[*draft for discussion purposes – please do not quote without permission*]

To Whom Does a Defense Industry Firm Owe a Duty When There is an Opportunity to Pay a Bribe

Philip M. Nichols*

Abstract

The defense industry has a long history with bribery. Bribes paid by defense businesses had a central role in the Congressional Hearings that preceded enactment of the United States' Foreign Corrupt Practices Act. Scarcely a year has gone by since then without revelations of bribes paid by a defense business somewhere in the world, and studies by Transparency International and the Organisation for Economic Cooperation and Development each suggest that bribery continues to plague the defense industry. The defense industry often counters that it works in a complex, multicultural environment in which personal payments to government officials are often expected. They also point to competition from weapons manufacturers that freely pay bribes. Bribery in the defense industry raises special concerns. For one thing, bribery tends to go hand in hand with diminished quality, which raises concerns about the safety of military personnel and others directly involved. For another, bribery tends to create an environment in which rules and regulations are ignored, which raises concerns about weapons flowing in contravention of rules intended to protect civilians and international order. The claims made by defense businesses and the concerns raised by bribery in the defense industry present a question: to whom does a defense business owe a duty when presented with an opportunity to pay a bribe? This paper concludes that because the market failures that allow bribery to flourish are the same market failures required for the defense industry to operate, and because defense industry firms benefit by operating in that imperfect market, they owe a duty to persons who would be harmed by the effects of bribery.

The defense industry has a long and troubled history with bribery. The disclosure of bribes paid by Lockheed Martin played a highly visible role in the congressional investigations and debates that culminated in the passage of the

* Class of 1940 Reunion Term Associate Professor of Legal Studies and Business Ethics, The Wharton School of the University of Pennsylvania.

Foreign Corrupt Practices Act in the United States. Decades later, the disclosure of bribes paid by BAE Systems played a highly visible role in undermining the credibility of the Serious Fraud Office's claims that it would rigorously enforce the United Kingdom's new Bribery Act. In between, and since, scarcely a year has passed without revelations of bribery in connection to a defense industry firm. Research into the defense industry suggests that unique factors that significantly shape that industry render it prone to corruption. This paper suggests that those same factors create a special responsibility on the part of defense industry firms to avoid paying bribes. These firms benefit from society's indulgence in allowing them to operate in a flawed market. Because those firms benefit from that indulgence, they owe society the benefit of their actions rather than harming society through self-serving behaviors.

I. Factors that Put the Defense Industry at Risk of Corruption

The non-governmental organization Transparency International has conducted what may be the most comprehensive analysis of bribery within the defense industry.[1] Transparency International offers five categories of factors that may contribute to the tendency of any given defense industry firm to engage in corruption: political factors, finance, personnel, operations, and procurement. Within each category Transparency International explores several particular factors that may influence tendencies toward corruption. Transparency International's research provides an excellent framework for a discussion of the issue.

Politics. Within the defense industry, politics can play a more prominent role than in many other industries. In non-democratic countries, members of the military often have influence or even control the government. Even in democracies, defense policy and policymakers sometimes have disproportionate influence. General and President Dwight Eisenhower, a career officer who devoted most of his life to military service, warned that "a close relationship

[1] An interactive summary of Transparency International's research can be found at http://www.ti-defence.org/corruption/typologies#tabs0291.

between government, military, and industry would lead to an unnecessary expansion of military forces, superfluous defense spending, and a breakdown of checks and balances within the public policymaking process. He feared that the influence of such an establishment would allow special interests to profit under the guise of national security."[2]

Military leaders sometimes leverage their power to enrich themselves. In many countries, the military is deeply involved in commercial activities, particularly in extractive industries or in exploitation of natural resources. These industries bear their own unique risks of corruption. Combining the political power that these militaries have with commercial power also contributes to higher levels of corruption. More insidiously, militaries are often tasked with local intelligence gathering and often have access to vast amounts of personal information, which also creates opportunities for abuse and for corruption.

The budgets through which the defense industry's clients pay the defense industry is also different than that of most other industries. As a matter of national security, these budgets are often opaque and subject to little review. In many polities, even the process through which these budgets are devised is not subject to public review. Transparency and public scrutiny are considered by many as critical tools in controlling corruption, but these tools cannot always be used when dealing with the defense industry.

The defense industry also occupies a unique regulatory position. Weapons, and who has them, can pose an existential threat to a polity. The same is true of health, and education, and the products of other industries, but in the case of the defense industry the threat can be immediate. Polities therefore impose many regulations and restrictions on the defense industry, including importation restrictions, exportation restrictions, restrictions on research and development, and on working with other firms or polities, and more. Regulations, particularly cumbersome regulations, create temptations to circumvent through bribery.

