Engaging Science, Technology, and Society 1 (2015), 1-24 DOI: http://dx.doi.org/10.17351/ests2015.001

Regulating the Academic "Marketplace of Ideas": Commercialization, Export Controls, and Counterintelligence[1]

JOHN KRIGE[2]
Georgia Institute of Technology

Abstract
Two revolutions, not one, are transforming the research enterprise in American academia. One is the commercialization of research. The other is the regulation of research by the national security state that was accelerated by the terrorist attacks of 9/11 and focuses increasingly on the risk of sensitive knowledge leaking to China and other countries of concern. Commercialization temporarily restricts knowledge circulation to secure a patent for personal and institutional gain. Regulation controls the flow of knowledge to select foreign nationals using multiple instruments, including export controls, along with informal surveillance by the FBI. Ironically, the neoliberal urge to roll back the state and commercialize research in a competitive global knowledge economy exposes the American academic research system to the risk of "industrial" espionage and rolls out the regulatory apparatus of the national security state. Alongside offices of technology transfer on campus we now have offices of export control and compliance. Faculty and graduate students have accommodated themselves to this new situation, even while they regret it; many are concerned by the challenge that it poses to academic freedom, intellectual dynamism and political openness.

Keywords
national security state; deemed exports; FBI; academic research; knowledge circulation

Introduction
Two revolutions, not one, are transforming the research enterprise in American academia. The first, which has been extensively and critically studied, is the commercialization of research facilitated by the neoliberal state (Kleinman and Vallas 2001; Mirowski 2011; Slaughter and Rhoades 2004). The second, barely recognized by scholars in the humanities and social sciences, is the regulation of research in science and engineering by the National Security State (NSS). The

[1] This work was supported by NSF Standard Research Grant SES 1230220.
[2] John Krige, Email: john.krige@hts.gatech.edu

first, which is generally traced back to legislative measures in the 1980s that shifted global competitiveness to the center of research policy, has unleashed the entrepreneurial sprit of the individual researcher and served as a vector for the dissemination of corporate culture on campuses. The second, building on challenges to university autonomy in the late cold war period and gaining further traction after the terrorist attacks of 9/11, has led to a tightening of export control and other regulatory legislation that is reinforced by an alliance between universities and the American Federal Bureau of Investigation (FBI). It has produced a regime that is profoundly transforming interactions between American researchers and foreign students and peers. The first restricts the free circulation of knowledge to protect intellectual property (IP) for personal and institutional gain. The second restricts the free circulation of knowledge to protect the US's economic and military security from global threats. Both are institutionalized. The commercial exploitation of academic research has spawned offices of technology transfer to help universities secure patents and negotiate licensing agreements with industrial partners. The government regulation of the production and circulation of knowledge on campuses is entrusted to trained export control officers and their legal advisers. They have established their own Association of University Export Control Officers (AUECO) to monitor proposed changes to the legislation that impacts the conduct of research on campuses. Their numbers are growing. Over the last few years, for example, an AUECO list-serve hosted by the University of Ohio has grown to include over 250 members representing over 100 academic organizations, colleges, and universities (AUECO, 2015).

This paper challenges the dominant narrative, that sees the "neoliberal" university as dominated by market forces, by exploring the role played by the NSS in shaping the practice of research in American academia today. First, I describe the historical evolution of the current policy framework beginning in the 1980s, which has adapted legislative instruments that were developed in the early cold war period (Daniels 2013; Dobson 2002; Masco 2014) to changing threats to American security. This is followed by a brief case study of how life at a government-regulated research environment at a major US science and engineering school (the Georgia Institute of Technology) is characterized by my informants who work there. The argument emphasizes that the protective cocoon that was put around academic research in the late cold war period has been steadily undermined by an expansion of the reach of the NSS in the 2000s. That expansion was initially driven by new legislation following the attacks of 9/11 and the need to contain the risk of sensitive knowledge leaking through the open sieves of research universities that could be exploited by "rogue states" and terrorists (especially in biotechnology). It was expanded in order to take defensive measures against countries like the People's Republic of China (China hereafter) that aggressively sought to acquire advanced knowledge to fuel its research system (and that paid scant attention to the international IP-regime). Universities were not only urged to track foreign nationals from "countries of concern." Indeed, the Departments of State and of Commerce increasingly demanded compliance with export controls on knowledge circulation with foreign nationals. The FBI launched an Academic Alliance Program to alert faculty to the dangers posed by university openness. An informal level of surveillance was

added to the administrative machinery, which now impacts the daily face-to-face interaction of research faculty and graduate students.

The case study draws on a set of interviews with thirty subjects, including faculty, students and administrators. The questions were informed by my extensive period of training in export control legislation and procedures. The study was restricted to unclassified knowledge. Most of the formal interviews were transcribed, and the identities of the interviewees have been suppressed. The transcriptions will be made available publicly through the Georgia Tech library at the end of the project.

The data reveal that the university community has adapted to government regulation of the circulation of knowledge, which they find onerous but unfortunately necessary. And while many of them remain dedicated to their missions as teachers and mentors, those in certain sensitive fields (like aerospace, computer science and information technology, robotics and new materials) must monitor the circulation of knowledge in their classrooms and laboratories when regulations apply. Indeed, as the commercialization of academia pushes the results of research closer to the civilian market and/or the military field, so the threats to national economic and military security become more palpable. To the need not to share knowledge publicly in order to protect IP is added the need not to share knowledge with foreign nationals in order to secure compliance with export controls. This poses challenges to academic freedom (Evans and Valdivia 2012), which are briefly touched on in the concluding remarks.

The National Security State as Driver of Technological Innovation Post-1980

Recent STS historical accounts of the commercialization of US academia sidestep the role of the NSS in technological innovation and its increased use of export controls and counterintelligence to pre-empt the leakage of sensitive knowledge abroad after 9/11. Typically, the rise of "academic capitalism" is framed by reference to the emergence of Japan as a major economic competitor, the end of the cold war, and the passage of the Bayh-Dole Act and related legislation in the 1980s—exemplars of the new neoliberal socio-economic paradigm that sought to roll back the state to make room for the free play of market forces and individual entrepreneurship. Bayh-Dole authorized universities to commercialize the results of federally-funded research, which was previously regarded as a public good. As one comparative economic indicator after the other pointed to the US's "decline" relative to Japan's rising economic power in the 1980s, enthusiastic researchers in some fields, notably in the emerging and fecund area of biotechnology, saw an opportunity to recapture lost economic ground (Beatty 2000; Rasmussen 2014; Vallas, Kleinman and Biscotti 2010). By some accounts, universities were transformed from "repositories for wisdom" into "profit centers for the generation of intellectual property" (Mirowksi and Sent 2002a, 10). Now little more than "temples of mammon," they redefined their mission to satisfy a "neoliberal blueprint for a vibrant 'marketplace of ideas' responsive to corporate concerns" (Mirowski 2011, 35). The discourse of superpower competition between two world systems that supported R&D to win the war against communism was replaced by an

equally "heroic" narrative that justified spending on science and technology to secure US leadership in a competitive global knowledge economy (Slaughter and Rhoades 2002, 70).

