Program Research Project

SEMICONDUCTOR TECHNOLOGY AND U.S. NATIONAL SECURITY

BY

COLONEL LAWRENCE K. HARADA
United States Army Reserve

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
21-04-2010	Program Research Project	

4. TITLE AND SUBTITLE

Semiconductor Technology and U.S. National Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Lawrence K. Harada

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Colonel Patrick J. Cassidy
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

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

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The transfer of semiconductor technology from the U.S. to offshore locations, in particular, China, is a national security concern. In this globalization era, U.S. industries hail China as an enormous opportunity. Others, however, cast a suspicious eye on China's military modernization. Export policies to China's rising semiconductor capabilities are largely ineffective. Officials point to China's active involvement to secure a semiconductor infrastructure and the corresponding loss of U.S. semiconductor industry leadership. However, restricting the flow of semiconductor technology in the name of national security is unwise. Instead, the U.S. must provide the technical leadership to the U.S. semiconductor industry through innovative research and development. A viable solution must involve realigning semiconductor export policies, aggressively enforcing semiconductor intellectual property, streamlining the decision making process, and establishing U.S. government-run fabrication facility dedicated to semiconductor research, development, and manufacturing. America needs to establish its worldwide leadership in semiconductor technology in order to maintain a clear technological advantage over any peer competitor.

15. SUBJECT TERMS

China, Trojan Horse, unity of effort

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC PROGRAM RESEARCH PROJECT

SEMICONDUCTOR TECHNOLOGY AND U.S. NATIONAL SECURITY

by

Colonel Lawrence K. Harada
United States Army Reserve

Topic Approved By
Colonel Patrick J. Cassidy

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Lawrence K. Harada

TITLE: Semiconductor Technology and U.S. National Security

FORMAT: Program Research Project

DATE: 21 April 2010 WORD COUNT: 4,996 PAGES: 30

KEY TERMS: China, Trojan horse, unity of effort

CLASSIFICATION: Unclassified

The transfer of semiconductor technology from the U.S. to offshore locations, in particular, China, is a national security concern. In this globalization era, U.S. industries hail China as an enormous opportunity. Others, however, cast a suspicious eye on China's military modernization. Export policies to China's rising semiconductor capabilities are largely ineffective. Officials point to China's active involvement to secure a semiconductor infrastructure and the corresponding loss of U.S. semiconductor industry leadership. However, restricting the flow of semiconductor technology in the name of national security is unwise. Instead, the U.S. must provide the technical leadership to the U.S. semiconductor industry through innovative research and development. A viable solution must involve realigning semiconductor export policies, aggressively enforcing semiconductor intellectual property, streamlining the decision making process, and establishing U.S. government-run fabrication facility dedicated to semiconductor research, development, and manufacturing. America needs to establish its worldwide leadership in semiconductor technology in order to maintain a clear technological advantage over any peer competitor.

SEMICONDUCTOR TECHNOLOGY AND U.S. NATIONAL SECURITY

"It's a creeping crisis, and it's not something the American psyche responds to well. It's not a Sputnik shot …"

—Craig Barrett, Former Chairman, Intel Corporation[1]

The methodical migration of semiconductor technology to the People's Republic of China (PRC) is a national security concern. With the media focused on the network and software cyber attacks, Craig Barrett underscores one reason the U.S. continues to ignore the semiconductor technology[2] migration to the PRC. Due to disjointed and unresponsive actions on the part of various agencies, the U.S. government has repeatedly failed to protect and secure semiconductor technology. Semiconductor technology is a vitally important building block of the military's reliance on high technology. Without effective long-lasting solutions, the continued transfer of semiconductor manufacturing and intellectual property (IP) to the PRC has ominous consequences for U.S. national security.

The semiconductor industry began in the research laboratories of Bell Laboratory in the early 1950's with Department of Defense (DOD) Funding.[3] From those humble beginnings, today's $255 billion[4] semiconductor industry continues to fuel the information age. In this globalization era, U.S. industries hail China as an enormous opportunity. Others, however, cast a suspicious eye on China's military modernization. The ability to export freely while protecting military semiconductor technologies remains paradoxical. Export policies to counter China's rising semiconductor capabilities are largely ineffective. Officials point to China's active involvement to secure a semiconductor infrastructure and the corresponding loss of U.S. semiconductor industry

leadership. However, restricting the flow of semiconductor technology in the name of national security is unwise. Instead, the U.S. government must provide the technical leadership to the semiconductor industry through continued support of innovative research and development. To reach this end, a viable solution must involve realigning export policies, aggressively enforcing intellectual property rights, streamlining the decision making process, and establishing U.S. government-run fabrication facility (fab) dedicated to semiconductor research, development, and manufacturing. These actions will reestablish America's worldwide leadership in semiconductor technology and maintain a clear technological advantage over any peer competitor. A "whole of government approach" is required to synchronize the myriad of activities required to protect, encourage, and rekindle U.S. semiconductor leadership that is critical for U.S. national security.

