REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE ***(DD-MM-YYYY)***	**2. REPORT TYPE**	**3. DATES COVERED** ***(From - To)***
08-06-2018	Final	

4. TITLE AND SUBTITLE
Trusted and Assured Microelectronics: Technological Challenges, Bureaucratic Conundrums, & Foundational Dilemmas Facing Technology in National Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lt Col Erik G. Brine

Advisor: Dr. Hayat Alvi

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Ethics and Emerging Military Technology (EEMT) Program
U.S. Naval War College
686 Cushing Road, Newport, RI 02841

8. PERFORMING ORGANIZATION REPORT

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES: **A paper s**ubmitted to the Faculty of the U.S. Naval War College in partial satisfaction of the requirements of the Ethics and Emerging Military Technology Graduate Certificate Program. The contents of this paper reflect my personal views and are not necessarily endorsed by the U.S. Naval War College or Department of Defense.

14. ABSTRACT: Microelectronics have become ubiquitous in our everyday personal and professional lives. They are the subcomponents in the supply chain embedded in every piece of electronic technology we rely on from the smartphone, tablet, laptop, or desktop computer to the MRI equipment, pacemaker, bank ATM, and any vehicle on the market today. They are also the components DOD and all national security organizations rely on for GPS, weapon systems, communications equipment, and every vehicle in the inventory. While these microelectronics support technology that our lives, professions, and U.S. national security depend upon, they also actually create a tremendous risk. Extensive competition in the industry and incredible up-front investment costs have forced many companies out of business and the majority of manufacturing of microelectronics overseas. International competitors like China have committed to making large-scale investments with a goal of dominating the market. This presents a threat to DOD and all sectors of the economy that need to be concerned about the security of their equipment and data. The enormous challenge is presented in this paper as a set of nested challenges within DOD, within the U.S. Government, and throughout the national economy. In the same respect, recommendations are made to address the challenge at each of those levels, creating an a la carte menu of options that taken together represent a holistic approach to what is both a national security and economic problem.

15. SUBJECT TERMS
Trusted assured microelectronics, semiconductors, supply chain. dual-use technology, EEMT

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Ass. Dean-Electives & Research
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		47	**19b. TELEPHONE NUMBER** ***(include area code)*** 401-841-3556

U.S. NAVAL WAR COLLEGE
Newport, RI

Trusted and Assured Microelectronics: Technological Challenges, Bureaucratic Conundrums, and Foundational Dilemmas Facing Technology in National Security

Erik G. Brine, Lt Col, USAF

A paper submitted to the Faculty of the U.S. Naval War College in partial satisfaction of the requirements of the Ethics and Emerging Military Technology Graduate Certificate Program.

The contents of this paper reflect my personal views and are not necessarily endorsed by the U.S. Naval War College or Department of Defense.

8 June 2018

Contents

ABSTRACT

Microelectronics have become ubiquitous in our everyday personal and professional lives. They are the subcomponents in the supply chain embedded in every piece of electronic technology we rely on from the smartphone, tablet, laptop, or desktop computer to the MRI equipment, pacemaker, bank ATM, and any vehicle on the market today. They are also the components DOD and all national security organizations rely on for GPS, weapon systems, communications equipment, and every vehicle in the inventory. While these microelectronics support technology that our lives, professions, and U.S. national security depend upon, they also actually create a tremendous risk. Extensive competition in the industry and incredible up-front investment costs have forced many companies out of business and the majority of manufacturing of microelectronics overseas. International competitors like China have committed to making large-scale investments with a goal of dominating the market. This presents a threat to DOD and all sectors of the economy that need to be concerned about the security of their equipment and data. The enormous challenge is presented in this paper as a set of nested challenges within DOD, within the U.S. Government, and throughout the national economy. In the same respect, recommendations are made to address the challenge at each of those levels, creating an a la carte menu of options that taken together represent a holistic approach to what is both a national security and economic problem.

ACKNOWLEDGMENTS

I first must always thank my wife, Kerry, and my children Molly, Jackson, Lucy, and Dylan for supporting me through this additional academic endeavor at the Naval War College, while also managing the additional travel and time commitments of the National Command College this year. I'd also like to thank Dr. Tom Creely and Dr. Tim Schultz for their vision and perseverance in founding the Ethics and Emerging Military Technology (EEMT) graduate certificate program. The importance of understanding the roles and capabilities of new technology, much of which is dual-use, cannot be overstated when studying current and future national security issues. Thanks to both Dr. Hayat Alvi and Ms. Isabel Lopes for their expertise, advice, and guidance in completing this paper. I'd also like to thank Dr. Hank Brightman, EMC Chair, whose program funded my attendance of the Office of Naval Research's Naval Innovation Process Adaptation Pilot. Finally, I'd like to thank the National Command College, students, and staff, who made this year more enjoyable and memorable than my family or I could have imagined. I greatly appreciate the relationships I have made with some amazing professionals this year and look forward to relying on the advice of so many of them in the years to come.

Introduction

Microelectronics have become ubiquitous in our everyday personal and professional lives. They are the tiny parts of computers that exist in everything from a smartphone, to a laptop, to a vehicle, and now in many cases even a home thermostat or refrigerator. Microelectronics are in every military-owned computer or mobile device, radio, rocket, missile, sensor, satellite, and every type of driving, flying, or sea-faring vehicle in the inventory. In some cases, those microelectronics are commercial off the shelf (COTS) products any company would purchase for things like phones and laptops, but in others, they are specialized and highly advanced microelectronics manufactured specifically for weapons and systems. Regardless, there are significant security threats for each whether the product is COTS or advanced and specialized. Most people today understand that cyber threats exist for anything that connects to the internet, but what many fail to realize is that threats also exist in all electronic products from the design and manufacturing of microelectronics, and the process by which those microelectronics end up embedded in the products we use.

In one of the opening scenes of the 2015 techno-thriller *Ghost Fleet*, set in the not too distant future, Hawaii is under a surprise attack from China.[1] During the battle, a Marine aviator jumps in his F-35 in an attempt to do his part to defend fellow Americans and his airfield as the invading Chinese are decimating U.S. forces all across the island. Once airborne he successfully prosecutes a few targets, but then is engaged by an unmanned autonomous vehicle (UAV). This UAV should be no match for the world's most advanced fifth-generation fighter, but there's a problem. Despite greater

[1] Singer, P.W. and Cole, August, *Ghost War: A Novel of the Next World War* (New York: Houghton, Mifflin, Harcourt Publishing, 2015)

performance and overmatched systems, the F-35 cannot shake the drone and its unimpressive air-to-air missile, which eventually blows the F-35 out of the sky. The F-35's defensive systems were armed, the pilot executed the correct maneuvers to defeat the enemy missile, but it just kept coming, as if it were locked on to the stealthy aircraft in a way that shouldn't be possible. Embedded in each F-35 are well over a hundred subsystems all with cascading electronic supply chains touching all fifty states and nine original allied partners' countries. Somewhere, years ago during production, that supply chain was compromised. That Chinese drone triggered malicious code embedded deep within its target that triggered all antennae in the F-35 to simultaneously emit. Comparatively, if it were a heat-seeking missile, that F-35 would have looked like the sun. It never had a chance, but not because of poor pilot performance, or even aircraft performance, but because of sloppy security in the acquisition process many years ago and thousands of miles away.

This example is taken from a novel about a fictional battle, but the threat is real. The number of manufacturers of the most advanced microelectronic components has dwindled to only four large corporations due to fierce competition, globalization, and incredible infrastructure costs.[2] Simultaneously, China has committed to a strategic investment of more than $150 billion over 10 years to dominate and control this market.[3] Not only is the threat real, it is much larger and more multifaceted than the role of nefarious actors in the manufacturing process. In fact, the threats facing all national security institutions within the United States Government come from a dizzying

[2] Lapedus, Mark, "Foundry Challenges in 2018". Semiconductor Engineering, December 27, 2017. https://semiengineering.com/foundry-challenges-in-2018/.