"The collapse of the national security imperative" (Mirowski and Sent 2002a, 26) to support R&D, and the reduction of the role of the state to a mere facilitator of unregulated entrepreneurial activity, was never as complete as this implies. On the contrary, to meet the Japanese threat the concept of national security was actually stretched to include the maintenance of economic competitiveness. This legitimated researchers in weapons labs like Los Alamos who, propelled by the Technology Transfer Act of 1986, became actively engaged in exploiting the commercial potential of the human genome project (Beatty 2000). It was also a response to the deep penetration of Japanese (civil) industry into the US military procurement system. In the early 1990s, a study by the Department of Commerce found Japan to be ahead of the US in five of twelve emerging technologies, and to be rapidly gaining ground in another five (Huntington 1991). Of particular concern was growing Japanese domination of the semiconductor market and its implications for defense. A report to the Council on Foreign Relations noted that in the 1991 Persian Gulf War "more than 20 of the weapon systems used in the war, including the F-15, F-16 and F-18 fighters, were built with foreign transistors and microchips" (Romm 1993). This dependence led some well-placed observers to conclude that "the same kind of effort we mounted to achieve technological superiority in the military area must now be mounted to integrate our military technology with commercial activities, to translate our edge in basic research and innovation into competitive and marketable high-tech products […]" (Sorenson 1990). Of course, the private sector still had the primary responsibility for developing, producing and marketing new products and processes. That obstacle could be bypassed, however, by conceding that "national security can no longer be viewed exclusively in military terms; economic security and industrial competitiveness [were] also vital considerations" (Romm 1993).

Expanding the definition of national security to embrace economic competitiveness also chimed with the new emphasis on the production of dual-use (civil and military) technologies through which the Department of Defense (DoD) could benefit from economies of scale on the commercial market. The DoD emphasized this in its specification of the twenty-one critical technologies it wanted to see developed in 1991 (Department of Defense 1991). Interdependence and dual-use were two key characteristics of its list. For example, advanced microelectronic circuits were needed for sophisticated computer architectures, which were, in turn, needed for innovations in simulation and modeling, computational fluid dynamics, signal processing, machine intelligence, and so on. Moreover, no less than fifteen of these critical technologies were both "vital" to DoD missions and had "significant commercial applications or potential." Indeed, all fifteen "corresponded closely to one or more of the technologies highlighted in the Department of Commerce's 1989 list of emerging technologies […]." The paper also noted that the trend to convergence between the two spheres, military and commercial, was likely to become more pronounced as advanced weapons systems relied increasingly on information technologies.

These empirical snapshots—they are no more than that—confirm that the National Security State has always been and remains a major driver of transformative technological innovation in the US (Block & Keller 2010; Weiss 2014). The market did not entirely replace it as a source of innovation in the 1980s. Rather, with the restructuring and consolidation of the major defense industries in the post-Vietnam period, and their inflexibility in the face of the "information revolution," the NSS turned to small firms to pursue R&D in generic technologies that meet military (or more generally "security") needs and respond to commercial opportunities. By fostering hybrid public/private research initiatives, it sought to secure US global technological leadership without falling foul of the traditional anti-statism that characterizes the US political system. Firms that successfully commercialized new dual-use products and processes drew attention away from the role of the NSS as a driver of transformative innovations that met military needs. Particularly since the 1980s, bipartisan political support in a "neoliberal climate" was secured by a strategy in which the NSS identified the emerging fields that mattered to US technological pre-eminence, engaged industry in "innovation hybrids" needed to bring ideas to fruition, and then stepped back to allow corporate collaborators to commercialize "dual-use" civil and military products and processes. There was no sharp rupture between the neoliberal and the cold war innovation regimes. Rather, their coexistence was facilitated by combining the technological vision of NSS funding agencies with new opportunities for entrepreneurship (in both universities and federal research centers) and the dynamism of American small businesses and venture capitalists.

In summary, Mirowski suggests that the IP-related stream of legislation enacted in the 1980s was intended to extricate "the government from previous Cold War science management as a prelude to turning over responsibility to the corporate sector" (Mirowski 2011, 22). My aim in this section has been to challenge that idea. I stress that the traditional cold war patrons of science and technology creatively adapted to new legislative opportunities in order to link transformative, long-term basic and applied science to market and to field, by parsing economic decline as a threat to national security and highlighting dual-use research projects. Put differently, there is a symbiosis between commercialization and national security, a tight coupling between producing transformative knowledge that both benefits from the economies of scale in a civilian market and gives rise to new widgets for the military.

Changing NSS Restrictions on Knowledge Circulation: A Brief History from the Late Cold War to the War on Terrorism

In the past three decades, the United States "has developed a sophisticated and complex innovation system in which the government plays an absolutely central role" (Block 2010, 3). Its protection of the associated national scientific and technological assets in a competitive international environment calls forth a complex regulatory apparatus to restrict knowledge flows. The commercialization narrative foregrounds the IP regime, but engaging with national (military and economic) security demands attention to multiple other forms of control. Classification and travel restrictions on foreign visitors traditionally restrict scientific openness.

Export regulations obstruct firms' access to foreign markets. The scope of both was revised to meet the changing global environment that was confronted by the American research system beginning in the 1970s.

The proximate cause of alarm in the late cold war period was a backlash against the liberalization of trade with the Soviet Union as occasioned by détente. By the end of the 1970s, the Soviets were able "to produce miniature ball bearings for intercontinental missiles, used American computers in their air-defense system, and Western firms were providing equipment and experience to aid the Soviet Union in developing chemical and biological weapons" (Lippert 2009, 198). In April 1981 the Reagan administration published the first of several glossy books entitled *Soviet Military Power* in anticipation of its promotion of a space-based defense system, or Strategic Defense Initiative (SDI) (Prados 2009, 91). It claimed that US-sponsored scientific exchanges and academic scientific communication practices, including the entire professional and open literature, had enhanced Soviet military strength. In an open letter published in *Science* in January 1982, Deputy Secretary of Defense Frank Carlucci gave multiple examples to confirm that the Soviets were using official scientific contacts with the US "in a highly orchestrated, centrally directed effort aimed at gathering the technical information required to enhance their military posture" (Carlucci 1982). A couple of months later, the Assistant Secretary of Commerce made the same point with even more emphasis:

> Operating out of embassies, consulates, and the so-called business "delegations" KGB operatives have blanketed the developed capitalist countries with a network that operates like a gigantic vacuum cleaner sucking up formulas, patents, blueprints and know-how with frightening precision (Brady 1982).

This network, he went on to say, exploited the "soft underbelly" of America's open society, including the "desire of academia to jealously preserve its prerogative as a community of scholars unencumbered by government regulations" (Brady 1982). This was a major new threat to academic freedom. At the time the "prevailing presumption within the US campus science community was that, [unless research was protected] it was open to observation, discussion and participation by students and professional peers, at the discretion of those principally responsible for its performance" (Relyea 1994, 117). This presumption was now under assault. Organizers of conferences being attended by researchers from the communist bloc had to withdraw invitations at the last minute to avoid being fined for violating government regulations. Visas were denied to foreign nationals who had planned to visit American campuses. By 1984 self-censorship was increasing. Some sessions in conferences and even some university courses were restricted to US citizens (Relyea 1994).

In response to these concerns, the Department of Defense and the National Academies set up a panel on Scientific Communication and National Security to evaluate the situation particularly as it applied to universities. Dale Corson, President Emeritus of Cornell University chaired the panel. The "Corson Report," as I shall call it, was published in fall 1982 (Corson 1982). The Panel recognized that the Soviet Union and its satellites had legally and illegally acquired a wide variety of dual-use technologies from the West in many sensitive areas. But they were

skeptical that the universities were to blame for this. Indeed, "discussions with representatives of all US intelligence agencies failed to reveal specific evidence of damage to US national security caused by information obtained from US academic sources." The Panel concluded that "*in comparison with other channels of technology transfer, open scientific communication involving the research community does not present a material danger from near term military implications"* (emphasis in the original) (Corson 1982, 41; Macrakis 2004). It opposed the pursuit of security by secrecy, advocating instead security by accomplishment. That is, it argued that national security lay in consolidating the US's scientific and technological pre-eminence that in turn required it to take full advantage of an open research system that fostered international scientific communication. These recommendations were enshrined in a policy directive that spun a protective cocoon around fundamental research on campuses (to be discussed below) and that temporarily liberated universities from major regulatory scrutiny.