A Seen and Unseen Threat

President Barack Obama stated, "It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day."[5] The visible threat is China, who has emerged even stronger and more nationalistic[6] from the global financial meltdown that still handicaps most nations today. At a conference on the People Liberation Army (PLA), Jason Bruzdzinski presented a paper that stated, "PLA analysts are carefully studying the vulnerabilities of U.S. weapons, platforms and military systems...to develop operational methods to counter technologically superior adversaries in a future war."[7] From the anti-satellite test in January 2007 to recent aggressive cyber attacks, Bruzdzinski's prescient

comments indicate that China may have other intentions than just being an economic power. The PRC's actions have changed from being a responsible member of the international community to a nation that "is focused not on the world but on itself."[8]

While China's efforts to expand its economic and military strengths are clearly visible, it is the unseen threat that concerns national security experts. One DOD concern is that advanced microchips will enhance the PRC modern weapon systems, another serious and underlying fear is the insertion of concealed "kill-switch circuitry" into DOD and intelligence agencies' acquired chips. The "kill-switch" circuitry, a semiconductor Trojan horse, is the most dangerous of sleeper cells and irregular warfare.[9] Two incidents, unconfirmed from government sources, indicate that employments of "kill switches" may have already occurred. It is alleged that during the Cold War, the Central Intelligence Agency (CIA) produced microchips with "kill switch" circuits and shipped them to the Soviet Union. The microchips failed as designed and resulted in a 3-kiloton explosion and destruction of a Siberian natural gas pipeline.[10] In 2007, IEEE Spectrum speculated that Israel deployed malicious circuits on a commercial off-the-shelf microprocessor that turned-off Syrian radar, thus enabling Israeli jets to bomb a suspected Syrian nuclear facility.[11] The assumption that DOD can simply buy commercial integrated circuits (IC) is precarious.

These compromised chips are "difficult to detect, and so dangerous to the nation."[12] The smaller the technology node (the smallest feature on an IC), the more difficult it is to detect "kill switches." For example, 250-nanometer technology used in most state of the art US military weapon platforms contains approximately 8 million transistors; today's leading integrated circuits contain over 2 billion transistors. The

likelihood of detecting a kill switch at 250 nanometers is difficult and at 22 nanometers is nearly impossible. The most modern of automated test equipment (ATE) can only verify "known" functionalities within each individual chip at rate of millions of transistors per second; ATE cannot detect "unknown unknowns."[13] Researchers at the University of Illinois concluded that malicious circuits are "more practical, more flexible and harder to detect."[14] This semiconductor Trojan horse is the unseen threat that gives the PRC the ability "to subdue the enemy without any fighting."[15]

Semiconductor Technology and National Security

America's National Interests, National Defense Strategy, and *National Military Strategy* highlight the importance of semiconductor technology to national security. Two related national interests interconnect China's rise with the semiconductor industry. *America's National Interests* identifies productive relations with China as a vital interest. An extremely important interest is to maintain a lead in "strategic technologies, particularly information systems"[16] of which semiconductor technology is the key component. Similarly, *The National Defense Strategy* stresses not only the importance of technology, but also to invest in "the right kinds of technology" [17] to stay ahead of potential adversaries. The *National Military Strategy* details the advantages of the networked force and the speed of information that implies extremely fast semiconductors.[18] The Defense Science Board (DSB) Task Force on High Performance Microchip Supply also concluded that national security depends upon the U.S.-based semiconductor competitiveness from research and development (R&D), design and manufacturing.[19] The guidance on the importance of semiconductor technology to

national security is unequivocal. Yet, DOD and intelligence agencies find themselves in a dilemma.

Semiconductor technologies that support U.S. national security also fuel the much larger worldwide economy. As a result, most semiconductor technologies for leading edge military applications arise from the commercial industry and not the military sector.[20] The importance of semiconductor technology to U.S. national security cannot be understated. Largely ignored as the intelligence inside U.S. military weapon systems, semiconductor technologies "provide the force multipliers that made the revolution in military affairs possible."[21] In *Joint Vision 2020*, semiconductor technology is the implied driver of the military transformation that will enhance the capabilities and the "revolution of joint command and control."[22] As the U.S. military moves to a network-centric force, the demands for extremely fast microchips will increase. DOD's Global Information Grid (GIG) requires high-speed connectivity, encryption, and decryption to support both weapon platforms and the soldier on the battlefield.[23] The ability to sustain and even surpass these high-speed requirements rests with the U.S. semiconductor industry.

Unfortunately, the PRC will be in a better position than the U.S. to manufacture the next several generations of microchips. This reversal of fortune is not by happenstance. As part of its strategic plan, China declared in 2000 with a "5 to 10 years' effort…. Domestic integrated circuit products will also satisfy most domestic demand and be exported as well while reducing the development and production technology gap with developed countries."[24] Today, China is on path to exceed this objective. With financial incentives from their government, Chinese semiconductor manufacturers have

an advantage over U.S. chipmakers. China's investment in semiconductor technologies is impressive. China will likely invest over $US 20 billion over the next five years in all semiconductor technologies.[25] This funding provides Chinese semiconductor manufacturers the necessary capital to build several state-of-art fabs and the capability to design leading edge chips.[26] China's incentives range from 5-year tax holidays to accelerated depreciation on equipment.[27] U.S. semiconductor manufacturers and industry consortia have requested the government for financial support to counter China's incentives that lure foreign investment to the PRC.

