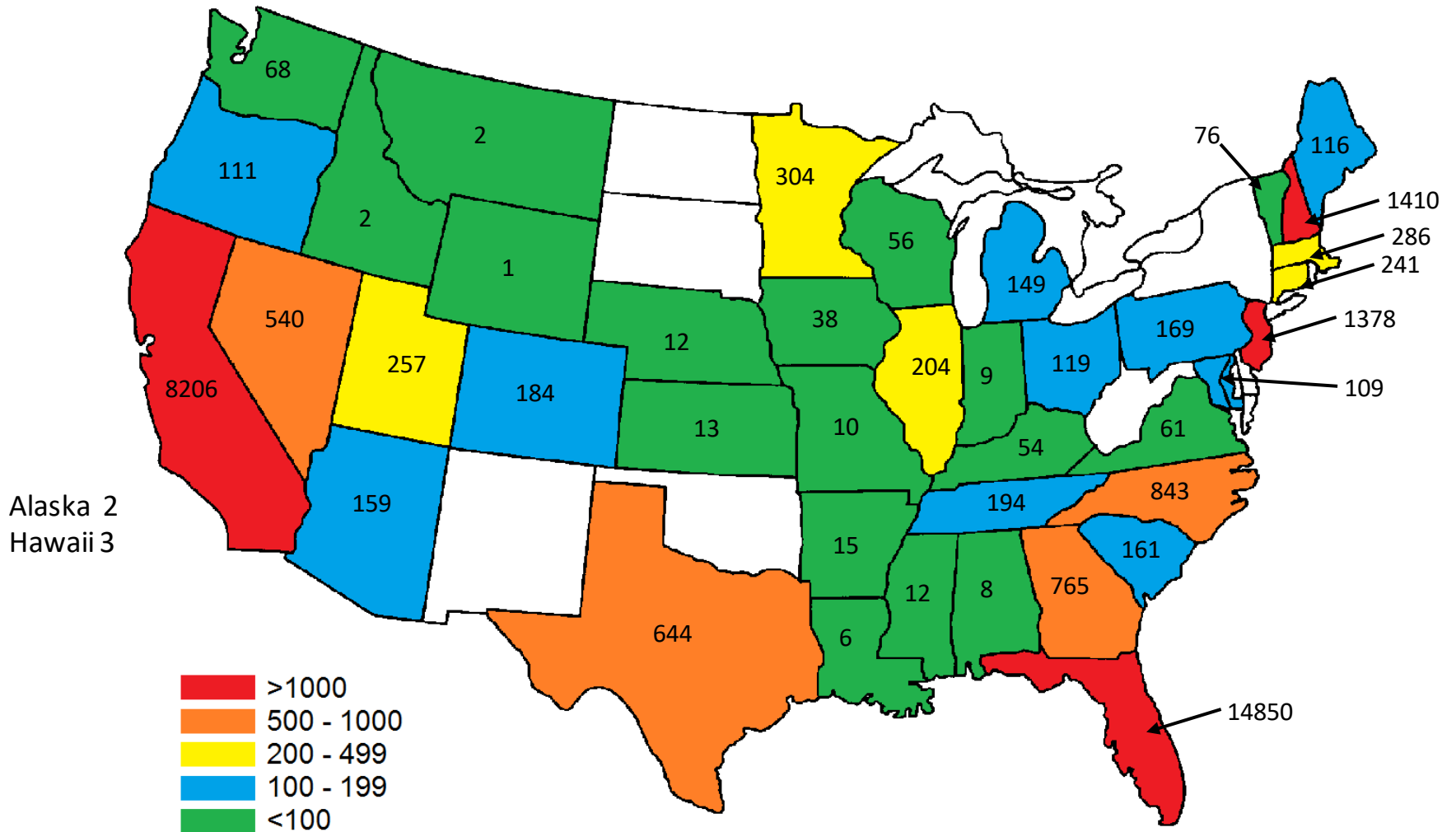


- Top 90<sup>th</sup> percentile of Chinese, Hong Kong Counterfeit Exporters to US
- 1999-2013 Operations (data being updated to 4Q2016)