During the 1990s there were growing concerns about knowledge in specific fields circulating too liberally, and to the US's disadvantage. James Watson, one of the discoverers of DNA and then director of the NIH's Center for Genome Research, notoriously accused Japanese researchers of being "free riders," exploiting open basic research done in the US to advance their national biotech industry (Beatty 2014; McGourty 1989). But it was China that really caught the headlines. During his second term, President Clinton's efforts to renormalize trade relations with Beijing, which had been disrupted by the Tiananmen Square massacre, came under heavy fire in a Republican-dominated Congress. In June 1998, a nine-man bipartisan Committee chaired by Chris Cox (R-California) was set up to investigate whether sensitive missile or space technology had been released to the PRC by two space satellite operators, Hughes Space and Communications and Loral. Both had advised Chinese engineers on the causes of the launch failures of their Long March rocket (Krige et al. 2013). In October 1998, the Cox Committee's inquiry was extended to include alleged lapses of security and espionage at America's three nuclear weapons laboratories (Los Alamos, Lawrence Livermore, and Sandia). A classified version of their report was submitted to the President in January 1999. When the declassified version was released a few months later, Cox was quoted as saying that "No other country has succeeded in stealing so much from the United States," with serious and ongoing damage to the country. House Majority Leader Dick Armey, throwing caution to the winds, stated publicly that "It's very scary, and basically what it says is the Chinese now have the capability of threatening us with our own nuclear technology" (Cirincione 1999).

As if to confirm the point almost simultaneously, Wen Ho Lee, a 60-year old Taiwan-born American nuclear physicist working at Los Alamos, was fired and later indicted by a federal grand jury on fifty-nine counts alleging that he had transferred sensitive data to unsecured computers and tapes at the lab. He was accused of releasing the "crown jewels" of the US nuclear weapons program, information that could "change the global strategic balance" (Anon 2004). Wen Ho Lee was later exonerated of all but one of the charges brought against him. Hughes and Loral, by contrast, admitted guilt and were fined heavily.

The attacks in September 2001 called forth a major expansion of the powers of the National Security State. As Masco puts it, the declaration of the national counter-terror state in

2001 was modeled on the invention of the national security state in 1947, with its "designation of new insecurities, new institutions to fight them, a public mobilization campaign grounded in fear and, above all, official claims that a new kind of war […] was a multigenerational commitment, constituting a new mode of everyday life rather than a brief intensity of conflict" (Masco 2014, 5). Like the cold war national security state before it, that "new mode of everyday life" comprises an always-on-alert global infrastructure of preparedness to meet external threats to the United States and its citizens (Lakoff 2006). During the cold war this goal was defined by the policy of Mutually Assured Destruction (MAD). The "counter-terrorist state" defines a state of preparedness more broadly as pre-empting a wide range of dangers, rather than just a nuclear attack, before they materialize. New legislation, including the Homeland Security Act and the Patriot Act, was passed to protect the nation. The Bureau of Export Administration in the Department of Commerce was significantly renamed the Bureau of Industry *and Security* in 2002. In defining "the health of the US economy and the competitiveness of US industry" as a national security issue, it transformed universally used practices of industrial espionage (with ever more sophisticated technologies and techniques) from "business as usual" into a threat to the homeland (BIS n.d.).

Control over the circulation of knowledge became a major priority. An extensive program was undertaken to reclassify documents in the national archives and presidential libraries, some of them dating back to World War I (Masco 2014, 9). The "mosaic theory of intelligence," which holds that "disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information," began to be used more aggressively by federal agencies (Pozen 2005). The scope of the "gray" category of Sensitive But Unclassified (SBU) Information was also expanded to cover a vast range of information previously in the public domain but now deemed of potential use to terrorists. Confusion reigned: employing ad-hoc, agency-specific policies, procedures and markings for SBU information, by 2010 the executive branch was using more than 100 different procedural regimes to deal with it (CUI 2011). A typical critique of the Department of Energy's use of the SBU category complained that "The Department's official definition is so broad as to be unusable. ...There is no ... common understanding of how to control ... [SBU] ... no meaningful way to control it that is consistent with its level of sensitivity, and no agreement on what significance it has for US national security" (Knezo 2006, 40). In response to these kinds of criticisms, a major new initiative has been taken to standardize the way the Executive branch restricts unclassified information (now called Controlled Unclassified Information), better to enhance communication within the system.

In sum, the terrorist attacks of 9/11 created a climate of fear that paved the way for the "counter-terror state" to massively extend the government's control over knowledge circulation with little public opposition. Universities were directly impacted. As one administrator explained, the SEVIS program, which monitors foreign students in the US for national security purposes, "went to a new level after 2001 […]." Now "universities had to start doing monthly reporting on what students are doing, in terms of whether they are enrolled in their classes and whether they're still on campus and what courses they are taking and whether they're making

progress." The government demanded increased compliance with export control regulations. The FBI initiated a new Academic Alliance Program that offered to help protect sensitive knowledge from leaking from campuses. This climate of hypersecurity posed new challenges to longstanding mechanisms that had been in place to protect the research system from government regulation, notably the Fundamental Research Exclusion.

The Fundamental Research Exclusion (FRE) and its Critics

A policy devised during the late cold war period, and stimulated by the findings of the Corson panel, still serves as a benchmark for the protection of academic openness today. It was officially formulated in President Reagan's National Security Decision Directive (NSDD) 189. This directive affirmed that "The strength of American science requires a research environment conducive to creativity, an environment in which the free exchange of ideas is a vital component" (NSDD189 1985). To that end NSDD189 carved up the knowledge field into two broad and familiar domains: classified information and openly published fundamental research. And it stated that "to the maximum extent possible, the products of fundamental research were to remain unrestricted." Fundamental research was defined as follows:

> "Fundamental research" means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

The pertinence of this Fundamental Research Exclusion (FRE) was confirmed unofficially by National Security Adviser Condoleezza Rice soon after the terrorist attacks of 9/11. In explaining her position, Rice emphasized that "open and collaborative basic research" led to scientific innovation, US technological pre-eminence, prosperity, military superiority and national security.

The FRE nominally created a space for universities to pursue research without having to worry about the knowledge leaking to foreign nationals to the detriment of US economic or military security. It is indifferent to the *process of knowledge production* focusing only on the *product*. A project falls within the FRE if its results are published openly, no matter how they were acquired (e.g., using the most advanced equipment on the market), whether or not they are dual-use, and of course, without regard to who was engaged in the research. As one lawyer recently put it, "The FRE is intended to provide this huge bubble around the activity on the campus, not to differentiate on the basis of technology, not to differentiate on the basis of nationality of the people involved" (Dong 2014). That said, many argue that the FRE is far too lax to deal with the current threats to the US, which call for tighter restrictions on knowledge circulation in academia. Three features of the current research system aggravate the dangers (Evans and Valdivia 2012).

First, there is the change in the nature and source of funding that pushes research closer to the "D-end" of the R&D spectrum. American industry has soared ahead of the government as a funder of R&D, very little of it for basic research: in 1985 its contributions were roughly the same ($58b and $53b) whereas by 2009 industry contributed more than two-thirds of national R&D expenditure ($247b compared to the $124b of the federal government). The federal government for its part is also aggressively financing research that is "transitional" and can be commercialized, e.g., through its new NSF I-CORP program and the more established SBIR (Small Business Innovation Research) and STTR (Small Business Technology Transfer) programs. These are public/private initiatives that use federal money to stimulate the corporate sector to commercialize cutting-edge research, specifically in partnership with a research institute such as a university, if they seek STTR funding (SBIR 2015). Changes in citation practices in patent applications confirm the shift to the "D-end" along the R&D spectrum. Prior to the 1980s patent applications that cited "prior art" referred predominantly to other patents. Increasingly these citations reference scientific or technical articles. Indeed, the average number of such articles cited per US patent has increased from about 0.4 in 1987 to 2.0 in 1997, a five-fold increase in a decade. Increasingly, basic knowledge no longer flows primarily among scientific communities but is also strongly coupled "to circuits that connect it to knowledge application and the corporate world" (Slaughter and Rhoades 2004, 312). Graduate students thus learn to do cutting-edge research that is destined for application in the market or the military field.