U.S. government financial support for semiconductor companies is problematic. The semiconductor industry requested what is essentially a creative fundraiser aimed at solving a complex military-industrial problem. The Semiconductor Industry Association (SIA) asked the federal government to match China's tax holidays, to allow U.S. companies to expense versus depreciating semiconductor equipment, and to reduce chipmakers' tax rates.[28] These incentives do not ensure that semiconductor manufacturing will remain in the U.S. nor do they ensure U.S. semiconductor leadership. One weakness of these financial incentives is they do not tie the desired "ends" of maintaining semiconductor leadership with the "ways" of shoring up U.S. semiconductor manufacturing. There are no assurances that tax law changes alone will motivate U.S. semiconductor firms to construct $3-5 billion fabs. In addition, even with financial incentives, U.S. manufacturers will likely continue to build where labor costs are low. Finally, the DSB's minority report states that the U.S. government's participation should be limited to the routine functions it already conducts for semiconductor industry, such as, the Defense Advanced Research Projects Agency's

(DARPA) R&D programs and the National Science Foundation (NSF) grants to university research. Instead of financial incentives, the U.S. government should provide the non-financial leadership "apparently missing in the semiconductor industry, to facilitate a better semiconductor industry long term strategic plan."[29]

Government non-financial leadership alone is not enough to encourage semiconductor companies to keep their manufacturing in the U.S. Since the DSB report, additional U.S. chipmakers have continued to shift production offshore, or have licensed leading edge technology to these foreign companies. DOD and intelligence agencies continue to lose secure access to their application specific integrated circuits (ASICs).[30] For example, in 2007, IBM licensed its 45-nanometer (the smallest feature on a microchip) complementary metal–oxide–semiconductor (CMOS) technology to Semiconductor Manufacturing International Corp. (SMIC), a PRC-backed company. Earlier, IBM licensed its 0.18-micron radio frequency (RF) CMOS technology to China's CSMC Technologies Corporation.[31] Up until mid-1990, semiconductor companies owned and operated the entire chip making supply chain from design, process development, fabrication, and assembly and test. The cost of constructing and maintaining fab prevented many IC designers from entering the business. To accommodate these entrepreneurs, the fabless-foundry model emerged. Most U.S. companies have transitioned to the fabless model where they focus on design and sales of their products and leave the fabrication of the chips to a semiconductor foundry who will fabricate the chip, usually in an area with a lower cost of labor. For the next several years, China will be that area of low cost production. This shift to fabless semiconductor model is a trend that will likely continue to offset the high capital costs of constructing a

new fab. Another problem that affects the number of domestic sources of microchips is chip companies perceive government as too bureaucratic and are reluctant to perform work for the government's specialized chips.[32] In a globalized market, U.S. chipmakers will pursue the most effective and efficient business solutions. They will require government intervention and its leadership in cases of IP protection and export controls.

The surge in Chinese semiconductor manufacturing and the corresponding decline in U.S. chip manufacturing are not entirely due to globalization. On one hand, China encourages foreign investments to promote a healthy economy. Proponents for engagement with the PRC tout semiconductor manufacturing and other economic ventures as way to bring the PRC into the international order as a responsible actor.[33] On the other hand, opponents argue that China does not abide by international trade rules that can disadvantage U.S. semiconductor manufacturers.[34] For example, less than 4 years after China's entry into the World Trade Organization (WTO), the U.S. Trade Representative (USTR) declared that China's theft of semiconductor IP reached "epidemic proportions."[35] U.S. semiconductor companies spend upwards to 22% of their annual revenues on R&D. [36] A loss of a U.S. semiconductor company's IP to another party has several financial impacts; lower revenues, unrecoverable R&D costs, loss of market share and litigation costs. A more serious concern, DOD and other agencies do not have any guidelines to prevent counterfeit parts from entering the supply chain.[37] China's IP violations create an unlevel playing field for semiconductor manufacturers and add another complex dimension to the national security issue.

The U.S. export control system is another factor that contributes to an unlevel playing field. However, calls for tighter export controls on semiconductor technologies

will not necessarily level the playing field. Free trade proponents argue that restricting semiconductor technology to China will more likely "damage than improve U.S. national security,"[38] since restrictions will impede economic growth. This situation highlights one complication associated with the migration of semiconductor technologies. On a larger scale, U.S. responses to China's semiconductor growth have been disjointed and perplexing. A lack of unity of effort of among governmental agencies coupled with the rapid advancement of semiconductor innovation, contributes to the decline of U.S. semiconductor technology leadership.

Lack of Unity of Effort

Unlike the unity of effort displayed by the PRC to secure a semiconductor infrastructure, "the U.S. government has never been able to provide such coordinated support."[39] On the issue of U.S. regulations for export controls, the problem stems from several causes. First, the primary federal departments, DOD, DOC and DOS, have overlapping and conflicting objectives that do not necessarily align with the export control system. Second, regulations and laws for control of dual-use exports cannot keep up with semiconductor technology's velocity of change. Third, U.S. efforts to restrict exports to China have repeatedly failed due to confusion on what semiconductor technologies need to be controlled. This lack of coordination and cooperation harms the U.S. semiconductor industry and U.S. national security. Today, the U.S. is experiencing the consequences of this lack of unity of effort.