---

[2] Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SEC. J. 39, 62 (2012).

Finance. The financing of defense purchases is closely related to some of the political factors described above. Secret budgets and the conflation of the military with commercial activities fuel corruption. Transparency International also points out that even when budgets are public, the financing package for any given transaction rarely is available or scrutinized by the public, which also creates opportunities for corruption.

Personnel. As in any industry, personnel and culture contribute to the amount of bribery that occurs. Nepotism thrives in some militaries, which means that the clients of the military industry may have acquired the power to make purchasing decisions through relationships and connections rather than through ability or integrity – such persons may be more likely to demand bribes. In some militaries, officers are expected to find alternative sources of pay for themselves and their troops, which again could lead to bribe demands.

Transparency International's investigation of the defense industry did not seem to indicate that the personnel at defense industry firms are more inclined to corruption than those in other industries. Firm culture, on the other hand, may cause some people who otherwise would not do so to pay bribes.

Operations. Transparency International points out that many of the largest purchasers of defense industry products are not only undemocratic but are also endemically corrupt. Defense firms are likely to face bribe demands in these countries.

With respect to operations, Transparency International also points out that business firms in the defense industry often work with clients whose own operations are questionable. Many international peace forces are poorly disciplined and engage in activities that are harmful to local populations. Defense industries also increasingly work with or themselves provide private military forces, which operate with very few checks and little accountability.

Procurement. Procurement constitutes an area rife with pitfalls. As is the case with the financing of a transaction, the technical requirements and specifications are often not publicly released or scrutinized, which removes a useful check on bribery and other forms of corruption. The technical complexity

of some transactions also makes oversight by untrained government supervisors difficult. The secrecy of procurement, again combined with the technical complexity of some products, lends itself to single source procurement, which removes the check of open competition. It also makes benchmarking transactions difficult, which means that government supervisors do not have industry standards against which to measure the commercial reasonableness of a purchase.

Transparency International found that defense industry firms use many third parties in the sale of their products, and that governments often use middlepersons as well. Defense industry firms have less control over third parties, and the potential for abuse by third parties is well known in other industries.

Procurement is often tied to issues that have little to do with the quality of the good or service offered by a firm, or that in other ways might contribute to corruption. Procurement is often tied to offsets. Offsets as offsets are not corrupt and can often contribute to the overall value generated by a transaction. Offsets, however, usually are effectuated outside of public scrutiny and create an avenue through which corrupt exchanges can occur. Bribes can also take the form of offsets.

II. THE HARM GENERATED BY BRIBERY

There are at least two types of harms that could be caused by corruption in the defense industry. One is harms caused by general failures in the market process. The other is harms caused by failures in the regulatory process.

Long ago, some people thought that corruption only moved rents from one party to another and had no net effect on economies. People also suggested that bribery was useful in overcoming regulatory barriers and facilitating entry into various economies.[3]

Persons who study corruption now have a much deeper understand of the phenomenon, and have much finer tools and techniques for studying it. Johannes

[3] *See*, David Hess & Thomas W. Dunfee, *Fighting Corruption: A Principled Approach: The C[2] Principles (Combating Corruption)*, 33 CORNELL INT'L L.J. 593 (2000) (noting and criticizing old ways of thinking).

Lamsdorff and others have shown that the notion that corruption merely transfers rent is erroneous, because corruption both effects the size of the rent and because it distorts allocations in unrproductive ways.[4] Daniel Kaufmann and Shang-Jin Wei, in turn, demonstrated that bribery does not reduce barriers to entry but in fact increases the time and money a firm spends interacting with government.[5] The literature on corruption is replete with examples of specific harms that it inflicts on societies and on people.[6]

With respect to understanding the potential harms associated with corruption in the defense industry, it is important to understand how corruption affects decision making by a government purchaser. In a market that is not corrupt, a buyer makes a decision based on the price and the quality of a good or service. A "rational" producer therefore uses its resources to bring the quality of a good or service as close as possible to that desired by the purchaser and to bring its price as close as possible to the price that the purchaser will pay.[7] In an endemically corrupt system, the purchaser makes a decision based on the quality of the bribe. A high quality bribe is one that a purchaser wants and can use. A "rational" producer uses its resources to craft high quality bribes.[8] In a market that is functioning properly, a producer that uses its resources to craft a bribe rather than to improve quality and lower prices will not be able to compete with a producer that uses its resources to produce low-cost, high-quality products. But in an endemically corrupt system the reverse occurs. A producer who devotes resources to the quality of goods or services cannot compete with a producer who uses all of its resources to craft high quality bribes. The world outside of defense

---

[4] Johann Graf Lambsdorff, *Corruption and Rent-Seeking*, 113 PUB. CHOICE 97, 120 (2002).