Second, there is the changing position of the US in the global economy. If in the 1980s the main threat to US scientific and technological pre-eminence came from Japan, today its leadership is challenged on many fronts. As one official report put it, in the latter half of the 20th century the US "was preeminent in many, probably most, fields of scientific and engineering endeavor. Today," it went on, "the United States is but one among a number of nations or groups of nations competing for leadership across the spectrum of scientific and engineering disciplines" (Deemed Export Advisory Committee 2007, 11). Some of them, like China, have aimed to "catch up and surpass" the US since the 1950s, and remain determined to do so.

Finally, there are the changing demographics of the graduate student community in science and engineering (S&E) itself (NSF 2012). In the two decades beginning in 1989, students from four Asian countries/economies (China, India, South Korea and Taiwan, in that order) earned more than half of US S&E doctoral degrees awarded to foreign students (122,200 of 223,200). China's growth has been phenomenal: over the same twenty-year period the number of S&E doctorates earned by Chinese nationals in the US increased by nearly six times. After stabilizing at about 2,500 annually at the turn of the century it soared to a peak of 4,500 in 2008. Most of these degrees were awarded in engineering, biological sciences, and in physical sciences. In the past it could be hoped that these graduates would stay on in the US. This is no longer the case. In 2008 the Chinese authorities launched the "1000 Talents" program aimed at the most outstanding members of its educated elite overseas. By summer 2011 about 2,100 of these gifted Chinese had returned home (Zweig 2013). Taken together, these three elements buttress the claim that America is not only training its own competitors but that universities are actually imperiling

its economic and national security by allowing foreign nationals, notably those from China, to do advanced research that is close to application.

The risk of sensitive but unclassified knowledge leaking abroad has led sponsors to subvert the FRE by inserting "troublesome clauses" in contracts that invalidate it by restricting publication (Norris n.d.). They have also curtailed the access of designated foreign nationals to the research site (so ensuring that the results are not "shared broadly"). In short, the boundaries of the FRE bubble are not fixed nor are they clearly drawn: they are constantly negotiated between the research community, their sponsors and the government, which struggle to agree on how to strike a balance between national security and the openness of academic research. Regulating deemed exports has been one of many important sites of that struggle.

Regulating Knowledge Flows: Deemed Exports

Soon after World War II the federal government put in place two major bodies of legislation to regulate the export of sensitive items by the United States to foreign countries. One, the International Traffic in Arms Regulations (ITAR) that is administered by the Department of State, deals with military items and defense services as specified on the US Munitions List (Krige et al. 2013; Skolnikoff 2001). The other, the Export Control of Act of 1949, was followed by the Export Administration Acts of 1969, 1979, and 1989, and is administered by the Bureau of Industry and Security (BIS). The BIS applies the Export Administration Regulations (EAR) and decides whether or not to grant a license for an item on the Commerce Control List (CCL). This is an evolving compendium of about 2,400 dual-use items that is under constant revision (Ferguson 2007). It includes things like mass spectrometers, infrared sources and detectors, gas turbine engines, numerically-controlled machine tools and genetically modified organisms that have specific properties.

Deemed exports are a particular mode of control under the EAR (Evans and Valdivia 2012; Krige 2014; Reppy and Felbinger 2011). The regulations here invoke concepts that stretch the meaning of "technology" and "export" in non-intuitive ways. Firstly, they control the flow of "dual-use" *knowledge.* It is not only the export of products and processes that can be subject to controls. Secondly, the knowledge that is controlled can be embodied in many different forms—products and processes, but also blueprints, drawings, photographs, plans, written or recorded instructions, computer software and documentation, engineering designs and specifications, manuals, as well as "know-how." Thirdly, to "export" does not simply mean to pack a widget in a box and to ship it. Instead, "technology" can also be "released" for export a) when it is made available to foreign persons for visual inspection; b) when it is shared orally; and/or c) when it is transmitted by practice or application under the guidance of persons with knowledge of the technology. Finally, and obviously related to this, to "export" does not necessarily mean to send abroad. It also means to pass on knowledge to an *individual,* not a country, more precisely to a foreign person. What is more, that exchange can occur *anywhere*, including in the US: you don't have to be on foreign soil for a "release" of "technology" to count as an export. For legal purposes

it is assumed that the individual will return to her or his country—hence the export is "deemed" to have taken place.

In 2004 the Inspectors General of several government departments with international responsibilities, in consultation with the Directors of the CIA and the FBI, wrapped the BIS over the knuckles for not ensuring compliance with deemed export legislation in industry and academia (Inspector General 2004). The Inspectors also criticized the FRE as a major regulatory loophole, particularly because it allowed foreign persons to use controlled technology during their research as long as the results were "ordinarily published." This flexibility pivoted on the contested interpretation of one word in the definition of "use" in the EAR. To use equipment in the EAR means to be engaged in its "Operation, installation (including onsite installation), maintenance, repair, overhaul and refurbishing." Universities interpret the "and" inclusively, claiming that anyone is only "using" equipment if *all six* conditions are met simultaneously. The Inspectors wanted the "and" changed to an "or," on which reading a license would be needed to perform *any one* of the six listed activities.

In June 2005 the university export control officers collectively made a firm plea to the BIS not to implement these suggestions (Phillips 2005). They "would eviscerate the fundamental research exclusion" and "alter the whole context of university fundamental research in critical ways." They insisted that the interpretation of the FRE in the current EAR "must include the right for foreign students and researchers to use, alter and create, and to receive information on how to use, alter and create, controlled equipment while conducting fundamental research." Anyway, it would be immensely time-consuming and costly to make a complete inventory of sensitive research equipment on university campuses and to apply for deemed export licenses to use it when the number of items could run to 50,000, 70,000 or more. Faced with this opposition, the BIS has backed down, at least for the time being.

The Inspectors General also wanted tighter criteria for the access of foreign nationals to controlled technology (apart from those from 22 "Designated Countries" like the U.K., Australia, Canada and New Zealand and many countries in Europe, who do not require a license). In fact, an application for an export license to employ a foreign national from an embargoed country or a country of concern should include, in addition to normal professional data and country of citizenship, personal details such as whether he/she has strong ties to the US (e.g., family, home ownership, etc.) and/or intends to become a US citizen. It should also specify the ties the foreign national has to his/her country of origin (Orr 2014). These considerations are not definitive, of course, but they are part of the interagency assessment of "the potential threat that might be posed by a foreign national who is the subject of a license application and whose loyalty is uncertain" (Deemed Export Advisory Committee 2007). This is particularly true of foreign persons from Iran, Iraq and North Korea of course, but also China, India and Pakistan.

Deemed export regulations strike at the heart of the face-to-face circulation of knowledge, and when coupled with concerns about the "loyalty" of foreign nationals they raise the specter of an intrusive and menacing NSS apparatus that was all too familiar in the late 1940s and 1950s (Wang 1996). Now, as then, the fear that sensitive useful knowledge will leak into nefarious foreign hands to the detriment of US national security explains the presence of the FBI

on campus.

Counterintelligence: The FBI

After 9/11 the FBI redefined its role from being a law enforcement agency to being a "national security and law enforcement" agency, simultaneously moving its focus from being "case-driven" and "domestic" to being "threat-driven" and "global" (Masco 2014, 34.) Characterizing its core mission as "mitigating risk" it sought to pre-empt the acquisition of sensitive knowledge that could harm national security—particularly the dangers posed by a terrorist or rogue state armed with a bio-WMD.