Departments of Commerce, State, and Defense have overlapping and often conflicting objectives. DOC's objectives to advance technology[40] seem incongruous to the DOC's Bureau of Industry and Security (BIS) whose objective is to restrict

technological exports due to national security concerns.[41] The State Department advocates a prosperous international system,[42] but its Directorate of Defense Trade Controls (DDTC) controls the export of defense items in order to protect U.S. national security.[43] While the balance between foreign trade policies with national security may be appropriate, the semiconductor industry points to the overlapping of licensing authority in DOS and DOC[44] and their enforcement of a dated export control regime as hindrances to compete in the global market.[45] Interestingly, DOD's Defense Technology Security Administration (DTSA) reviews export licenses and only advises DOS or DOC.[46] DTSA has neither compliance nor enforcement authority. There is no lead organization or a centralized coordination center for export controls.[47] To paraphrase Army doctrine, unity of effort is paramount where there is no apparent lead organization.[48]

The slow methodical pace of government cannot keep up the rapid technological advancements. Supercomputers provide an excellent example of the difficulty that the U.S. government faces in keeping up with the velocity of technological developments where export threshold "had to be continually increased as technological and commercial realities have made prior levels obsolete."[49] For example, in July 1999, the export control threshold for supercomputers was 6,500 million theoretical operations per second (MTOPS). With the rapid advancement in semiconductor technology and the slow governmental approval process, this threshold became obsolete in only six months.[50] According to a GAO Report, DOD's Militarily Critical Technologies List (MCTL), which lists several semiconductor technologies, is out of date and not used, even by DOD's DTSA.[51] In order to remove certain export controls on semiconductor

technology, DOC conducts “foreign availability” assessments to determine if there are any such foreign sources of technologies, like semiconductor manufacturing equipment.[52] However, a 2002 GAO report discovered that manufacturers had not filed a foreign availability study in 25 years since “government’s prior effort to complete a study took several years and was outdated at issuance.”[53]

During the Cold War, the military funded the majority of semiconductor R&D, purchased a majority of the integrated circuits and controlled semiconductor exports. Today, semiconductors are a commercial and largely consumer-based industry, but the export restrictions of semiconductor technologies remain unchanged. Confusion among government agencies exacerbates the situation. DOD and DOC have not assessed what semiconductor technologies can be exported to China.[54] DOS and DOC continue to restrict the delay of the sale of semiconductor equipment, but ultimately grant an export license after a routine waiting period.[55] Dry Etch technology is an export control item. Etch systems create the nanometric lines on the most complex semiconductors. Shanghai's Advanced Micro-Fabrication Equipment (AMEC) is a competitor on the U.S. top semiconductor equipment maker, Applied Materials.[56] Since AMEC is not subject to export controls, it can deliver a system quicker than Applied Materials who will have to wait up to six months for an export license.[57] The lack of coordination among DOD, DOS and DOC hinders U.S. semiconductor companies from competing globally and does little for national security. On an international level, the lack of interdepartmental coordination is evident by the multinational export regime, Wassenaar Arrangement, on export controls for conventional arms and dual-use technologies. This international agreement does not hamper China’s ability to obtain semiconductor technologies. The

primary reason for this failure has been the lack of multilateral engagement where the U.S. “has not provided the strong leadership needed to make the system effective.”[58]

The result of the disunity of effort is the joint DOD and NSA’s Trusted Foundry Program (TFP). This program is a stop-gap measure to prevent malicious circuits from entering the semiconductor fabrication process – a 400-plus step manufacturing process that takes up to two months to complete. This program ensures DOD and intelligence agencies receive “trusted” microchips. The TFP exists because the US government approved the sale of SVG, a small U.S. chipmaker to a Dutch company ASM Lithography (ASML) and the sale of DuPont Photomasks to a Japanese company, Toppan Printing. The sale of these two companies left no reliable U.S. supplier in the photolithography market and only one marginal player in mask making equipment. These technologies provide semiconductor makers with the intricate nanometric patterns required to make a microchip. The mask-making component is “untrustworthy” under TFP.[59] Despite strong objections from DOD, the Department of Treasury’s Committee on Foreign Investment in the United States (CFIUS) allowed foreign entities to acquire these technologies. CFIUS is an inter-agency committee that consists of numerous U.S. departments and agencies, including the Defense, State, and Commerce departments.[60] The settlement to move the acquisition forward consisted of a trade-off. ASML agreed to spin off its subsidiary that supplied satellite parts to DOD.[61] In the short term, the U.S. prevailed. Unfortunately, in the long term, the U.S. lost. The lack of unity of effort among government departments of yesteryear contributed to the problem the nation faces today.

TFP is limited; DOD and intelligence agencies must still tap the commercial market for leading edge microchips. The trusted foundries currently under contract are not at the leading edge. For example, the first trusted foundry, IBM's Burlington, Vermont fab develops products at the 90-nanometer node on 200mm silicon wafers. However, IBM's state-of-art fab in East Fishkill, New York is at the leading edge of semiconductor technology – 22 nanometers fabricated on 300mm silicon wafers. While current weapon systems are using 250-nanometer or an early 90's semiconductor technology,[62] the GIG architecture and networking platforms require faster and denser chips. The trusted foundries cannot supply them. DOD must procure leading edge chips and system platforms from the commercial market. Intel, the world's largest semiconductor manufacturer declined to participate in the TFP[63], yet DOD will likely use Intel's powerful computer and network processors. The TFP is a stop-gap fix for a narrow band of microchips and it does not address leading edge semiconductor technologies.