[3] King, Ian, "China Has Big Plans for Home Grown Chips". Bloomberg, June 25, 2015, https://www.bloomberg.com/news/articles/2015-06-25/china-has-big-plans-for-homegrown-chips.

combination of foundational dilemmas, bureaucratic conundrums, and technical challenges. Each of these areas alone represents a difficult problem set to contend with for the Department of Defense or any national security institution, but together they seem insurmountable due to limitations of both resources and authority. Attacking this nested set of problems will require effective research and development programs, innovative policy decisions, collaborative interagency budgeting, and reimagining the roles of government, academia, and industry in technology areas like microelectronics manufacturing, where the capitalistic system built in the United States seems to be falling prey to more coordinated and prescriptive countries.

PART I – WHERE'S THE PROBLEM

The Department of Defense (DOD) and other national security agencies do not have all of the authority or capacity needed to address all of these problems alone, but they do have resources and capability at their disposal that can make a difference. Therefore, the Department of Defense must address the technical challenges with the resources and authorities it has, confront the bureaucratic conundrums to the best of their ability with interagency partners, and proactively seek assistance from Congress and the Administration on the foundational dilemmas around critical technology areas like trusted and assured microelectronics. This paper will identify these problems from the top down starting with the big picture national security, national economic, and ethical dilemmas, work through the interagency bureaucratic conundrums, and down to the technical challenges of access to trusted and assured microelectronics. Then, recommendations will be provided in the opposite order to build options for a course of action up from the

tactical level within the Department of Defense to the strategic, national-level effort that will be required to overcome some of the issues that lay ahead.

Foundational Dilemmas

Technology has democratized across the globe and permeated throughout the international community. Access to the internet and mobile computing have supported the sharing and stealing of intellectual property as well as the increasing pace of rapid improvement in technologies from one generation to the next. Globalization has upended previous supply chains and supported market efficiency by allowing larger market shares of some products to move to regions where manufacturing can be done at the lowest costs due to lower required wages, taxes, standards, and real estate costs. Simultaneously, technologies are increasingly dual-use, meaning they have both military and commercial applicability. In the past, some of the most integral military weapon systems like a tank or a tactical fighter aircraft had an obvious intended use and weapons manufacturer understood and expected that use. The weapon systems of today, be it a laptop computer, satellite, or unmanned aerial vehicle (UAV), not only offer the capability of greater possible destruction but also have easily as many commercial applications as they do military. Additionally, the manufacturer or developer may have never intended for their product to be used in malicious, destructive, or militaristic manner. The laptop computer can be used to hack into a command and control network or shut down a power grid, but is also needed for just about any business and is likely found in some capacity in nearly every home and business in America. Satellites are critically needed for weapons systems position, navigation, and timing (PNT) and secure military communications, but are also integral for every commercially available GPS service and satellite TV. Nearly

the same UAVs may be used to inspect power lines, spray insecticides on wheat fields, or deliver a package for Amazon in the near future, as could be used by state and non-state actors to collect intelligence or surgically deliver a lethal explosive. At the heart of, or at least in the brain of all of these technologies and so many more like them, are microelectronics.

Rapid advances and the melding of commercial and military technologies have created some real ethics based problems for technology companies. Many of these companies do not consider themselves part of the defense industry, but due to the capability and use of their products or services by DOD and adversaries alike, now must consider their impact on national security. Google has recently announced that it will not renew a contract that supports Project Maven with artificial intelligence capabilities due to employee backlash founded on the belief that Google's technology should not be used for unethical purposes like supporting drone strikes.[4] This, however, hasn't stopped Google from competing for DOD multi-million dollar cloud storage contract.[5] Does this ethical stand by 4,000 Google employees who signed a petition make sense? Surely, countless terrorists, drug dealers, thieves, and even foreign military actors have used Google Maps or Google Earth to plan attacks, escapes, or even military incursions. Are any employees concerned about the ethical use of those products that have been used against allies or even their fellow countrymen? Google's search engine is used at every military installation, maybe by every military member, and often in support of their

[4] Daisuke Wakabayashi amd Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," *The New York Times*. June 1, 2018. www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html

[5] Douglas MacMillan, "Google Won't Seek to Renew Pentagon Contract After Internal Backlash," *The Wall Street Journal*. June 4, 2018

primary military functions. Then should Google stop providing access to all of its products by military installations or even military members because they may support a warfighter? Maybe that is ethical because those services are not contracted directly to military and are instead available for free to everyone. The U.S. Naval War College uses Google's mail platform as its email provider while it educates future leaders in fields of national security strategy and policy. That is supported by a contract directly to the Navy, so is it ethical to support the military if it is two steps removed from possible kinetic action? Google is set to release an internal set of ethical guidelines in the coming weeks that will set limits on how it will permit its technology to be used in the future.[6] These are questions emerging technology companies will need to answer.

Google is not alone. No one believes that Mark Zuckerberg was intentionally developing a tool for the Russians to undermine the 2016 election when he developed Facebook. He, however, personally admitted, "it is a new challenge for internet communities to have to deal with nation-states attempting to subvert elections." [7] Aside from nation-state supported use, terrorists have long been known to uses social media platforms like Twitter and Facebook to communicate and recruit.[8] What is the ethical responsibility of companies whose products and services are used in ways they didn't imagine to malicious ends?

While technology has been racing ahead, U.S. policy and institutions have moved ahead at a snail's pace. The systemic national security and national economic problems

---

[6] Douglas MacMillan, "Google Won't Seek to Renew Pentagon Contract After Internal Backlash," *The Wall Street Journal*. June 4, 2018

[7] Andre Spicer, "Why Facebook's About-face on Russia Ads?", *CNN*. September 22, 2017. www.cnn.com/2017/09/22/opinions/facebook-advertisements-russia-spicer-opinion/index.html

[8] Elias Groll, "Twitter Suspended Far Fewer Terrorist Accounts in First Half of 2017." *Foreign Policy*. September 19, 2017. http://foreignpolicy.com/2017/09/19/twitter-suspended-far-fewer-terrorist-accounts-in-first-half-of-2017/

facing the United States in the area of microelectronics can be boiled down to three major foundational dilemmas: rising investment costs for manufacturing, diminishing competition in the marketplace, and an inflexible U.S. system poorly designed to counter foreign government targeted investment. These problems are of course not unrelated and, in fact, are quite dependent on one another.

Technology advancement in the area broadly referred to as microelectronics has followed what is widely known as Moore's Law, the projection that the number of transistors in an integrated circuit doubles about every two years.[9] This consistent rapid advance in technology causes many challenges, but the relevant one here is cost. In order to manufacture high-end microelectronics, a major capital investment needs to be made in a semiconductor fabrication facility (often referred to as a "fab") and all the necessary tools and expertise needed for the chipmaker to start production. As microelectronics continue to get smaller, the wafer and the tooling required to build the chips gets larger to accommodate production of more chips at the same time. This design is intended to be more efficient, but it also means an older facility will likely not be capable of creating smaller, state-of-the-art chips nor accommodate the larger tooling required. Therefore, new equipment must be purchased and a new facility built. The cost of that new facility and equipment today is somewhere in the vicinity of $30 billion[10].

This tremendously high price point for manufacturing infrastructure has naturally led to the second foundational problem, which is a declining number of manufacturers of state-of-the-art microelectronics at the leading edge of what is currently technologically

[9] Moore's Law. Accessed January 3, 2017. www.mooreslaw.org

[10] Shah, Agam, "China Responds to U.S. Chip Threats with a $30 Billion Factory". IDG News Service, January 20, 2017, https://www.computerworld.com/article/3159639/it-industry/china-responds-to-us-chip-threats-with-a-30-billion-factory.html.

possible. Due to the outsized upfront investment, new companies do not enter this market and existing companies consolidate, sell this part of their business, or decide to continue production of a legacy technology rather than chase the state-of-the-art. Today, as previously mentioned, there are only four major international manufacturers in this state-of-the-art area.[11] After the sale of IBM's microelectronic business to Globalfoundries in 2015, only one of these companies, Intel, is a U.S. based company. Only two of the four companies, Globalfoundries and TSMC, are foundry model manufacturers meaning they produce microelectronics designed by other companies for their own purposes. Both of these issues have caused problems for DOD and other government agencies based on access and trust. Access has become a problem because of cost and numbers associated with the order. DOD has specific needs and requirements, not common to other chip consumers, and a surprisingly small number are needed compared to commercial competitors. This makes such chips extremely expensive and not worth producing by the chipmaker who remains better off selling chips to the companies that place larger orders and don't have such specific technological requests. U.S. government security agencies also have very specific requirements for security in order to consider advanced microelectronics "trusted". These requirements again put the chipmaker and the government purchaser at odds. Meeting the government's security requirements for a small batch of microelectronics does not make financial sense when consumer demand is meeting or exceeding their company's capacity to build. These two issues alone leave DOD on the outside looking in as large commercial clients gain access DOD desires to the most advanced technology.