\* Data courtesy of Adam Hauch, DSS  
Compilation by Kyle Bunch, Arnett Brown, Kerry Bernstein



# Counterfeit Destinations by State 2003-2013



\* Data courtesy of Adam Hauch, DSS  
Compilation by Kyle Bunch, Arnett Brown, Kerry Bernstein



# SHIELD: The DARPA Supply Chain Solution

HW Root-of-Trust  
Fragile Key Storage

Full Encryption Engine

Unpowered  
Passive Sensors

Inductive Powering  
and Communication

**Microscopic  
SHIELD dielet  
inserted in pkg**

**SHIELD Target Spec**

- **100 $\mu$ m x 100 $\mu$ m (0.01 mm<sup>2</sup> Area)**
- **100K Devices**
- **100 MHz Clock Rate**
- **50  $\mu$ W Total Power**
- **T  $\leq$  120 $^{\circ}$ C**
- **32nm CMOS**
- **4 Levels Metal**
- **3.7 $\mu$ m thinned sub**
- **<0.8 $\cent$  per dielet**

**DARPA SHIELD will develop the ability to provide:**

- **100% assurance against certain known threat modes;**
- **quickly, on demand, at any step of the supply chain; and**
- **essentially for *free*.**

**SHIELD makes counterfeiting too expensive and too hard to do.**



## Fab of Origin (ClearMark, Chromologic, IC Forensics)

- Fab-of-Origin looks for fab-signatures to identify origin of a component
- Idiosyncrasies associated with fab-specific tooling, recipe, sequence
- Needed to trace DoD, non-DoD clones and counterfeits to originating foundry (Smart Grid, Cyber Systems, Communications, etc...)

### **MTO SBIR SB133-03: Fab of Origin**

**Was it made HERE?**



**Or HERE?**

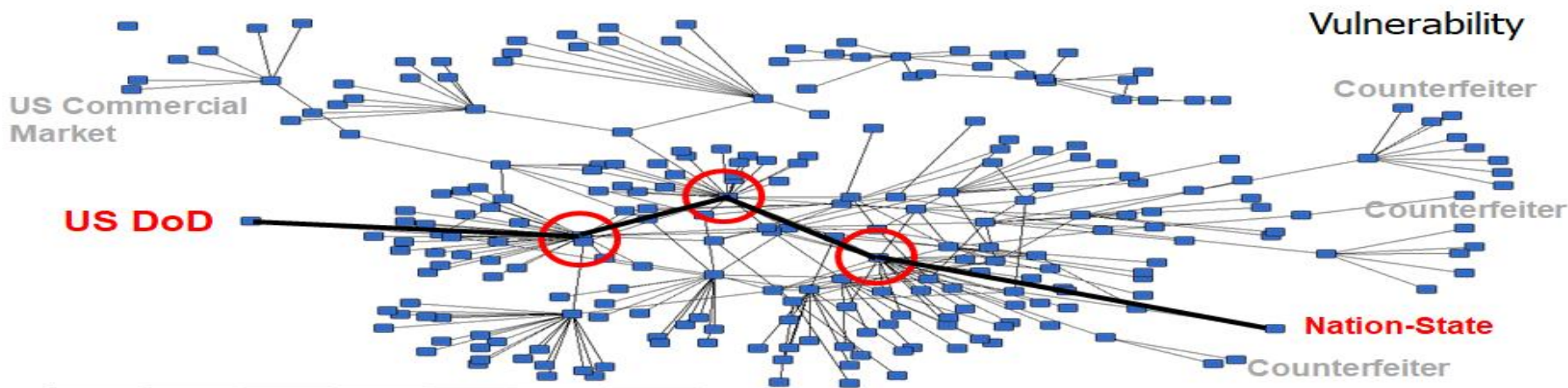
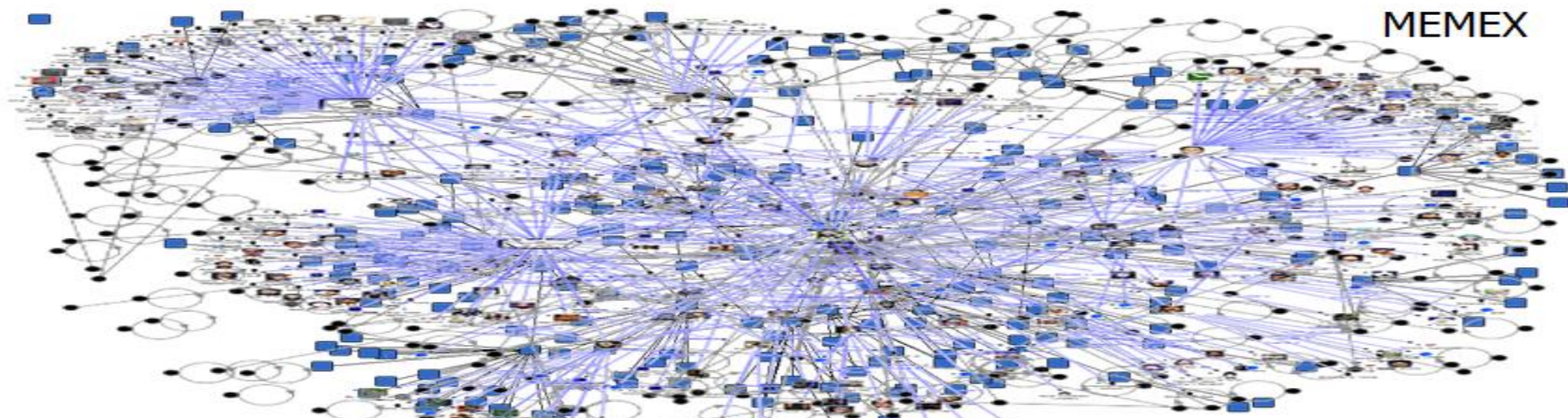