Proposed U.S. Semiconductor Strategy

The complexity of the U.S. semiconductor industry problem spans multinational firms, government agencies, the U.S. military, and a potential peer competitor looming on the horizon. The "whole of government" approach used to integrate the efforts of the departments of the U.S. Government to achieve unity of effort in military operations is appropriate to support the proposed U.S. semiconductor strategy. The "ends" of this strategy formulation is ensuring U.S. semiconductor superiority. Since the rate of change in the semiconductor industry is roughly a two year cadence as dictated by Moore's Law, the proposed "ways" must be adaptive to this requirement. The

government's unity of effort must match the pace of semiconductor advancements. The collaboration of all the instruments of national power, diplomatic, information, military and economic (DIME) allows the government to "achieve unity of effort toward a shared goal."[64] Therefore, an appropriate U.S. semiconductor strategy is *to preserve America's semiconductor technology leadership to meet the challenges and opportunities of globalization.*

This semiconductor strategy is not without risk. Interagency and departmental competition will likely impede effective and efficient coordination.[65] In addition, government agencies tend to proceed in what is in their own interests. [66] The current slow and methodical pace of government action is a major gap between the ways and ends. Changes to accelerate the policy and decision making process are in order. To ensure "first access and assured access" to microchips the "ways" must include a government-run semiconductor fab that can meet the chip demands of DOD and intelligence agencies while providing a venue for a national center for semiconductor excellence, however, the resources may be difficult but not impossible to attain.

Sensible, flexible, and expedient semiconductor export control policy

The U.S. method of export controls for the semiconductor industry is out-dated, slow, and fundamentally flawed. Semiconductor export controls were appropriate during the Cold War where DOD initially funded semiconductor R&D to provide components to the Minuteman II.[67] Today, government departments lean on the side of caution and continue to enforce outdated semiconductor export controls. The delays that U.S. chipmakers must endure hurt their ability to compete economically against foreign companies. These delays contradict the *National Security Strategy* that touts free

markets and free trade that will stimulate global economic growth.[68] The contradictory actions make it difficult to pursue multilateral consensus on semiconductor export controls. Unity of effort is required of the Departments of State, Defense, and Commerce to achieve the desired results. Representatives from all three departments working together with private industry can best determine if an export license is required, approved, or denied. Working together on a common issue should expedite the process that has frustrated the semiconductor industry.

A sensible approach for multilateral export regime controls is for the U.S. to work with the international community to revise the restrictions on semiconductor equipment that is plaguing the effectiveness of the Wassenaar Arrangement. The United States is the sole member that repeatedly denies China's acquisition of semiconductor technologies outlined in the Wassenaar agreement.[69] Unfortunately, other countries do not agree that these technologies should be restricted. Therefore, foreign suppliers continue to jump in to make the sale leaving U.S. companies with a financial and market share loss. Rather than pursuing the issue unilaterally, the U.S. should apply soft power in an attempt convince the Wassenaar members to restrict exports or opt to acquiesce on the export controls that are clearly not dual-use. The result should be a balance between U.S. economic competiveness and national security.

Aggressive enforcement of semiconductor IP violations

U.S. fabless semiconductor companies' greatest concern is the loss of IP on their product designs. Strict enforcement of U.S. semiconductor IP will level the playing field. According to trade group Semiconductor Equipment Materials International (SEMI), IP violations range from patent infringement, theft of core technologies and

counterfeiting.[70] Counterfeit military-grade chips potentially entering the DOD supply chain greatly affect national security. The USTR, a 120 person cabinet level agency, is responsible for trade-related intellectual property protection.[71] A coordinated effort among chip companies, DOD, DOC, DOS and USTR is required to protect both private industry and national security. Unity of effort stands a better change for a favorable outcome from the WTO for these IP violations.

Streamlining the Decision making process

The decision making process for U.S. semiconductor export controls and IP protection issues will need to match the pace of semiconductor advances. Semiconductor technology is shrinking faster than the export regulatory agencies can revise the export nets. The ability to review and to approve regulations and policy changes in a single organization would improve effectiveness.[72] However, unity of effort among the different government departments and agencies working in tandem with industry can improve both effectiveness and efficiency.[73] U.S. semiconductor manufacturers have a valid concern that their offshore competitors have a competitive advantage from the slow-moving U.S. regulation of semiconductor technology exports.[74] The decision-making mechanism for semiconductor export control must match the pace of technological advancement. A new system of export controls and IP protection measures must be more agile and effective.

Actions to streamline decision-making involve a “whole of government” approach. This approach is appropriate since coordination among the agencies is emphasized “to ensure that the full range of available capabilities are leveraged, synchronized, and applied toward addressing”[75] complex problems associated with the semiconductor

industry. To achieve the broad success envisioned in a whole of government engagement, all must be integral to unified action. As such, DOD and intelligence agencies should actively participate in decision making with other departments and agencies that affect the semiconductor industry.[76] As recommended by the *Beyond Fortress America* committee, the government should establish a coordinating agency to handle all aspects of export control licenses to streamline the licensing and decision-making process.[77] A shared repository for IP violations improves the communications among agencies to prevent counterfeit parts from entering the government supply chain.[78]

These practical solutions only attempt to re-level the playing field for US semiconductor companies. Although export control, IP protection, and efficient decision-making are reasonable solutions, DOD and NSA's "first access, assured access" for microchips cannot remedy the problem. U.S. trusted foundries are incapable of fabricating state-of-art semiconductors and their numbers are dwindling. In order to maintain a trusted long-term supply of integrated circuits, to encourage R&D, and to re-establish its leadership in semiconductor technology, the U.S. government must operate its own semiconductor fab. This government owned fab will be dedicated to semiconductor research, development, and manufacturing for all critical government semiconductor needs.