[11] Mission Executive Council, "A Strategic Framework for Trusted and Assured Microelectronics", October 14, 2016

The third major problem facing U.S. government national security agencies and industry alike is the significant investment by foreign governments into securing and consolidating specific global technologies and manufacturing capability within their borders or at least under their direct control or influence. China, for example, has plans to dedicate $150 billion over 10 years into capturing global semiconductor manufacturing capability, and that's just government investment. China is also using its model of government directed business as well, giving it the ability to move swiftly to purchase emerging technology businesses in other countries, enter into joint ventures where they have a directing share or at least receive access to partnering companies' intellectual property[12]. Additionally, China is well known for its extensive execution of corporate espionage, so that which they cannot buy, they steal. Aside from acquisition and theft of technology, such lofty investment has begun to generate a domestic technology development capacity. Far more fabs have been started in China over the last few years than anywhere else in the world.[13]

While these problems may be more immediately concerning from a national security perspective, they are also very concerning from a national economic perspective. Monopolies are never good for the general consumer as quality tends to fall and prices rise. Additionally, as competitors exit a market, efficient processes and decisions tend to overtake ethical ones, which can cause some serious problems especially in areas of advanced technologies where there is already only a small subset of the population that

[12] Brown, Michael and Singh, Pavneet, "How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation". Defense Innovation Unit Experimental, February 2017.

[13] Lapedus, Mark, "China: Fab Boom or Bust?" Semiconductor Engineering, March 16, 2017, http://semiengineering.com/china-fab-boom-or-bust/.

truly understands the implications. In these areas it is actually the competitors in the advanced technology market which society often relies on to provide transparency and a moral compass. Without competitors with diverging interests, goals, incentives, and intentions, who will call attention to business focused, but unethical decisions or actions especially in the areas that so few technical acumen needed to do so. As microelectronic laden devices continue to become more integral in daily life, quality and security need to dramatically increase. Who wants less quality, security, and ethical consideration for their future bionic arm, driverless car, pacemaker device, or artificial intelligence supported retirement savings investment portfolio? Aside from quality, security, and ethics, simple access could easily become a problem for U.S. manufacturers that have foreign suppliers of microelectronics. Access to the parts needed to make everything from iPhones to magnetic resonance imaging machines (MRI's) to fifth-generation fighter jets could easily be disrupted by a trade war not to mention an actual armed conflict. Without an indigenous, healthy manufacturing capability within the United States, government and industry should be prepared to lose access to the very supply chain they need to conduct business. In fact, the United States could simply lose many of those businesses to overseas locations with the necessary supply.

Bureaucratic Conundrums

One layer down from the foundational problems that affect both the national economy and national security organizations are those bureaucratic conundrums that affect only government agencies and institutions. Deciding how to resource organizations and procure necessary goods are challenges that any organization faces, but for government, these problems are based in the institutional processes that make our

government effective at times, but also slow and inflexible at others. The federal government's responsibilities are wide-ranging across areas like defense, diplomacy, education, energy, commerce, and more. The executive branch of the U.S. government has been organized to include 15 executive departments and a myriad of different agencies directly employing over 2 million employees to execute the direction of the President in these areas of responsibility.[14] Congress is empowered to resource these organizations and does so annually through an appropriations process that generates a budget for every federal government institution through a series of subcommittees constructed to take a deep look into the funding requirements of each to meet their mandated responsibilities. As one would expect, this creates a system where a budget is developed for every agency and the sum of those agency budgets become the federal budget or at least the discretionary part of the federal budget that does not include Social Security, Medicare, Medicaid, and interest on the debt. This is a useful way to be organized and transparent, but it also creates silos, which lead to challenges when collaboration across government is needed. In this case, those challenges are both the purchase of advanced microelectronics and setting the requirements for needed advanced microelectronics.

The way that DOD or any agency purchases microelectronics can be viewed in two ways: either independently as a subcomponent for something that a government defense entity plans to use for research and development or prototype production, or as a subcomponent of a larger piece of technology buried way down the line in the supply

[14] Office of Personnel Management, Federal Employment Reports. Data, Analysis & Documentation. https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/historical-tables/executive-branch-civilian-employment-since-1940/

chain. In either case, there are challenges with purchases by agencies across the federal government, and for both, the challenge is the failure in collaboration when setting requirements but in different ways.

In the first example where the tiny microchip is the product purchased, it is purchased based on either what has been purchased before for the same purpose, what is cheapest, or what is expected to work, all without collaborating outside of that agency to see what similar decisions everyone else is making. This is a daunting effort for sure because it assumes someone may know or have access to all the people who are looking for similar products. These aren't products you can just purchase through the U.S. General Services Administration (GSA), the government entity used to promote greater purchasing power and lower costs through economy of scale across government, like a laptop or printer.[15] There is, however, that same need. Especially since DOD and government as a whole increasingly represent a smaller percentage of the technology consumer base, it must pool requirements to leverage purchasing power as much as possible. Additionally, it needs to be careful to avoid continuously putting itself in the position where it has sole-source contracts because there is no other manufacturer still making one specific type of chip either because it is becoming obsolete or because it was never really successfully used anywhere else in the marketplace. Neither of these issues will ever be eliminated entirely because some government agencies have unique missions and will occasionally have totally unique requirements. For example, not a lot of government agencies are responsible for nuclear weapons like the National Nuclear Security Administration (NNSA) is, but that also doesn't mean that their requirements

[15] U.S. General Services Administration. Background and History. https://www.gsa.gov/about-us/background-and-history

can't be met by microelectronics also needed by another agency, for example, the Missile Defense Agency (MDA). It may be that a chip exists that is not the first choice of either agency, but can meet the requirements of both. This may make the chip the best product for the government to procure and actually a better choice for each agency in the long haul when costs remain lower and obsolescence is held off for longer. These are the types of decisions that have to be made early on, through collaboration across government, in the research and development phase though, because once a new technology advances through development and prototype to production, costs and timelines skyrocket if re-engineering is required down to the microelectronic level. At that point, it's too late.

In the second example where a microchip is buried deep in the supply chain, the issue is often less about cost and obsolescence and more about security. The piece of technology is so ubiquitous it can be bought through GSA or commercial off the shelf, or it has very specific military utility but was developed by a defense contractor and the decisions on the types of microelectronics were left to them. In either case, the product may contain microelectronics that were made in a less than friendly part of the world and those microelectronics may be preprogrammed to fail or have another purpose. Starting in 2016, it was revealed that U.S. users of some Android phones had their locations, contact lists, and text messages sent directly to a Chinese server.[16] In some cases, the phone manufacturer was even American but had foreign subcomponents or foreign software that created the exploited vulnerability. The world's largest maker of

[16] Matt Appuzzo and Michael S. Schmidt, "Secret Back Door in Some U.S> Phones Sent data to China, Analysts Say". The New York Times. November 15, 2016. https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html

surveillance cameras, Hikvision, a 42% Chinese government-owned entity, was called out in 2017 by the Department of Homeland Security for having similar "flaws."[17] It turns out that those cameras were not only being used to keep watch over Memphis city streets, but U.S. Army bases, and even the U.S. embassy in Kabul.