Consistent with its new emphasis on pre-emption, the FBI has taken some unusual steps to contain the threat of bioterrorism, collaborating with scientists themselves to monitor research that may pose a national security threat. A California-based grassroots community exploring DNA sequencing, DIYbio, attracted the attention of the FBI who feared that the informal research network might publish information that posed a security risk. The Agency teamed up with the leaders of the project to "mitigate […] risks and gaps" in their research. It even financed (in collaboration with the American Association for the Advancement of Science, the US Department Health and Human Services, and the Department of State) a synthetic biology conference in 2009 that brought the science and security communities together to "promote a culture of responsibility" (Lempinen 2011).

This spirit informs its activities on American campuses. The FBI emphasizes that "the open environment of a university is an ideal place [for foreign intelligence services] to find recruits, propose and nurture ideas, learn, and even steal research data […]" (FBI 2011, 3). Its Academic Alliance Program offers a range of services that includes protection against bio-terrorism and "Animal rights and ecoterrorism" (FBI n.d.). It watches for the theft of intellectual property and it helps defend the campus from cyberattacks, mostly from China (reported to be in the millions per week) (Pérez-Peña 2013). And it draws its net wide to include very generalized concerns about knowledge leakage (e.g., foreign agents may seek to acquire "technologies during the research and development phase regardless of classification, since the application and new research may later become classified" (FBI 2011). It also invites faculty and staff to pass on information to the authorities if they see "suspicious incidents" on campus.

The FBI's Academic Alliance Program includes a National Security Higher Education Advisory Board (NSHEAB), established in 2005. This Board brings together the apparatus of the national security state (the CIA, FBI, DoD, etc.) with about twenty university presidents and chancellors. In 2010 its membership included representatives from UCLA, NYU, SUNY, Carnegie Mellon, Cornell, Duke, Northwestern, and Georgia Tech. Its stated goal is to prevent the theft of sensitive research at American universities. It is impossible to know how active the FBI is or what nefarious activity it successfully pre-empts. Suffice it so say, though, that Rice University President David Leebron, himself a member of the NSHEAB, recently remarked, "There's a real tension between what the FBI and CIA want to do and our valid and necessary international

openness" (Golden 2015). At the very least, then, we can say that these two agencies of the NSS are calling for action that challenges traditional American academic and political values.

Anecdotal evidence indicates the breadth of the FBI's engagement with campus life. It holds town-hall meetings for engineering faculty and staff in order to alert them to the dangers of illicit knowledge acquisition. It contacts individual science and engineering faculty and offers to help them protect their research. It approached one of my graduate students who was program chair of an international STS conference and asked her to keep an eye on the Chinese participants at the meeting (Did they attend all sessions? Did they disappear mysteriously?). One agent presented a paper restricted to US citizens and permanent residents at a national conference of academic export control officers, informing them of the multiple technological strategies used to acquire information illicitly.

The freedom of research authorized by the FRE stands in stark contrast to the range of concerns that animate an NSS that sees all research as a potential target for illicit foreign exploitation, that takes national security to cover both economic and military security, and that seeks to defend the campus pre-emptively against the leakage of sensitive knowledge to countries of concern. As one research faculty member who has had extensive contact with the security services explained to me "we live in an environment where there are risks. We live in an environment where there are people who are very, very aware, of what can literally go on in the mountains of Afghanistan or some other remote places." Many faculty members are not aware of these dangers so that "[…] there are all of these technologies where, in your world you think why in gods name would you control this, and in their world they know exactly why he would control it." Denied detailed knowledge of these deep secrets (Pozen 2010), but accepting that the danger is real, inflates "a not-yet-existing but potentially catastrophic danger to such a degree that it overwhelms all other concerns" (Masco 2014, 152). It forbids a critical scrutiny of the risks involved that would require divulging the knowledge in question, it removes control over its circulation from the research community, and it consolidates their compliance with the mechanisms put in place by the NSS to police the circulation of knowledge on campuses. There is no doubt that the US research system is vulnerable to external threats; the question is how best to contain the risks without violating the fundamental principles of openness that energize it and that are celebrated as hallmarks of the political system in which it is embedded. It is impossible for the academic community to debate that question rationally as long as the risks are shielded behind a wall of silence.

Living with Export Controls: A Brief Case Study

University faculty prize their role as teachers. To that end the administration and sponsored Principal Investigators (PIs) do all they can to keep their research free from government regulation by exploiting the FRE. As a result, no more than perhaps 5-10% of sponsored contracts deal with sensitive but unclassified knowledge that is subject to export controls or related restrictions. These are typically in fields like aerospace, new materials and computing and information technology, as well as biotechnology. However, even if the number of programs

directly affected is small, the reach of export controls is wide. MIT faculty members are advised that "If you collaborate with people in other countries, your emails are exports. When you travel, you're exporting everything you take with you" (MIT 2014, 64). Anyone who leaves the US on university business has to confirm that their laptop computers do not have sensitive files on them. Many are issued clean computers instead. Everyone doing cutting-edge sensitive research is careful about what they say for fear of sharing unauthorized information with foreign nationals.

From the outset some major research universities have affirmed their deep concern about the threat to academic openness and non-discrimination imposed by export controls and other government regulations. MIT has been particularly proactive in this regard. As early as June 2002, an Ad Hoc Faculty Committee on "Access to and Disclosure of Scientific Information" affirmed scientific openness as a guiding principle and proposed policies to reconcile it with national security when needed (MIT 2002). Distinguished MIT political scientist Gene Skolnikoff devoted his Branscomb Lecture in 2001 to the dangers of ITAR (Skolnikoff 2001). MIT President Charles Vest spent one of his 2005 Clark Kerr lectures discussing the threats of the new regulatory regimes to academic freedom (Vest 2007). In fact, MIT strives to keep its main campus as a completely separate teaching and research space within the FRE bubble; restricted research is done off-campus where it was forced to move in response to anti-Vietnam war protests in the 1960s. Many other universities, including Georgia Tech, do not map the FRE onto a separate geographic space, but mingle controlled and exempt research on the same site.

Beginning in about 2004, Georgia Tech's relatively low-profile administrative procedures to manage knowledge flows were, like those on many other campuses at that time, expanded considerably. New machinery was gradually put in place to ensure compliance with federal regulations on knowledge transfer. Today it is based in the Office of Research Integrity Assurance (ORIA), along with other regulatory activities, e.g., ensuring compliance with ethical standards of conduct in research.

The system in place to evaluate whether or not a sponsored project is subject to export control involves about a dozen people, some for only part of their time. Three or four administrators in the ORIA are there to ensure that all research faculty and students show due diligence in the conduct of their research and respect the restrictions imposed on the circulation of knowledge, if there are any. Three lawyers (and external consultants) assist in making legal judgments as to whether or not a particular research project is subject to the constraints imposed by the ITAR or the EAR. Four or five researchers act as Export Control Coordinators. In 2014, they were located in the College of Computing, the School of Aerospace Engineering (two), and the Georgia Tech Research Institute, which has extensive classified contractual relationships with the government and industry. The ORIA buys between a quarter and a half of their time to provide the technical advice needed by administrators, lawyers and faculty alike to assess the pertinence of the restrictions defined in ITAR's US Munitions List and EAR's Commerce Control List to their research project. My empirical study targeted senior officials in ORIA, the export control coordinators, departmental administrators, lawyers, senior researchers and graduate students.

To respect what many faculty believe to be the fundamental mission of the university—teaching and research—every effort is made to work within the FRE bubble. At the same time, faculty are torn between their wish to work in this open, regulation-free environment and the recognition that their research is increasingly vulnerable to what amounts to industrial espionage (given how close their work is to application/commercialization). As one senior scientist and research manager put it, "If you were a Chinese spy or you were trying to figure out how to get US technology, how would you go about it? [...] The technology-centric institutions in the US are very, very, very, very open organizations from which there is leading-edge technology that is much, much easier to access" than through companies like IBM. Georgia Tech is "somewhere in the group of ten leading technology-focused institutions." So if you were in Pakistan or China, wondering where to send to people, "Tech is top of that list." Statistically, the numbers are small: "One-tenth of one percent of all people do something stupid and bad. [But then] we have four thousand international students on campus, and one-tenth of one percent is four students, and that's about what we saw every year, and that is cyber threats, students on campus performing in clearly active ways to do things that they shouldn't be doing that caught the attention of various organizations outside of Tech. […] And most were Chinese." One of his colleagues implied that the Chinese threat was more general than that: "They're overtly doing everything they can to steal everything they can," he said.