Dedicated U.S. Operated Semiconductor R&D and Manufacturing Fab

Acquiring and operating a semiconductor fab is a logical and prudent option for the U.S. government. To protect, in particular, DOD and intelligence agencies' past, present and future high technology weapon platforms, a national center for

semiconductor R&D and manufacturing is vitally necessary. A government owned fab safeguards and hedges against future migration of semiconductor manufacturing to offshore locations. A state-of-art government fab eliminates the need for antiquated government production fabs operated by NSA, DOD and other agencies. A government fab is the most effective means of regaining semiconductor leadership. By gaining recognition as a semiconductor center of excellence, the center for semiconductor excellence becomes a magnet to attract innovative minds geared towards research and development.

The TFP fails to address the next generation of DOD and intelligence agencies needs. Trusted foundries are several generations behind today's leading edge solutions. The U.S. can no longer rely on the commercial semiconductor market for its advanced chip-making capability. The TFP validates and approves U.S. based fabs to supply the government with secured access to microchips. However, since the TFP does not address the issues of export controls, IP protection, and more importantly, the continued migration of semiconductor manufacturing to offshore locations, it is only a short-term fix. A government fab provides DOD and intelligence agencies a short and long-term source of trusted microchips and hedges against the continued migration of semiconductor manufacturing to offshore locations.

Believing they could simply purchase ICs from the commercial market, government agencies failed to modernize the very few fabs under their control. Moreover, the presumption that cost was prohibitive contributed to the stagnant state of these fabs.[79] A reasonable assumption is NSA's 20,000 square foot fab is inadequate to produce its specialized chips; otherwise, NSA would not be a joint partner of the TFP.

The Defense Microelectronics Agency (DMEA) provides DOD with chips that are no longer in the supply chain and its fab is limited to chip production that the commercial market no longer provides.[80] Neither fab has the capability to produce leading edge chips. Consolidation of the government's R&D and manufacturing through a dedicated government-run fab eliminates the need for production fabs operated by NSA, DOD and other agencies.

A properly operated and maintained government fab can serve as the channel through which semiconductor research reaches out to both private and educational institutions while at the same time meeting the government's national security requirements. This dedicated government fab is the most effective means of regaining semiconductor leadership. Research universities' top-notched technical programs can enrich their R&D through a collaborative relationship with an identifiable government fab. A government fab enhances the already coherent R&D system among industry, universities and government.[81] If R&D follows manufacturing as the experts posit, then a national center for semiconductor excellence is a necessary first step to encourage R&D to remain in America.

Sputnik jarred the nation into becoming the world's technological leader. Today, there are no significant technological events, just a steady quiet migration of semiconductor technology to the PRC. The paths of U.S. semiconductor industry and national security are destined to intersect to an unfavorable outcome. One path leads to a significant lost of semiconductor leadership and the other leads to a potential attack on the nation's information infrastructure. If the government continues to regard the nation's security on the economic growth of the U.S. semiconductor industry, then the

U.S. needs to re-level the playing field, encourage unity of effort among the relevant government agencies, and create a national center for semiconductor R&D and manufacturing. Failure to act along both avenues of approaches will lead a crisis that the American psyche responds to well, but it may be too late.

Endnotes

[1] Task Force on the Future of American Innovation, *The Knowledge Economy: Is America's Losing its Competitive Edge?*" February 16, 2005, 16, www.futureofinnovation.org/PDF/Benchmarks.pdf, (accessed February 11, 2010).

[2] The terms semiconductor technologies, integrated circuits, microchips and chips are used interchangeably.

[3] National Research Council, *Securing the Future: Regional and National Programs to Support the Semiconductor Industry*," Charles W. Wessner, ed., Washington, DC: National Academies Press, 2003, 1.

[4] Gartner says Worldwide Semiconductor Revenue in 2010 to Rebound to 2008 Levels, *Gartner Newsroom*, November 16, 2009, http://www.gartner.com/it/page.jsp?id=1228116 (accessed April 10, 2010)

[5] Barack H. Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," (Washington DC, The White House,, May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/, (Accessed April 3, 2010)

[6] John Pomfret, "Newly Powerful China Defies Western Nations," *The Washington Post*, March 15, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/14/AR2010031400368.html (accessed April 2, 2010).

[7] William R. Hawkins, *Testimony before the U.S. China Commission Hearing on U.S. Export Controls*, March 17, 2006, 3.

[8] Francis Fukuyama, "What Kind of World Power China Will Be?," as shown on Fora TV, University of Sydney, Sydney, Australia, May 28, 2008, http://fora.tv/2008/05/28/Francis_Fukuyama_American_Foreign_Policy_After_Bush#Francis_Fukuyama_What_Kind_of_World_Power_China_Will_Be (accessed March 1, 2010)

[9] Clark and Levin.