These were cameras in some cases that were actually procured through GSA, although GSA has since removed Hikvision from their list of automatically approved suppliers. The problem here is enormous. In some cases, procurement of these types of electronics goes back over a decade to a time before "the internet of things" was really a thing anyone thought about. Now they are superhighways of data delivered to an adversary and soft targets into secure systems. In order to defend against these threats the government writ large needs to not only make better decisions about requirements, it needs to go back and assess every electronic device it ever bought to see if it is a threat. Doing so requires knowing the full supply chain of every piece of equipment the government purchases, and not only is that difficult it's also expensive. In cases of previously purchased items it may be impossible, but even if it just started now, going forward, the challenge is extreme. For starters, for some electronics, the supply chain is the secret sauce in the recipe that makes the item valuable. It is the manufacturer's intellectual property that they may not be interested in sharing, even for an additional fee. For those who do share the full supply chain breakdown, it will come at a cost. Not only will the U.S. government need additional people and resources to track these supply chains and products, so will the manufacturers, which will undoubtedly drive up the cost

[17] Dan Strumpf, Natasha Khan, and Charles Rollet, "Surveillance Cameras Made by China are Hanging All Over the U.S.". The Wall Street Journal. November 12, 2017. https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949?shareToken=st9a295d08b78c40349a46e455c5ea3b8b&reflink=article_email_share

of the product to the government as well. In short, addressing these issues is a conundrum and one that is going to take time, people, and a whole lot of money to overcome. Despite the costs, there is an ethical imperative for both government and industry to take the necessary steps to develop real security in technologically advanced products. Anything less should be considered criminal neglect when failures in technical security start to impact human physical and financial security.

Not only will addressing these issues take time, people, and money, it will most importantly take communication and collaboration, which is certainly not easy given those silos discussed earlier. Those silos isolate the people that both develop and procure and the funding that gets budgeted by agencies and appropriated by Congress. The communication and collaboration piece cannot be undersold as it is integral from the beginning in setting requirements in R&D and production, through procurement and continuing into the life-cycle management of any piece of technology. The next problem is that this is everyone's challenge, but no one's responsibility.

Specific Challenges

In addition to the larger foundational and bureaucratic problems, there are also some specific challenges DOD and other government agencies face in conjunction with keeping access to trusted and assured microelectronics. Trust in, assurance of, and access to advanced microelectronics directly threaten U.S. national security agencies today. Nefarious tampering with microelectronic products to perform an ulterior purpose or simply fail in a given situation affect government and industry alike. Poor quality control, which produces a product that never performs to meet expectations, is very difficult and expensive to catch. Excessive cost for small batch sizes for niche

capabilities is another challenge that can be problematic for all types of organizations. All of these challenges will be addressed in terms of relationship to trust, assurance, and access to advanced microelectronics with DOD.

Trust

Trust in the world of defense microelectronics according to the Defense Microelectronics Activity (DMEA) is defined as, "assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components."[18] It includes all of the physical security of manufacturing and the authorized chain of custody to prevent tampering, reverse engineering, and modification of products. In order to be considered a "trusted foundry" or supplier of microelectronics to national security agencies, manufacturers must be accredited through DMEA to ensure facilities, processes, and staff all meet necessary security requirements. There are, however, some specific problems with reliance on this accreditation process. It is expensive and time-consuming for a company to go through the "trusted" process for what is often a relatively small part of manufacturers' total business. There are typically requirements for the foundry to be both geographically located in the United States and be a U.S. owned company. This has become increasingly challenging as manufacturing, especially at the leading edge of technology, has moved overseas, and some of what remains here in the United States has been bought by foreign entities. This was the case with Globalfoundries, the second largest pure-play foundry, which is owned by the Abu Dhabi Emirate through Advanced Technology Investment Company. Globalfoundries purchased IBM's trusted foundry facilities in 2015 and has since secured a temporary

[18] Defense Microelectronic Activity, www.dmea.osd.mil/trustedic.html.

agreement to continue production for DOD despite its foreign ownership.[19] The other problem with using gates, guards, and custody to define security is that it also is never 100% successful.

Assurance

Assurance, the idea that the product does what it is supposed to, only what it is supposed to do, and only when it is supposed to do it, is another concern that always presents a challenge for all consumers of microelectronics. It is larger than just concern for malicious actors but includes flaws in design and manufacturing, as well. In the first days of 2018, computer security experts disclosed two major security flaws in the design of processors that power "most of the world's computers."[20] The flaws named "Specter" and "Meltdown" allow hackers to access sensitive information and open an illicit backchannel to a computer containing chips with these flaws. Finding flaws like this in tiny integrated circuits is hard. In order to test one chip from a batch of millions, it may take up to a month to test, cost thousands of dollars, and in the end, the one chip tested and perhaps verified is assured, has also been destroyed in the process of testing it. So, most consumers rely on trial and error processes for lack of a better one. If they find problems with multiple chips in the same lot, then they assume the entire lot is bad, which can be a costly assumption.

Access

[19] A Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Armed Services "Assessing DOD's Assured Access to Microelectronics in Support of U.S. National Security Requirements." House of Representatives One Hundred Fourteenth Congress, First Session, October 28, 2015.

[20]The Economist Science & Technology, "The Chips Are Down." January, 4 2017. https://www.economist.com/news/science-and-technology/21734044-fixing-underlying-problems-will-take-long-time-two-security-flaws-modern?cid1=cust/ddnew/email/n/n/2018014n/owned/n/n/ddnew/n/n/n/nna/Daily_Dispatch/email&etear=dailydispatch.

Access is a different problem for DOD and government agencies, and one they are not accustomed to having. The Department of Defense is a lot of things, a fighting force, an enormous bureaucracy, and maybe the largest single procurement organization in the world, but what it is not is a manufacturer. It has never had to be because it is such a gargantuan customer that typically it has no problem procuring in any market and is accustomed to the role that it heavily influences markets so there is extensive regulation to ensure fairness in source selection and a competitive process for bids. For decades, DOD was the largest purchaser of electronics and had its normal influence in the semiconductor and microelectronics market, but times have changed. Now, DOD makes up less than 0.5% of market share.[21] The advent of the personal computer, mobile phone, laptop, smartphone, tablet, and now the entirety of the "internet of things" has driven demand through the roof. Suddenly, DOD has found itself competing with companies whose demand is often more generic, more constant, more flexible, and significantly larger. DOD's problems with access also extend beyond their small market share requirement. Aside from their orders being small in number, they are also specialized, varied across many types of technologies, and highly inflexible. DOD is also widely considered one of the most difficult customers to work with because of extensive paperwork, accreditation, and regulation.

From a microelectronics manufacturer's perspective, none of these things make the United States Government a very attractive client. Extra security, paperwork, accreditation, custody tracking, and specific requirements raise costs. That extra cost can make DOD a worthy client for a while, but as the market changes and demands newer

[21] Mission Executive Council, "A Strategic Framework for Trusted and Assured Microelectronics", October 14, 2016

technology, many of the products DOD procures do not. This puts some producers in a bad spot because in order to keep up with customer demand they eventually need to start making smaller microelectronics, but DOD needs to keep procuring the same chip for the same system long after the commercial market would have moved on to more current technology. Eventually, the manufacturer either leaves the country because they can produce the same product somewhere else cheaper (and perhaps be closer to more of their clients, or receive some great incentive from another government), goes out of business because their deal with DOD is no longer profitable, is bought by another company, or decides to discontinue making the product DOD requires. Due to these types of situations, DOD and defense agencies have found themselves in several sole-source relationships, where the current provider of microelectronics, is the only available and approved provider. This is obviously not ideal for any supply chain much less one integral to national security.

PART II – TIERED SOLUTIONS

There is no doubt that the challenges are immense and in mass seem insurmountable. There are threats potentially hidden in every single piece of technology we all touch daily and throughout the security architecture, all Americans have come to rely on to sleep well at night. How does DOD, the U.S. Federal Government, or the nation as a whole dig itself out of this? Start by taking a lesson from Will Rogers. "If you find yourself in a hole, stop digging." There has been tremendous admiration of the problem, and an admirable problem it is indeed. So, in an attempt to address it, it should be deconstructed and broken into digestible pieces. This paper provides an architecture or design to begin filling in the hole. Since the problems that exist range from the

technical nature of advanced technology, to the policy realm of how government operates, to the foundational nature of government and what it and others' roles and ethical responsibilities are in a capitalistic democracy, this paper deconstructs the problem in that fashion from a perspective of national security and primarily DOD. Recommendations, therefore, will come in reverse order of the problems laid out. First will be suggestions that DOD can execute independently, then options that can be addressed by government, and finally what needs the assistance or buy-in of the President him or herself and the people that put him or her in office, because some of these recommendations would require the efforts of more than just the federal government. As the recommendations proceed up the food chain, they get harder to accomplish, but the impact becomes far greater as well. Every victory closer to the top of that food chain or the end of this paper has a dramatic trickle-down effect that will have a great impact on DOD and national security.