Faculty accept the need for regulations, even if they regard them as "unwieldy, unmanageable, unmanaged, out-of-control, to the point where it's severely stifling innovations, severely stifling the ability for companies to be competitive, severely stifling the mission, the role of the university to develop and disseminate knowledge." A Technology Control Plan (TCP) is required whenever a project does not fall under the FRE. The TCP establishes whether or not there is a foreign national on the project, and asks how communication will be controlled in both physical and cyber space. Will there be separate rooms, restricted access, locked doors? Will data be stored on servers, jump drives, emails?

American students working on basic science projects that may eventually have dual-use civil and military applications have to be hived off from foreign nationals in their own groups. "The computers that we're using are dedicated to this project. They're physically located in a room that's been inspected by, again, somebody from this … security infrastructure at Georgia Tech. The door is locked. The student closes the door when he works on the project. There are issues about the computer equipment that we use for this, so we don't carry around memory sticks or hard disks with data, and certainly not outside of the country."

Physical segregation is complemented by self-censorship. A faculty member will tell his graduate student: "This is what you can talk about. You don't need to show that piece of hardware. The data that comes from that device need not be shown." Applications are particularly sensitive. He explained that, when talking about their research on, say, photonic crystals, the student "can discuss in very basic scientific terms, use the same words, I suppose, that other scientists working this area can use, but he can't, or at least I have told him not to talk about the applications […], who is the sponsor or what they're going to use this for." This compartmentalization defines the terms on which the graduate must collaborate with foreign

students in the same group. As his supervisor explained, "I actually have a visiting student from China […] who is working also on photonic crystals related insofar as the basic science goes, and there's almost a firewall between these two people. I mean, I really can't send her to talk to my own graduate student beyond just the most basic things."

This self-censorship permeates the research environment. It calls for vigilance in the classroom when there are foreign nationals present. "I just finished teaching a class on the science and design of gas turbine combustors that are used for military and civil commercial engines, and there are times when something might pop into your head from research, 'Well we'd better just move on.' You might want to bring it up but you just self-censor."

It affects one's relation with peers, especially if they are Chinese. I was told that if one is asked to evaluate a paper from China submitted for publication to an IEEE journal it is preferable to restrict your remarks to pointing out errors and avoid making specific suggestions for improvement. One can say "This is a well-explained phenomenon," or "Equation 7 doesn't really converge like you say it does." But one must "avoid the sharing of insights you may have from your own research about how this paper could be made better. You don't need to go there if you don't have to." There is little opposition. We're "kinda beaten into submission," one senior engineer told me. And that, by three levels of fear: personal, institutional and geopolitical.

In terms of personal ruin, one important feature of the export regime is that penalties for infraction are a personal, not an institutional, responsibility: the individual who willfully violates dual-use export control laws, for example, can be fined up to $250,000 or imprisoned for up to ten years, or both. Indeed, one professor from the University of Tennessee has just completed a four-year jail sentence for violating export control regulations by recruiting Chinese and Iranian students to work in his plasma laboratory on a new device for improving the performance of drones (Golden 2012).

There is also fear that the institution will lose its ranking as a secure site for doing sensitive research, and therefore lose its external funding. "It's not the fine; it's our institutional integrity," an export control officer said. "We would lose so much more than those fines in our credibility as a research institution, in our ability to do research and get funding for our research. […] And our faculty would say, 'Hey, look, if I can't get my research funding I am out of here.'"

Finally, there is fear that the leak of a controlled item might jeopardize the economic or military security of the US without one realizing it. "It's a scary world out there. People ask 'Do you realize what could happen if someone got that piece of information?' We don't want them to get that piece of information. We don't even want them to know what that piece of information is. We cover it…you know, we have people who are trying to do really, really, really bad things to us."

What of the graduate community? Some are not concerned about the regulated environment in which they study: "Science will still continue to march forward no matter what, no matter what regulations are in place." Others are less sanguine. They object to the discriminatory access imposed by ITAR that splits projects and hives off sensitive/interesting work that only American nationals can do. As one French student said, it was "almost degrading" to have to do research on what was left after American students were allocated the

more cutting-edge work in a NASA project. "We come to the United States to bring something to you, and you are rejecting us because we are not US citizens." A Costa Rican student put it differently: "I am the kind of person who, if someone's working on something, I like to ask, 'Hey, tell me what you are doing.'" Yet, if he asks someone who is on an export controlled project, he knows that the answers will be incomplete: "and I think it's a challenge for you as an engineer to come to terms with the fact that even though you're being trained and that you're paying for school and that you are all hired by the same institution […] you don't have the same opportunities." Discrimination on the basis of nationality also distresses some of the American graduate students. One American's "knee-jerk" reaction to Chinese students being watched more closely than others was "extremely negative. […] It sounds like a misguided attempt at tightening up security for people who may or may not be responsible. I mean, there's a lot of these cases where it's not a Chinese national who steals the information, its somebody else […]" even if it eventually winds up in China. An American student who worked on an ITAR project for his first three years deplored the fact that he could not share knowledge with foreign students: "They're being treated like lesser citizens of our research community for sure." He was embarrassed by the fact that he had his own secured office as a first-year graduate student, while fifth-year foreign nationals writing theses were crammed into public cubicles. He regretted that as a new graduate he could not benefit from insights of some of the brilliant senior Indian students since he could not talk to them about his research. And he surmised that standards in the program were actually dropping so that more and more Americans could be admitted to avoid the export control regulations. Eventually he moved over to a new FRE project that allowed him to publish freely and to speak about his work at conferences and thereby expand his career options. "I can say without reservation that working on an ITAR project is not a smart decision for a graduate student if you want to be tenured faculty someday," he wrote, though it might help those who wanted to work in industry.

As we can see, at least some of the graduate students I interviewed were outspoken about discrimination on the basis of nationality in the research space. It divided their cohort and undermined open communication. From both principled and pragmatic points of view, some found government regulations on sensitive but unclassified domains regrettable and counter-productive. For them, the "universalistic," nondiscriminatory norm of science was not simply a "traditional" value to be aspired to, but rather essential to maintaining standards, stimulating exchanges and improving career options. Classification was the only acceptable way to control knowledge flows—in which case, some argued, the research should not even be done on a university campus in the first place.

Concluding Remarks

Over the last decade or more American research universities have functioned in a context quite different to the regulation-free environment that was put in place in the 1980s. This is due both to changes in the nature and context of research practice itself and to the reconfiguration of the NSS after 9/11 to meet the terrorist threat. The standard literature on the commercialization of

research, with its emphasis on the rise of neoliberalism, misses the ongoing presence of the national security state as a driver of transformative technological change. It also ignores the new dangers after 9/11 that the NSS seeks to pre-empt through the implementation of government restrictions on the free circulation of knowledge to select foreign nationals in sensitive fields of research.

It is by "following the money" that the limits of the neoliberal model of university research funding emerge. True, industry is the major funder of R&D *nationally*, but not of *university* R&D (where the federal government's contribution has climbed steadily over the last two decades and is consistently about eight-fold more than industry's.) Beginning in the 1980s, the NSS tailored its patronage to promote phased dual-use research projects that broke new ground, it encouraged coupling between research institutes like universities and the corporate sector, notably small businesses, and it stepped back to allow commercially promising new military and civilian technologies to be exploited for profit (sometimes lending a hand by providing venture capital). Highlighting the role of the private sector in bringing breakthroughs to the market secured bipartisan support for a decentralized and somewhat covert form of industrial policy that relied on government initiative and oversight upstream. The dynamic role played by the state in defining promising research trajectories was masked by the "neo-liberal" rhetoric surrounding the explosive growth of firms in key sectors like biotechnology and their contribution to enhancing US competitiveness in the global market place.