[10] William Safire, "The Farwell Dossier," The New York Times, February 2, 2004, http://www.nytimes.com/2004/02/02/opinion/02SAFI.html?pagewanted=1, (accessed April 2, 2010)

[11] Sally Adee, “The Hunt for the Kill Switch,” IEEE Spectrum, May 2008, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0 (accessed November 30, 2009)

[12] Wesley K Clark and Peter L Levin, “Securing the Information Highway,” Foreign Affairs, Nov/Dec 2009, Vol 88, Issue 6, in ProQuest (accessed April 2, 2010)

[13] Clark and Levin.

[14] Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhow, “Designing and Implementing Malicious Hardware,” University of Illinois, http://www.cs.uiuc.edu/homes/kingst/Research_files/king08.pdf, (accessed April 19, 2010).

[15] L.J. Fullenkamp, “Battle-Centric Theories,” briefing slides with scripted commentary, Carlisle Barracks, PA, U.S. Army War College, September 8, 2008, slide 5.

[16] The Commission on American’s National Interests, *America’s National Interests*, Cambridge, MA: Belfer Center for Science and International Affairs, 2000, 6.

[17] George W. Bush, *The National Security Strategy of the United States of America* (Washington, DC: The White House, March 2006), 19.

[18] Richard B. Myers, *The National Military Strategy of the United States of America* (Washington, DC: The Pentagon, 2004), 16.

[19] Defense Science Board Task Force, *High Performance Microchip Supply*, (Washington, DC: OSD/AT&L, February 2005), 8

[20] National Research Council of the National Academies, *Beyond “Fortress America” National Security Controls on Science and Technology in a Globalized World*, (Washington, DC 2009), 1, http:/books.nap.edu/catalog/12567.html (Accessed February 14, 2010)

[21] Ibid, 17.

[22] Henry H. Shelton, *Joint Vision 2020*, (Washington, DC: The Pentagon, June 2000), 3.

[23] Joseph I. Lieberman, “White Paper: National Security Aspects of the Global Migration of the U.S. Semiconductor Industry,” June 2003, 2.

[24] Daryl Hatano, “Fab America – Keeping U.S. Leadership in Semiconductor Technology,” Presentation, August 27, 2003, slide 20.

[25] Lily Feng, “China Semiconductor and PV Market Overview,” Presentation at SEMICON Japan, December 2, 2008, slide 5, http://www.semi.org.cn/img/video/ppt/ 200812100959389055.pdf (accessed March 21, 2010)

[26] Ibid.

[27] Hatano, slides 21 and 27.

[28] George Scalise, "China's High Technology Development," *Testimony before the U.S. China Economic and Security Review Commission*, April 21, 2005, http://sia.mini.browsermedia.com/galleries/press_release_files/testimony_china_050421.pdf, (accessed February 14, 2010)

[29] Defense Science Board Task Force, *High Performance Microchip Supply*, 103.

[30] Richard McCormack, "It's Like Putting a Band-Aid on A Bullet Hole," Manufacturing News, Vol 15, No. 3, Feb 28, 2008, http://www.manufacturingnews.com/news/08/0228/art1.html, (Accessed March 29, 2010)

[31] Mark LaPedus, "Is IBM Handing Over Key IC Technology to China?" EE Times, October 19, 2009, http://www.eetimes.com/showArticle.jhtml?articleID=220700109, (Accessed October 25, 2009).

[32] Bureau of Industry and Security, *Defense Industrial Base Assessment: U.S. Integrated Circuit Fabrication and Design Capability*, (Washington, DC: Department of Commerce, May 2009), 10.

[33] Adam Segal, "Practical Engagement: Drawing a Fine Line for U.S.-China Trade," *Council on Foreign Relations*," http://www.cfr.org/publications/7063/prctical_engagement.html. (Accessed October 26, 2009)

[34] Wayne Morrison, *China-U.S. Trade Issues*, (Washington, DC: Congressional Research Service, May 16, 2009), 12.

[35] Hawkins, 3.

[36] Scalise.

[37] Bureau of Industry and Security, *Defense Industrial Base Assessment: Counterfeit Electronics*, (Washington, DC: Department of Commerce, January 2010), ii.

[38] James Lewis, *Export/Dual Use Technology and Technology Transfer Issues*, Center for Strategic & International Studies, Washington, DC, January 17, 2002, http://csis.org/testimony/export-controlsdual-use-technology-and-technology-transfer-issues, (Accessed October 26, 2009)

[39] Lieberman, 5.

[40] Department of Commerce Home Page, http://www.osec.doc.gov/omo/dmp/default.

[41] Bureau of Industry and Security, Department of Commerce, "Guiding Principles of the Bureau of Industry and Security," http://www.bis.doc.gov/about/bisguidingprinciples.htm, (accessed April 14, 2010).

[42] Department of State Home Page, http://www.state.gov/s/d/rm/index.htm

[43] Directorate of Defense Trade Controls homepage, Department of State, http://www.pmddtc.state.gov/index.html

[44] Ian F. Fergusson, *The Export Administration Act: Evolution, Provisions, and Debate*, (Washington, DC: Congressional Research Service, July 15, 2009), 19.

[45] Karen Murphy, *Testimony Before the House Committee on Foreign Affairs Field Hearing on The Impact of U.S. Export Controls on National Security*, Washington, DC, January 15, 2010, http://www.internationalrelations.house.gov/111/mur011510.pdf, (Accessed February 1, 2010).