Inside the Wire

The challenges laid out above are not a surprise to people familiar with this topic and there are some moves in progress by DOD to address many of them. In fact, some of the proposed or ongoing actions may have an overlapping effect and improve more than one of the specific challenges of trust, assurance, and access. Many in the DOD research community believe that the long-term solutions to many of these specific challenges can be overcome through advances in science and technology. It would be helpful to have a full government effort in this area, but DOD does represent about half of the federal

discretionary budget and therefore invests nearly half of all federal dollars in R&D efforts, so it is better resourced than any other agency to take on these challenges.[22]

There are several possible paths to tackling the trust challenge, all of which researchers believe will be less costly and more effective than the current policy of gates, guards, and secure custody. The first idea overlaps trust with assurance and entails improving the testing process to the point where it can be done in hours versus weeks, accomplished inexpensively, and not destroy the device it tests. Then, it would be possible to test larger numbers in a lot of microelectronics or even all of them, raising the confidence that the product is free of tampering and does what it is supposed to, when it is supposed to, and only when it is supposed to do it. Essentially, this would replace the trust needed in the process with trust provided in the product. If this can be done, then the only security needed is to protect intellectual property and actual product from being stolen, just like any other product. This sounds easy, but it is far from it and no one really knows if and when the technology needed for this idea will become a reality.

Additional ideas to address access and trust focus separately on the two halves of a microchip fabrication, the front end and back end. The front end is basically the integrated circuit (IC) design and power platform that the rest of the chip is built on. The back end is where the specific functionality of the IC is fabricated. New processes focused on technological advancements involving leveraging state-of-the-art mask techniques along with obfuscation techniques could allow for greater security while still tapping into commercial markets.[23] One idea here is that DOD could use generic,

[22] Office of Management and Budget. FY18 Federal Budget, Research and Development. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_18_research.pdf

[23] Mission Executive Council, "A Strategic Framework for Trusted and Assured Microelectronics", October 14, 2016: 29

commercially produced front end of line microelectronics for specialized needs by adding all of the advanced components and classified design in the back end of line at more secure private or government-owned facilities after the fact. This is a simplistic description, but basically, the generic chip would serve as a base or platform to build the remainder of a customized chip on later. Another possibility is that both front end and back end are produced separately but still assembled by a commercial provider to keep costs lower, but developed techniques would keep all parts of the fabrication process from having all the necessary design details to steal or co-opt the IC. Both of these possibilities keep DOD mostly out of the fabrication business and could continue to facilitate access at the leading edge of technology in the commercial sector.

Another science and technology solution that could change trust and access is the development of "mini-fabs." As previously discussed, microelectronic fabrication facilities are incredibly expensive and require increasingly large facilities. They are big for a few good reasons. It takes sufficient power, water, cooling, resources, and tooling to manufacture tiny microelectronics, and surprisingly as the size of the products get smaller the tooling gets larger. Also, in order to make up for the tremendous cost of these facilities, it is necessary to use economy of scale to make the facility worth the investment. But what if that wasn't the case? If you could dramatically shrink the size of the facility needed, say to the size of a multi-modal shipping container, it would change the industry. Instead of relying on high-volume to defray production costs, boutique production and unique designs would not need as large of a market in order to reach production scale. This would help DOD dramatically as it is usually a smaller-scale

customer. Mini-fabs could be government or industry owned, and likely both would be useful.

On the contrary, there are other ideas that overlap trust with access but increase DOD's role in fabrication. Since DOD already generally requires small batches of microelectronics compared to commercial standards, perhaps it does not make sense to try and meet those requirements commercially. While DOD does not have significant inherent manufacturing capability, it does have tremendous research and development capacity and capability. It may be possible to meet more governmental manufacturing requirements at government-owned labs instead. This is done in some areas already. DOD's Defense Microelectronic Activity has a fabrication facility, but more government facilities, like MIT/Lincoln Labs, Los Alamos, or Sandia National Labs could potentially be used.[24] All necessary security measures are already in place and funded. This would be helpful for legacy practices but does not help with access to the most advanced technologies that are only available from those few advanced commercial manufacturers.

These are just a few of the possible solutions that can address the trust, assurance, and access issues that DOD faces. Any combination of successes in these areas would be game-changing for DOD and the industry, but the reality is that it's hard to know which of these ideas will yield results and when. So, it is important to invest in as many of these good ideas as possible, knowing that some will fail and many will take too long to develop to be useful. Placing many of these relatively small bets dramatically increases the chance that DOD achieves a break-through technology that is sorely needed.

Whole of Government Effort

[24] Defense Microelectronics Activity (DMEA) website. https://www.dmea.osd.mil/actech.html

Some of the challenges can and eventually will be overcome by advances in technology, but there are also many that can be mitigated, influenced or resourced through policy, process, or legislation. Especially in the U.S. where all government funding is appropriated by Congress, legislation matters. Not only does the funding matter, both how much and for what, but the authorizations matter as well.

If agencies are going to work better together to collaborate on both setting requirements and procurement it means increased communication as well. Not just between the agencies collaborating but between those agencies and their respective congressional appropriators and committees of jurisdiction. The challenges of government agencies working between the silos is real, even for something like joint investment in one of the technology areas mentioned above, but it is not debilitating. Elected officials and staffers alike want to see the U.S. succeed. They want to be part of the solution rather than part of the problem, but they need to be informed to do so. Budget cycles are long, indeed, in DOD they are five years long, but even for other agencies that are just working a year out it can be difficult to know what opportunities will exist for co-investment a year or two from now. Pooling resources between federal departments will be challenging. Not only would a proposal like this need to survive the budgeting process within each department, it would also need to survive the authorizations and appropriations process on Capitol Hill through many separate subcommittees, simultaneously. Many career budgeting experts would assess this process as high-risk, but it would also yield a high reward.

Agencies could, however, start small. Each relevant agency should invest some level of resources into a technology advancement in this area that another agency is

leading on. It can be as simple as a direct monetary investment with the other agency, a grant to a supporting institution, in-kind support through donated equipment, facilities, or people. Every agency has the authority and the budget space to do one of those things immediately, and all of them are needed. Then take that example to Congress through the Legislative Affairs shop at that agency to tell them about the successes so far and the needs of the future. Staff may even share authorities agencies didn't even know already existed. For example, The Defense Production Act is an authority that is used to expedite the purchase of materials and equipment from industry that is required for national defense.[25] Different Titles of the Act are delegated to different agencies like DOD, Department of Homeland Security (DHS), or even The Federal Emergency Management Agency (FEMA), but all can act as the executive agent and work together. Aside from simply requesting funds agencies must work with the Hill and inter-agency partners to share microelectronic requirements as much as possible to minimize churn and obsolescence further in the future

One of the biggest challenges mentioned is keeping track of what microelectronic needs exist today and what will be needed for across an extremely wide range of electronic systems, platforms, and products for all military services and government agencies and regularly comparing that to the availability of trusted and assured microelectronic products. This would be easy for one computer or weapon system, but for thousands of systems, it becomes nearly impossible, especially because often this is information that may not be available to DOD. In the past, information at the micro level

[25] Federal Emergency Management Agency. Defense Production Act Program. https://www.fema.gov/defense-production-act-program

of the supply chain was not required of the defense industry, and it still isn't for commercial products.

There is progress, though. GSA has banned several companies from selling COTs technology to government agencies.[26] Regulation is now changing to require supply chain information, but tracking thousands of legacy systems is labor intensive and will take time. The supply chain of procured products and systems is an entropic list of microelectronic sizes and uncoordinated decisions lead to diverging rather than converging investments. The Office of Manufacturing and Industrial Base Policy in OSD is undertaking an enormous effort to map those supply chains and highlight vulnerabilities.[27] Additionally, the Deputy Secretary of Defense chartered a Joint Federated Assurance Center (JFAC) in February 2015 to accomplish many of the things discussed here.[28] JFAC is tasked to increase collaboration on requirements across DOD, develop and maintain software and hardware detection capabilities, and develop remediation opportunities. These are good steps, but they are entirely within DOD and not cross-cutting throughout government as they need to be.