**Once SHIELD determines a chip to be a counterfeit, Fab-of-Origin will provide the insight needed to identify where it was made.**





# MEMEX-derived Global Counterfeit Network



US Commercial Market

Distributors

Counterfeiters

DoD Program Acquisitions

Targeted IC Collections





U.S. Department of Justice

United States Attorney  
District of Connecticut

Connecticut Financial Center (203) 821-3700  
157 Church Street Fax (203) 773-5376  
New Haven, Connecticut 06510 www.justice.gov/usao/ct

**FOR IMMEDIATE RELEASE**  
**December 10, 2015**

**CONTACT:** Tom Carson  
Public Information Office  
(203) 821-3722  
(203) 996-1393 (cell)

**THREE CHINESE NATIONALS ARRESTED FOR BRAZEN SCHEME  
TO STEAL AND ILLEGALLY EXPORT  
MILITARY-GRADE SEMICONDUCTORS**

Deirdre M. Daly, United States Attorney for the District of Connecticut, today announce that DAOFU ZHANG, 50; JIANG GUANGHOU YAN, also known as “Ben,” 33; and XIANFENG ZUO, 37, all Chinese nationals, have been arrested on federal criminal complaints in connection with a brazen scheme to obtain and illegally export sophisticated semiconductors stolen from the U.S. military. ZHANG, YAN, and ZUO were arrested this morning in Milford, and all three made initial appearances before U.S. Magistrate Judge Sarah A.L. Merriam in New Haven, Connecticut.

As alleged in the criminal complaints, federal law enforcement agents began investigating YAN and a Chinese company known as HK Potential in 2012 for trafficking in counterfeit semiconductors. In October 2014 and in March 2015, YAN sold a total of forty-five counterfeit Intel microprocessors to an undercover agent, who had advised YAN that the components would be used on a U.S. Navy contract involving submarines.

In July 2015, YAN asked whether the undercover agent could obtain twenty-two Xilinx semiconductors, military grade, for which YAN would pay \$37,000 each. After the undercover

**Chinese nationals arrested in Milford for stealing military parts**