Growing concerns about the leakage of military and sensitive dual-use technologies to China in the late 1990s produced calls for tighter controls on knowledge circulation that were amplified many times over by the terrorist attacks of 9/11 and the anthrax scare a week later. The counter-terror national security state that was put in place was erected on institutional and affective foundations built during the cold war. The control of knowledge and information was given new urgency by the need not only to pre-empt another unexpected and lethal attack on American soil by a terrorist or rogue state with a WMD but also to ensure the nation's economic and military security in an increasingly competitive global knowledge economy. Research moved closer to the D-end of the R&D spectrum, pushed by the urge to commercialize, exposing increasing numbers of foreign nationals to cutting-edge science and technology that could readily be exploited to the detriment of the US's economic pre-eminence or military advantage once they returned home.

The twin exigencies of *stimulating transformative scientific and technological innovation* and *regulating the circulation of knowledge* produced new challenges for an entrepreneurial research system that was founded on the principles of openness and international exchange. American scientific and technological leadership both depended on, and was increasingly threatened by, the circulation of knowledge in the global "marketplace of ideas." Universities that had successfully pushed back against the government regulation of unclassified research during the cold war—or fields that sought to self-police research that posed a security risk—were now caught up in a quest for hypersecurity that tipped the balance against academic freedom.

Government constraints on the practice of research became broader and deeper as the cold war morphed into the war on terror. Export controls that were originally devised to restrict

the transnational flow of military and dual-use goods and services sold by American business were invoked to regulate the circulation of *knowledge* in the research system. Foreign nationals were targeted by inserting restrictive clauses in research contracts. Universities were asked to tighten up the implementation of "deemed export" provisions that are unique to the US and restrict information flows in face-to-face encounters with students and visiting scholars from countries of concern. The intellectual trajectory of foreign students was closely monitored to ensure that they posed no threat to national security.

Coupled with the mosaic theory of intelligence (Pozen 2005), these and similar measures exploited a vague and flexible concept of "sensitive but unclassified information" that massively expanded the ability of the NSS to selectively withhold knowledge and to expand its reach to cover what seemed to be even the most innocuous kinds of research. A further layer of security was provided by the FBI, which works closely with senior university officials to mitigate the risk of information leakage by pre-emptive action.

The Fundamental Research Exclusion (FRE) remains the key instrument protecting unclassified research on campus from government control. Its scope is vigorously protected by university export control officers, who enforce local compliance with government regulations by instilling the necessary discipline in faculty and students alike. By and large, the research community has come to terms with new constraints on academic freedom with regard to sensitive subjects. While they understand that they are necessary, and fear the consequences of violating them, some feel that the dangers are exaggerated by the national security apparatus and those that have access to its deep secrets. Time and again, the research establishment insists that security lies in achievement, in advancing pre-eminence through openness, in building "high walls around small fields" comprising only the most militarily consequential knowledge. As one recent report put it, "the nation will be better served, in balance, by seeking to accelerate its own technical prowess than by seeking to deny potential enemies access to broad ranges of knowledge" (Deemed Exports Advisory Committee 2007, 95). These arguments have only limited traction in an age of asymmetric warfare where relatively simple weapons in the hands of determined adversaries can wreck havoc. We are thus faced with two alternatives: blanket policies that regard the loss of any item of sensitive cutting-edge knowledge as a threat to US economic or military security, and selective policies that scrutinize the detail of the knowledge that is being produced and evaluate the possible effects of it being acquired illegitimately. The apparatus of the NSS prefers a blanket approach, while the research community favors a selective approach. Balancing scientific openness with national security has been a challenge since the earliest days of the cold war. It is one that continues to haunt us today.

Acknowledgements

I thank the editors, two anonymous reviewers, and Sara Angeli Aguiton, John Beatty, David Citrin, Sy Goodman and especially Mario Daniels for their helpful insights.

References

Anon 2008. "What Happened." Accessed April 25, 2015. http://www.wenholee.org/what.

AUECO. 2015. University Export Control List Serve. Accessed March 9, 2015. http://aueco.org/id5.html.

Beatty, J. 2000. "Origins of the US Human Genome Project: Changing Relationships Between Genetics and National Security." In *Controlling Our Destinies*, edited by P. R. Sloane, 131-53. Notre Dame IN: University of Notre Dame Press.

BIS, n.d. Bureau of Industry and Security, Mission Statement. Accessed April 30, 2014. http://www.bis.doc.gov/index.php/about-bis/mission-statement..

Block, F. and M.R. Keller. 2010. *The US Government's Role in Technology Development.* Boulder CO: Paradigm Publishers.

Brady, L. J. 1982. "Taking Back the Rope." Cited in Corson 1982. 9-10.

Carlucci, F. 1982. "Scientific Exchanges and US National Security. *Science*, 215(4529):140-1.

Cirincione, J. 1999. "Cox Report and the Threat from China." Presentation to the CATO Institute, June 7, 1999. Accessed September 6, 2014. http://carnegieendowment.org/1999/06/07/cox-report-and-threat-from-china/4jww?reloadFlag=1.

Corson, D. 1982. *Panel on Scientific Communication and National Security.* Washington D.C.: National Academy Press.

CUI 2011. *Controlled Unclassified Information. 2011 Report to the President.* Accessed April 27, 2015. http://www.archives.gov/cui/reports/report-2011.pdf

Daniels, M. 2013. "The Enemy is Reading: Soviet Espionage and the Debate over Unclassified Technological Information in America, 1945-1947," unpublished paper presented at the German Historical Institute, Washington D.C., March 2013.

Deemed Export Advisory Committee. 2007. *The Deemed Export Rule in an Era of Globalization.* Accessed March 10, 2015. http://fas.org/sgp/library/deemedexports.pdf

Department of Defense, 1991. *Critical Technologies Plan for the Committees on Armed Services. United States Congress. 1 May 1991.* Accessed March 9, 2015. http://www.dod.mil/pubs/foi/Science_and_Technology/Other/240.pdf

Dobson, A. P. 2002. *US Economic Statecraft for Survival, 1933-1991: Of Sanctions, Embargoes and Economic Warfare.* London: Routledge.

Dong, N. 2014. Session "Deemed Export and Reexport — Technology Transfers." Second Annual Conference on the Impact of Export Controls on Higher Education & Scientific Institutions. Georgia Tech, May 2014. Accessed March 9, 2015. http://researchintegrity.gatech.edu/files/Export/2014-conference-audio/Deemed_Export.MP3

Evans, S. A.W. and W. D. Valdivia. 2012. "Export Controls and the Tensions Between Academic Freedom and National Security." *Minerva* 50: 169-90.

FBI n.d. *The FBI's College and Security Effort*, Accessed March 10, 2015. www.fbi.gov/about-us/investigate/counterintelligence/us-academia-1

FBI. 2011. *Higher Education and National Security: The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education.* Accessed March 10, 2015. http://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-national-security

Ferguson, I. F. 2009. *The Export Administration Act: Evolution, Provisions, and Debate,* Congressional Research Service Report 7-5700, July 15.

Golden, D. 2012. "Why the Professor Went to Prison," *Bloomberg News,* November 1.

Golden, D. 2015. "Sex, Lies and Espionage. Did a Professor Spy for the FBI?" *Bloomberg News*, February 15.

Huntington, S. P. 1991. "America's Changing Strategic Interests." *Survival,* 33(1): 3-17.

Inman, B.R. and D. F. Burton Jr. 1990. "Technology and Competitiveness: The New Policy Frontier." *Foreign Affairs,* 69(2): 116-34.