Once those efforts expand outside of DOD to include all of federal government and significant supply chain information is available, one of three possible policy solutions could solve the problem of potential obsolescence. First, authorization for

[26] Dan Strumpf, Natasha Khan, and Charles Rollet,. "Surveillance Cameras Made by China are Hanging All Over the U.S." *The Wall Street Journal*. November 12, 2017. https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949?shareToken=st9a295d08b78c40349a46e455c5ea3b8b&reflink=article_email_share

[27] U.S. Department of Defense Manufacturing Technology Program. Manufacturing and Industrial Base Policy. https://www.dodmantech.com/initiatives/MIBP

[28] Hurt, Thomas. "DOD Joint Federated Assurance Center (JFAC) 2017 Update." Office of the Deputy Assistant Secretary of Defense for Systems Engineering. 20th Annual NDIA Systems Engineering Conference, Springfield, VA. October 26, 2017. https://www.acq.osd.mil/se/briefs/19910-NDIA17-Hurt-JFAC.pdf

procurement of lifetime purchases of necessary microelectronics could be made at the time of procurement. Second, lifetime purchase of necessary microelectronics could be authorized as soon as a sole-source situation is identified. Third, the design, intellectual property, and equipment needed to manufacture the microelectronics could be purchased, facilitating transfer to a new manufacturer should the previous relationship terminate for any reason. None of these, however, is the most cost-effective approach considering DOD rarely accurately estimates the lifetime of any major system.

Of course, there is another whole of government policy solution: fully funding the development of government-owned fabrication facilities for all known requirements. This would take care of the trust, assurance, and access issues, but was estimated to conservatively require an initial investment of $100-$140 billion,[29] equivalent to approximately 20% of the annual defense budget. The Office of Science and Technology Policy estimates that one new facility in the U.S. today would cost approximately $12 billion, and the government would need at least 10 to bring the expertise and capabilities in-house, so that estimate isn't far off.[30]

National Effort

The incredibly complex challenge of manufacturing the tiniest of products is quite an enormous and even foundational dilemma. This paper has focused primarily on DOD's national security concerns, but it turns out this is a national economic dilemma and several ethical challenges as well. The initial list of national security concerns for

[29] Estimation developed by the National Security Division, Office of Management & Budget, April 2017

[30] President's Council of Advisors on Science and Technology. "Report to the President – Ensuring Long-Term U.S. Leadership in Semiconductors." January 2017. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pd

DOD including rising costs, diminishing competition, and other governments seeking to corner the market can affect the U.S. national economy in nearly the same crippling fashion. Access to trusted and assured microelectronics is critical throughout the economy. The internet of things will continue to invade and dominate in all sectors of the economy: finance, healthcare, transportation, manufacturing, education, and more. All of the computing power and technical equipment those industries rely on are built with thousands to millions of microelectronics. With that in mind, how do you bring all instruments of national power to bear against such a complex and insidious threat, especially in a capitalistic democracy that values competition, transparency, and fairness? How does the government convince new non-defense industry partners that it is ethical for them to support national security organizations? The answer is, carefully, through a collaboration of and coordination with all relevant institutions. In an authoritarian or dictatorial regime where the state has total control, this is significantly easier. Virtue ethics prevail, where all things are done for the survival and success of the state in these societies. Any supporting actions are deemed virtuous. When leadership can direct the priorities, actions, and investments across government, industry, and academia, moving the country in unison is not only possible, it can be done expeditiously.

This is a problem that DOD or even all U.S. government institutions cannot take on alone. There needs to be government participation and even leadership at the highest level, but it needs to be an individual or entity that reports to the President and has the authority to direct federal agency action and make use of their relevant facilities, programs, and people, while convincing industry and academia to do the same. This entity could take the shape of a public-private partnership that not only allows

government agencies to pair resources and requirements but allows the government to work with U.S. industry partners and academic institutions to foster a critical but fragile part of the U.S. economy. Each of these sectors brings forth different resources necessary for a stable and prosperous microelectronics manufacturing market. Industry partners have a large majority of the capital investment and manufacturing capability. "While total U.S. government spending on all non-defense R&D was $65.9 billion in 2015, the semiconductor industry alone nearly matched this level of R&D spending at $55.4 billion."[31] Academic institutions provide the training throughput for the necessary workforce and add value in research and development. U.S. government still invests far more in research and development than any individual company and brings a convening authority necessary to facilitate success. There are of course challenges here as well. Government is typically allergic to partnerships with industry for fear of accusations of favoritism followed by lawsuits for wrongful practice based upon the Federal Acquisition Regulations (FAR). However, when does the government's ethical requirement to protect its citizens and institutions supersede its commitment to fairness? Regulation and legislation changes would likely be needed to make successful recommendations a reality, but recent trends in authorities granted and initiatives started suggest that this could be possible.

Experts in the President's Office of Science and Technology Policy suggest that "U.S. policymakers can help a diffuse set of players in academia, industry, and government laboratories organize around important common goals and support catalytic

[31] President's Council of Advisors on Science and Technology. "Report to the President – Ensuring Long-Term U.S. Leadership in Semiconductors." January 2017. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf

activities that remove obstacles to fundamental technological and industry progress. This approach lies somewhere between "top-down" and "bottom-up:" government should set ambitious and clear goals, rather than assuming that all progress is equally useful and support only key activities, rather than trying to comprehensively dictate all activities. In short, semiconductor innovation should not be viewed as an independent goal—rather, it must be part of broader innovation in the ways semiconductors are used."[32] The real goal must be greater support of a developing a robust ecosystem surrounding indigenous manufacturing of advanced microelectronics including everything from greater investment in research and development of tooling, techniques, and design to workforce development initiatives to feed the growing number of government and civilian jobs in the field. To be successful, effort and investment will need to take a holistic approach to the industry.

Given the challenges previously discussed, how does U.S. government convince those technology companies opposed to working with DOD, that not only is it morally acceptable to work with DOD, but they should be ethically bound to do so? There are a number of very reasonable arguments that justify support from non-defense industry technology company partners, even those who have employees opposed to the concept of supporting military capability. First, a utilitarianism approach could be used to convince companies that cooperation and collaboration with the U.S. government is not only in the best interest of the company for fiscal reasons but also because it is the morally correct course of action which maximizes benefit over harm to the largest U.S. and even

[32] John P. Holdren and Eric S. Landler, "Cover Letter for Ensuring Long-Term PCAST letter Ensuring Long-Term U.S. Leadership in Semiconductors. "January 2017. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf

international population. Collaboration with DOD will allow both government and any U.S. company to improve capability and security benefitting consumers and citizens alike. A utilitarian approach suggests that any technology company is morally obligated to provide the best product or service to its customer and it surely cannot do that without security and the security that it can provide is only increased through cooperation with the U.S. government and DOD. Additionally, to maintain its own security from foreign competitors and

Those employees of companies who are not convinced by the utilitarian approach because they believe war by nature is unethical may be swayed by one of many consequentialist arguments. These individuals believe that war is unethical because of the harm to humanity it brings, but what if cooperation with DOD actually helps to limit casualties in war? Would these employees feel compelled to support DOD? Support of DOD with the most advanced microelectronics helps to keep safe U.S. service members and civilians. Use of artificial intelligence and machine learning may help the military accurately and effectively target threats limiting both the extent of a conflict through effectiveness and collateral damage or unintended. Military conflict will still occur regardless of a technology company's participation, but without its participation human suffering may actually be greater, which should actually morally compel the company to participate. In fact, this argument for consequentialism could be taken even further. The end goal of DOD and the ethical company are actually one in the same. They both would like to avoid war and any military conflict. DOD is more successful at deterring threats and avoiding conflict when it has the greatest capability advantage over its adversaries. If this is agreed to be a true statement, than the support of the technology company for

DOD capabilities, than that support is actually preventing war and withholding that support is actually inviting war. Finally, another consequentialist approach could raise the concern that not all countries and companies will make the same decisions on ethical standards. If any advanced technology that has a dual use capability is kept from military exploitation in the U.S. based on a company's ethical decision, it may put DOD in serious disadvantage compared to strategic competitors whose society's, based on their authoritarian or dictatorial constructs not limited by ethics, will in turn be putting forth all government and industry effort to exploit an asymmetric technological advantage. Yielding of technological advantage not only puts the U.S. government and DOD at risk, but also U.S. society itself and therefore the company we are referring to. In order to secure its own future existence and the ability to continue to act ethically and responsibly a consequentialist argument may convince technology companies that it is not only in their best interest to support DOD, but it is also just. There are other arguments to made to justify ethical participation or collaboration of private U.S. companies with DOD if neither of these suffice, but the point is that any U.S. technology company that avoids working with DOD based on an ethical argument, has not fully thought through their argument to a logical conclusion from an ethics standpoint.