[46] Defense Technology Security Administration Home Page, http://policy.defense.gov/sections/policy_offices/dtsa/index.html

[47] Ibid.

[48] U.S. Army Department of the Army, *Operations*, Field Manual 100-5 (Washington, DC: U.S. Department of the Army, June 1993), 2-5

[49] Semiconductor Industry Association, "Press Release: Export Controls, Semiconductor Industry Applauds Report of Export Controls," June, 8, 2001, http://www.sia-online.org/cs/papers_publications/press_release_detail?pressrelease.id=618 (Accessed March 30, 2010)

[50] Leslie D. Simon, "The Net: Power and Policy in the 21st Century," *The Global Century: Globalization and National Security*, ed. Richard Kugler and Ellen Frost, Washington DC National Defense University, Chapter 28, 626. http://www.ndu.edu/inss/books/Books_2001/Global%20Century%20-%20June%202001/globcencont.html, (Accessed February 10, 2010)

[51] U.S. Government Accountability Office, *Defense Technologies: DOD's Critical Technologies Lists Rarely Inform Export Control and Other Policy Decisions*, (Washington, DC: U.S. Government Accountability Office, July 2006), 11.

[52] U.S. Government Accountability Office, *Export Controls: Rapid Advances in China's Semiconductor Industry Underscore Need for Fundamental U.S. Policy Review*, (Washington, DC: U.S. Government Accountability Office, April 2002), 25.

[53] Ibid.

[54] Ibid, 4.

[55] Michael Santarini, "Export Rules Hurt U.S. Firms," Electronics Design, Strategy, News, July 1, 2006, http://www.edn.com/article/CA6348055.html (Accessed October 26, 2009)

[56] Karen Murphy, *Testimony Before the House Committee on Foreign Affairs Field Hearing on The Impact of U.S. Export Controls on National Security*, Washington, DC, January 15, 2010, http://www.internationalrelations.house.gov/111/mur011510.pdf, (Accessed February 1, 2010).

[57] Santarini.

[58] Hawkins, 6.

[59] Brian Sharkey, "Trust in Integrated Circuits Program," (Washington DC, Defense Advanced Research Projects Agency, March 26, 2007) Slide 11, http://www.darpa.mil/mto/Solicitations/baa07-24/Industry_Day_Brief_Final.pdf, (Accessed November 29, 2009)

[60] Committee on Foreign Investment in the United States (CFIUS) Home Page, http://www.cfius.us/.

[61] Lieberman, 9.

[62] Defense Science Board Task Force, *High Performance Microchip Supply*, 62.

[63] McCormack.

[64] U.S. Army Department of the Army, *Stability Operations*, Field Manual 3-07 (Washington, DC: U.S. Department of the Army, October 2008), 1-4, 1-5.

[65] Nora Bensahel, *International Perspectives on Interagency Reform"* Testimony presented before the House Armed Services Committee, Subcommittee on Oversight and Investigations on January 29, 2008, 8.

[66] Ibid.

[67] Jan Rabaey, "The International Semiconductor Roadmap and Its Impact on Semiconductor-related Research,"slide 10, http://www.scribd.com/doc/21382993/The-International-Semiconductor-Roadmap-and-Its-Impact-on-Semiconductor-Related-Research, (accessed November 29, 2009).

[68] Bush, *National Security Strategy*, 1.

[69] U.S. Government Accountability Office, *Export Controls: Rapid Advances in China's Semiconductor Industry Underscore Need for Fundamental U.S. Policy Review*, 17.

[70] SEMI, "Innovation is at Risk as Semiconductor Equipment and Materials Industry Loses up to $4 Billion Annually Due to IP Infringement," http://www.semi.org/en/Press/P043775, (accessed April 2, 2010)

[71] Christina Sevilla of the United States Trade Representative, Army War College Washington DC Visits, June 24, 2010.

[72] William Keller and Janne Nolan, “Proliferation of Advanced Weaponry: Threat to Stability,” *The Global Century: Globalization and National Security*, ed. Richard Kugler and Ellen Frost, Washington DC National Defense University, Chapter 27, 804. http://www.ndu.edu/inss/books/Books_2001/Global%20Century%20-%20June%202001/globcencont.html, (Accessed February 10, 2010)

[73] Ibid.

[74] Murphy.

[75] U.S. Army Department of the Army, *Stability Operations*, Field Manual 3-07 (Washington, DC: U.S. Department of the Army, October 2008), 1-17.

[76] Defense Science Board Task Force, *High Performance Microchip Supply*, 59-60

[77] National Research Council of the National Academies, *Beyond “Fortress America” National Security Controls on Science and Technology in a Globalized World*, 6.

[78] Bureau of Industry and Security, *Defense Industrial Base Assessment: Counterfeit Electronics*, iii.

[79] U.S. Government Accountability Office, *Defense Microelectronics: DOD-Funded Facilities Involved in Research Prototyping or Production*, (Washington, DC: U.S. Government Accountability Office, March 2005), 12.

[80] Defense Microelectronics Activity homepage, http://www.dmea.osd.mil/home.html.

[81] Daffel Frear, “Globalization of the Electronic Materials Industry,” Freescale Semiconductor, February 14, 2005, www.tms.org/pubs/journals/JOM/0506/Frear-0506.pdf, (accessed February 2, 2010).