Inspector General. 2004. *Deemed Export Controls May Not Stop the Transfer of Sensitive Technology to Foreign Nationals in the US*, Accessed March 10, 2015. http://www.oig.doc.gov/OIGPublications/IPE-16176.pdf

Kleinman, D. L. 2010, "The Commercialization of Academic Culture and the Future of the University." In *The Commodification of Academic Research. Science and the Modern University*, edited by H. Radder, 24-43. Pittsburgh PA: University of Pittsburgh Press.

Kleinman, D. L. and S. P. Vallas. 2001. "Science, Capitalism, and the Rise of the 'Knowledge Worker': The changing structure of knowledge production in the United States." *Theory and Society*, 30: 451-92.

Knezo, G. 2004. *'Sensitive but Unclassified' and Other Federal Security Controls on Scientific and Technological Information: History and Current Controversy.* CRS Report for Congress. Accessed March 10, 2015. http://fas.org/sgp/crs/RL31845.pdf

Krige, J. 2014. "National Security and Academia. Regulating the International Circulation of Knowledge." *Bulletin of the Atomic Scientists,* 70(2): 42-52.

Krige, J., A. Long Callahan and A. Maharaj. 2013. *NASA in the World, Fifty Years of International Collaboration in Space* (New York: Palgrave Macmillan).

Lakoff, A. 2006. "Preparing for the Next Emergency." *Public Culture,* 19(2): 247 – 71.

Lempinen, E. W. 2011. "FBI, AAAS Collaborate on Ambitious Outreach to Biotech Researchers and DIY Biologists." Accessed April 21, 2015. http://www.aaas.org/news/fbi-aaas-collaborate-ambitious-outreach-biotech-researchers-and-diy-biologists?sa_campaign=Internal_Ads/AAAS/AAAS_News/2011-04-01/jump_page

Lippert, W. D. 2009. "Economic Diplomacy and East-West Trade During the Era of Détente," in *The Crisis of Détente in Europe*, edited by L. Nuti, 190-201. London: Routledge.

Macrakis, K. 2004. "Does Effective Espionage Lead to Success in Science and Technology? Lessons from the East German Ministry for State Security." *Intelligence and Security,* 19:1, 52-77

Masco, J. 2006. *The Nuclear Borderlands. The Manhattan Project in Post-Cold War New Mexico.* Princeton NJ: Princeton University Press.

Masco. J. 2014. *The Theater of Operations. National Security Affect from the Cold War to the War on Terror.* Durham NC: Duke University Press.

McGourty, C. 1989. "Speak Softly or Carry a Big Stick," *Nature,* 341, 26 October, 679.

Mirowski, P. and E.-M. Sent. 2002. *Science Bought and Sold. Essays in the Economics of Science.* Chicago: University of Chicago Press.

Mirowski, P. and E.-M. Sent. 2002a. "Introduction." In *Science Bought and Sold,* edited by P. Mirowski and E.-M. Sent, 1-66. Chicago: University of Chicago Press.

Mirowski, P. 2011. *Science-Mart. Privatizing American Science.* Cambridge MA: Harvard University Press.

MIT. 2002. *In the Public Interest. Report of the Ad Hoc Faculty Committee on Access to and Disclosure of Scientific Information.* Accessed March 9, 2015. http://web.mit.edu/faculty/reports/pdf/publicinterest.pdf

MIT. 2014. *MIT Export Control Website.* Accessed March 10, 2015. http://osp.mit.edu/sites/osp/files/export-controls-at-mit-2014-12-16.pdf

Norris, J. T. (n.d.) *Restrictions on Research Awards: Troublesome Clauses. A Report of the AAU/COGR Task Force*. Accessed February 11, 2015. http://www.aau.edu/WorkArea/DownloadAsset.aspx?id=1634

NSDD189. 1985. *National Policy on the Transfer of Scientific, Technical and Engineering Information,* September 21, 1985. Accessed March 9, 2015. http://fas.org/irp/offdocs/nsdd/nsdd-189.htm

NSF. 2012. *Higher Education in Science and Engineering*. Accessed March 10, 2015. http://www.nsf.gov/statistics/seind12/pdf/c02.pdf

Nuti, L. 2009. *The Crisis of Détente in Europe.* London: Routledge.

Orr, K. 2014. "US Department of Commerce: When Research meets the Deemed Export Threshold – BIS Perspective." Second Annual Conference on Impact of Export Controls on Higher Education and Scientific Institutions. Georgia Tech, May 2014. Accessed March 9, 2015. http://researchintegrity.gatech.edu/files/Export/2014-conference-presentations/Deemed_Exports_Re_exports_Dong_Miller_Orr_Peters.pdf

Pérez-Peña, R. 2013. "Universities Face a Rising Barrage of Cyberattacks," *New York Times,* July 16.

Phillips, K. 2005. "Comment Letter on Department of Commerce Recommendations on Deemed Export Controls." Accessed March 3, 2015. http://www.cogr.edu/Pubs_ExportControls.cfm

Pozen, D. 2005. "The Mosaic Theory, National Security and the Freedom of Information Act." *Yale Law Journal,* 115:3, 628-79.

Pozen, D. 2010. "Deep Secrecy." *Stanford Law Review*, 62:2, 257-339

Prados, J. 2009. "The Strategic Defense Initiative. Between Strategy, Diplomacy and US Intelligence Estimates." In *The Crisis of Détente in Europe*, edited by L. Nuti, 86-98. London: Routledge.

Radder, H. 2010. *The Commodification of Academic Research. Science and the Modern University*. Pittsburgh PA: University of Pittsburgh Press.

Rasmussen, N. 2014. *Gene Jockeys. Life Science and the Rise of the Biotech Enterprise*. Baltimore MD: Johns Hopkins University Press.

Relyea, H. C. 1994. *Silencing Science. National Security Controls and Scientific Communication*. Norwood NJ: Ablex Publishing Corporation.

Reppy, J. and J. Felbinger. 2011. "Classifying Knowledge, Creating Secrets. Government Policy for Dual-Use Technology." *Research in Social Problems and Public Policy*. 19: 277-99.

Romm, J. J. 1993. *Defining National Security. The Nonmilitary Aspects*. New York, NY: Council on Foreign Relations.

SBIR. STTR. *America's Seed Fund*, at https://www.sbir.gov/, accessed September 4, 2015.

Skolnikoff, E. B. 2001. "Research Universities and National Security. Can Traditional Values Survive?" Accessed March 9, 2015. Cited with author's permission. http://web.mit.edu/clawson/www/polisci/research/skolnikoff/branscomb_lecture.pdf

Slaughter, S. and G. Rhoades. 2002. "The Emergence of a Competitiveness Research and Development Policy Coalition and the Commercialization of Academic Science and Technology (1996)." In *Science Bought and Sold*, edited by P. Mirowski and E.-M. Sent, 69-108. Chicago: University of Chicago Press.

Slaughter, S. and G. Rhoades. 2004. *Academic Capitalism. Politics, Policies and the Entrepreneurial University*. Baltimore MD: Johns Hopkins University Press.

Sorenson, T. C. 1990. "Rethinking National Security," *Foreign Affairs*, 69(3): 1-18.

Vallas, S. P., D. L. Kleinman, and D. Biscotti. 2010. "Political Structures and the Making of U.S. Biotechnology." In *State of Innovation: The US Government's Role in Technology Development*, edited by Fred Block and Matthew Keller, 57-76. Paradigm Publishers.

Vest, C. M. 2007. *The American Research University from World War II to World Wide Web: Governments, the Private Sector, and the Emerging Meta-University*. Berkeley, CA: University of California Press.

Wang, J. 1999. *American Science in an Age of Anxiety. Scientists, Anticommunism and the Cold War*. Chapel Hill NC. University of North Carolina Press.

Weiss, L. 2014. *America Inc.? Innovation and Enterprise in the National Security State*. Ithaca NY: Cornell University Press.

Zweig, D. 2013. "Luring Back the Chinese Who Study Abroad," *New York Times*, January 21.