Once the ethical issue of technology company participation is superseded, there are some possible models for similar efforts in the recent past like the National Alliance for Advanced Transportation Battery Cell Manufacture formed in 2008 or the 2011 Department of Energy's SunShot initiative designed to reduce the cost of solar energy by 2020. According to Robert Atkinson, CEO of the Information Technology and

Innovation Foundation, both of these efforts were modeled after Sematech.[33] Sematech was a consortium of 14 U.S. semiconductor companies and the Departments of Defense and Energy along with the National Science Foundation (NSF) established in 1987 with a goal of regaining technical superiority and market dominance as it had been steadily losing ground to the Japanese throughout the 1980s.[34] This consortium was more of a Government-Industry Partnership (GIP) and has widely been credited with supporting the resurgence of the industry. The consortium continued through 2015 when it was absorbed by SUNY Polytechnic institute which invested $300 million to move the organization and use it to leverage advances in other emerging technology areas.[35] One of the reasons cited for the dissolution was the previously mentioned devolution of the industry to four major industry players at the advanced end of the microelectronics technology spectrum. Perhaps it is time for a similar effort to be made with slightly different goals in mind.

Other recent examples of the public-private partnership model are the Obama Administration investments in Advanced Manufacturing. These Institutes could be a model for such an effort in the area of microelectronics. "Established in 2014, *Manufacturing USA* brings together industry, academia, and federal partners within a growing network of advanced manufacturing institutes to increase U.S. manufacturing competitiveness and promote a robust and sustainable national manufacturing R&D

[33] Robert D. Hof, "Lessons from Sematech." MIT Technology Review. July 25, 2011. https://www.technologyreview.com/s/424786/lessons-from-sematech/

[34] Gregory James Benzmiller. "Assessing the Success of Dual use Programs: The Case of DARPA's Relationship with SEMATECH—Quiet Contributions to Success, Silenced Partner, Or Both." November 2011: 16 https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1067&context=etd

[35] Diana, Chelsea. "Why Sematech is merging with SUNY Polytechnic Institute." Albany Business Review. May 13, 2015. https://www.bizjournals.com/albany/morning_call/2015/05/why-sematech-is-merging-with-the-suny-polytechnic.html

infrastructure."[36] The goals of the institutes, according to a Deloitte assessment, are to increase the competitiveness of U.S. manufacturing, facilitate the transition of innovative technologies into scalable, cost-effective, and high-performing domestic manufacturing capabilities, accelerate the development of the advanced manufacturing workforce, and to support business models that help these Institutes become stable and sustainable.[37] The original intent of the White House was to build this network of institutes under the Department of Commerce to provide a government focal point in one location with the health of the national economy directly in mind. Congress, however, did not agree and refused to appropriate the necessary authority and funding for the effort. Not to be thwarted, the Administration instead funded the now 13 institutes through specific agencies with relevant interests in each specific technology field. For example, DOD sponsored an institute to develop "Lightweight and Modern Metals Manufacturing" while DOE sponsored "Next Generation Power Electronics Manufacturing." [38] Each institute will receive in total approximately $70-110 million in appropriated government investment with equal or greater matching funds from industry partners.[39] While the challenge of manufacturing trusted and assured microelectronics is broader and would be more expensive the President's Council of Advisors on Science and Technology believe it could be a good model to address the microelectronics manufacturing problem.[40]

---

[36] A National Advanced Manufacturing Portal. Manufacturing USA. https://www.manufacturing.gov/

[37] Manufacturing USA, A Third Party Evaluation of the Program Design and Progress. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-mfg-manufacturing-USA-program-and-process.pdf

[38] The White House Office of the Press Secretary, *Obama Launches Competition for Three New Manufacturing Innovation Institutes*, May 9, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/obama-administration-launches-competition-three-new-manufacturing-innova

[39] Manufacturing USA. https://www.manufacturing.gov/funding

[40] President's Council of Advisors on Science and Technology. "Report to the President – Ensuring Long-Term U.S. Leadership in Semiconductors." January 2017.

A final possibility would be to direct one government institution to be responsible for the coordination, collaboration, and acquisition across government. Since microelectronics are embedded in everything electronic the government purchases, this would require the creation of government-wide equivalent to the combination of the Defense Logistics Agency, Defense Microelectronic Activity (DMEA), JFAC, and GSA. This would be an expensive endeavor but could be a good way to pool expertise and dramatically overhaul government acquisition. In order for this to solve all of the systemic problems mentioned, this government entity would also require the authority and resources to build government owned and equipped fabrication facilities to maintain access where requirements exist and accredited manufacturing capability does not. This proposal is surely high cost and as previously mentioned would quickly exceed over $100 billion to really be effective as a government only initiative. This definitely presents its own problems in a relative time of budget austerity for domestic government programs. That said an idea like this could fall into two areas ripe for additional government funding, defense, and infrastructure. This idea could gain favor if it was seen as a legitimate effort to slay the unwieldy dragon of defense acquisition or was made part of a countrywide infrastructure redevelopment program. There is still the challenge, however, of accessing the greatest talent, capability, and capacity that exists in the commercial sector, but if the budget is available, access can be purchased.

---

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf

In a free, open, transparent, and capitalistic society all of these institutions must choose to work together in unison. The U.S. government should develop a collaborative organization that brings together resources from industry, academia, and government into a network or ecosystem to support the indigenous manufacturing of advanced microelectronics. The shared facilities, expertise, workforce development, and investment could support a range of activities, including early-stage research and development, prototyping, production, design, and technology transfer. This organization could even be used to advise on national level policy in technology areas, but most importantly it needs to have active participation from all three sectors and the government convening authority needs to report directly back to the Administration in some capacity as to not be downgraded or buried within any one agency.

Conclusion

Our dependence, as a society, on new technology is not likely to diminish at any point in the foreseeable future. New technologies create wonderful solutions for humanity, but they also create new risks. Microelectronics are the building blocks of those technologies that increasingly creep into all aspects of our lives for better or worse. The United States has been the lead innovator in manufacturing capability and capacity but is quickly losing ground to competitors like China. In order to defend its national security supply chain and technology economy, the U.S. government in conjunction with academia, and industry must find ways to address the systemic problems in the microelectronics manufacturing industry of exploding costs, a dwindling number of trusted manufacturers, and foreign competitors seeking to corner the market.

If manufacturing of microelectronics moves entirely overseas or even just the most advanced companies do, it puts at risk access to those downstream sub-components needed for every single piece of technical equipment made from ATMs, to laptops, to pacemakers, to every form of the transportation vehicle. If those microelectronics are made almost entirely overseas it won't just be text messages and surveillance video that may be getting sent back to China; it may be health records, banking information, and every piece of information that is important to any individual or company in the United States. This is terrifying but it gets worse. What if the capability exists to not only siphon information, but to direct action like liquidating a person's bank account, or change the formula in a child's prescription, or have a car speeding south along Route 1 take a hard right into the Pacific Ocean? It actually doesn't have to be as difficult as that. Perhaps those deeply embedded microelectronics just need to fail on command. With that capability, one could stop a pacemaker, shut down the New York Stock Exchange, or fail electric grids.

Imagine a scenario where the Air Force deploys in the next major war its most advanced and lethal aircraft. As those F-35s use their stealth capability to approach, undetected, the adversary's Air Defense Identification Zone (ADIZ), each one simultaneously ejects its pilot and crashes into the ocean because deeply embedded in those aircraft systems were hardware or software coded to trigger the ejection seat as soon as it was flown into a specific geographically defined area. This would be a phenomenal capability. It would have the potential to destroy significant combat capability while destroying the evidence, potentially kill no U.S. citizens, scare the wits out of every military member on Earth, and force the U.S. to immediately distrust every

piece of equipment in its inventory. Perhaps Peter Singer's example from *Ghost Wars* is more plausible as it only requires a simple subcomponent to do what it is supposed to do, just at the wrong time. Either way, the possible vulnerabilities are terrifying.

In order to avoid this scary and potentially dystopian future, it is important to act now. The national security and national economic challenges of trust, assurance, and access to microelectronics facing the U.S. are significant, but there are a variety of solutions that can help to alleviate the problem or at least mitigate the risks. No single suggestion provided addresses all of the challenges, so multiple recommendations throughout DOD, the federal government, and the country need to be pursued simultaneously to appropriately mitigate the risk. The DOD only solutions may be the equivalent of using duct tape to fix cracks in the dam, compared to the public-private partnership approach, which would be more akin to a new dam. The duct tape is always useful to keep you dry now, but the new dam is what will keep you and your children from someday drowning.

Bibliography

Appuzzo, Matt and Schmidt, Michael S., “Secret Back Door in Some U.S> Phones Sent data to China, Analysts Say”. The New York Times. November 15, 2016. https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html

“Assessing DOD’s Assured Access to Microelectronics in Support of U.S. National Security Requirements”. A Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Armed Services, House of Representatives One Hundred Fourteenth Congress, First Session, October 28, 2015.

Benzmiller, Gregory James. 2011. "Assessing the Success of Dual-use Programs: The Case of DARPA's Relationship with SEMATECH—Quiet Contributions to Success, Silenced Partner, Or Both." November 2011. https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1067&context=etd

Bradsher, Keith and Mozur, Paul. "Political Backlash Grows in Washington to Chinese Takeovers." New York Times Company, https://search.proquest.com/docview/1765523112?accountid=322.

Browning, Larry D., Janice M. Beyer, and Judy C. Shetler. 1995. "Building Cooperation in a Competitive Industry: SEMATECH and the Semiconductor Industry." *The Academy of Management Journal* 38 (1): 113-151.

Carayannis, Elias G. and Jeffrey Alexander. 2000. "Revisiting Sematech: Profiling Public- and Private-Sector Cooperation." *Engineering Management Journal* 12 (4): 33-42.

Defense Microelectronic Activity, www.dmea.osd.mil/trustedic.html.

Defense Production Act (DPA). Federal Emergency Management Agency website. https://www.fema.gov/defense-production-act-program

Deloitte. *Manufacturing USA, A Third Party Evaluation of the Program Design and Progress*.https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-mfg-manufacturing-USA-program-and-process.pdf

Department of Defense

Diana, Chelsea. “Why Sematech is merging with SUNY Polytechnic Institute.” Albany Business Review. May 13, 2015. https://www.bizjournals.com/albany/morning_call/2015/05/why-sematech-is-merging-with-the-suny-polytechnic.html

Federal Emergency Management Agency. Defense Production Act Program. https://www.fema.gov/defense-production-act-program

Fox, Justin. “U.S. Manufacturing isn’t Dwindling Away (or Booming).” *Bloomberg*. March 7, 2018. https://www.bloomberg.com/view/articles/2018-03-07/u-s-manufacturing-isn-t-beating-china-but-it-s-not-doomed

Grindley, Peter, David C. Mowery, and Brian Silverman. 1994. "SEMATECH and Collaborative Research: Lessons in the Design of High-Technology Consortia." *Journal of Policy Analysis and Management* 13 (4): 723-758.

Higginbotham, Stacey. "Sematech Rethinks Mission." *Austin Business Journal*, Vol. 22, Iss 26.September 13, 2002.

Hof, Robert D. “Lessons from Sematech.” MIT Technology Review. July 25, 2011. https://www.technologyreview.com/s/424786/lessons-from-sematech/

Hurt, Thomas. “DOD Joint Federated Assurance Center (JFAC) 2017 Update.” Office of the Deputy Assistant Secretary of Defense for Systems Engineering. 20th Annual NDIA Systems Engineering Conference, Springfield, VA. October 26, 2017. https://www.acq.osd.mil/se/briefs/19910-NDIA17-Hurt-JFAC.pdf

King, Ian, “China Has Big Plans for Home Grown Chips”. Bloomberg, June 25, 2015, https://www.bloomberg.com/news/articles/2015-06-25/china-has-big-plans-for-homegrown-chips.

Lipsky, Jessica. “IBM-GlobalFoundries Deal Finalized.” *EE Times*, July 1, 2015. https://www.eetimes.com/document.asp?doc_id=1327029

Mak, Marie A. “Trusted Defense Microelectronics Future Access and Capabilities are Uncertain.” United States Government Accountability Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Armed Services, House of Representatives. October 28, 2015

Manufacturing USA. https://www.manufacturing.gov/funding

Marques de Sa, Isabel, “How DO You Build Effective Public-Private Partnerships?” Yale Insights, Yale School of Management. May 16, 2017. https://insights.som.yale.edu/insights/how-do-you-build-effective-public-private-partnerships

McFadden, W. Clark. 2012. "Praise for SEMATECH." *Issues in Science and Technology* 28 (4): 15-17.

Moore’s Law. www.mooreslaw.org

Mozur, Paul. "Plan for $10 Billion Chip Plant shows China’s Growing Pull." New York Times Company, https://search.proquest.com/docview/1866495792?accountid=322.

National Research Council Staff and Charles W. Wessner. December 27, 2012. *Government-Industry Partnerships for the Development of New Technologies: Summary Report*. Washington: National Academies Press.

Office of Management and Budget. FY18 Federal Budget, Research and Development. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_18_research.pdf

Office of Personnel Management, Federal Employment Reports. Data, Analysis & Documentation. https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/historical-tables/executive-branch-civilian-employment-since-1940/

Organization for Co-operation and Economic Development. *Public/Private Partnerships in Science and Technology: An Overview Background.* http://www.oecd.org/sti/scitech/introductionstireviewno23publicprivatepartnershipsinscienceandtechnology.htm

Platzer Michaela D. and Sargent Jr, John. “U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy.” Congressional Research Service. June 27, 2016.

President’s Council of Advisors on Science and Technology. “Report to the President – Ensuring Long-Term U.S. Leadership in Semiconductors.” January 2017. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf

Science & Technology, “The Chips Are Down”. The Economist. January, 4 2017. https://www.economist.com/news/science-and-technology/21734044-fixing-underlying-problems-will-take-long-time-two-security-flaws-

modern?cid1=cust/ddnew/email/n/n/2018014n/owned/n/n/ddnew/n/n/n/nna/Daily_Dispatch/email&etear=dailydispatch.

Sematech History. Sematech. 2013. https://web.archive.org/web/20130702191328/http://www.sematech.org/corporate/history.htm

Singer, P.W. "Hacked Hardware Could Cause the Next Big Security Breach", *Popular Science*, February 17, 2015, https://www.popsci.com/nowhere-to-hide#page-2

Singer, P.W. and Cole, August. "Ghost War: A Novel of the Next World War (New York: Houghton, Mifflin, Harcourt Publishing, 2015)

Stolk, Pieter. "A Public Health Approach to Innovation." Background Paper 8.1 Public Private Partnerships. World Health Organization. http://www.who.int/medicines/areas/priority_medicines/BP8_1PPPs.pdf

Strumpf, Dan, Khan, Natasha, and Rollet, Charles. "Surveillance Cameras Made by China are Hanging All Over the U.S." *The Wall Street Journal.* November 12, 2017. https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949?shareToken=st9a295d08b78c40349a46e455c5ea3b8b&reflink=article_email_share

SUNY Poly SEMATECH, SUNY Polytechnic Institute. 2017. https://sunypoly.edu/research/centers-programs/suny-poly-sematech.html

Trustable Access to Leading Edge Technology. Joint Working Group Team 2 White Paper. NDIA. July 2017. https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/tmjwg-documents/ndia-tm-jwg-team-2-white-paper-finalv3.ashx?la=en

The White House Office of the Press Secretary, *Obama Launches Competition for Three New Manufacturing Innovation Institutes*, May 9, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/obama-administration-launches-competition-three-new-manufacturing-innova

U.S. Department of Defense Manufacturing Technology Program. Manufacturing and Industrial Base Policy. https://www.dodmantech.com/initiatives/MIBP

U.S. General Services Administration. Background and History. https://www.gsa.gov/about-us/background-and-history