[5] Daniel Kaufmann & Shang-Jin Wei, *Does "Grease Money" Speed Up the Wheels of Commerce?* (National Bureau of Economic Research Working Paper No. 7093, 1999).

[6] *See* Philip M. Nichols, *The Business Case for Complying With Bribery Laws*, 49 AM. BUS. L.J. 325 (2012) (summarizing research).

[7] Mark B. Bader & Bill Shaw, *Amendment of the Foreign Corrupt Practices Act*, 15 N.Y.U. J. INT'L L. & POL. 627, 627 (1983).

[8] *Id*.; Shouyoung Shi & Ted Temzelides, *A Model of Bureaucracy and Corruption*, 45 INT'L ECON. REV. 873, 874 (2004).

offers many examples of the results of corrupt procurement processes, in the forms of unwanted infrastructure that has no function, shopping centers and housing projects that collapse, substandard education and health facilities, and much more.

Unfortunately, the defense industry also offers examples of low-quality products associated with highly-connected persons. Multiple deficiencies with the heavily-lobbied-for M4 infantry rifle, for example, are argued to have contributed to the deaths and injuries of many soldiers in an infamous battle in Wanat, Afghanistan.[9] A Florida firm with close connections to Florida's then-senior Senator reportedly provided defective grenades to the military.[10] Possibly thousands of other examples exist.[11]

The second type of harms inflicted by corruption in the defense industry is those that could be ascribed to regulatory failures. The defense industry faces numerous regulations around the world, defying an easy, comprehensive typology. This paper will discuss types of regulation not for the purpose of creating a typology but instead to attempt to more finely parse possible harms.

Some regulations are designed to keep technologies developed by one polity out of the hands of threatening polities. South Korea, for example, has numerous regulations that attempt to prevent North Korea from obtaining technology that could be used against the south.[12] These types of regulations are violated. Brian Patrick Regan, for example, a civilian contracted to the National Reconnaissance Office, solicited thirteen million dollars in bribes from the governments of China, Iran, Iraq, and Libya in exchange for technical details

---

[9] Jimmy Wu, *Small Arms Failures Contribute to Wanat Debacle*, DEFENSETECH (Oct. 12, 2009), http://defensetech.org/2009/10/12/small-arms-failures-contributed-to-wanat-debacle/.

[10] *Company Provided Faulty Grenades to Army*, ASQ (Feb. 7, 2011), http://asq.org/qualitynews/qnt/execute/displaySetup?newsID=10559.

[11] *See* Barry Kellman, *De-Coupling the Military/Industrial Complex – The Liability of Weapons Makers for Injuries to Servicemen*, 35 CLEV. ST. L. REV. 351 (1987).

[12] Jaewon Lee, *South Korea's Export Control System* (SIPRI Background Paper Nov. 2013), *available at* http://books.sipri.org/files/misc/SIPRIBP1311.pdf.

about missile delivery systems used by the United States.[13] Israel has long sold US military technology to China which in turn has sold that technology to Iran, which is antagonistic to the United States.[14] Neither South Korea nor the United States has faced existential crisis because of these breaches, but the possible harms are apparent.

Some regulations are intended to keep dangerous weapons out of the hands of polities or organizations that embrace mayhem in general. Most members of the North American Treaty Alliance, for example, have enacted laws that prohibit the transfer of technology and of weapons or military-oriented materials to organizations deemed as terrorist.[15] China has enacted legislation intended to prevent the acquisition of China's nuclear technology and hardware by terrorist organizations.[16] The United States, Russia, and other large nations are negotiating sets of regulations intended to prevent weapons from reaching the Islamic State.[17]

These rules too are abrogated. The Islamic State, for example, acquires many of its weapons through capture or theft, but strong evidence suggests that it acquires many of its most sophisticated weapons through convoluted sales arrangements that may be facilitated by corrupt officials.[18] Similarly, Boko

---

[13] Sarah Frances Cable, Note, *An Unanswered Question in* Kennedy v. Louisiana*: How Should the Supreme Court Determine the Constitutionality of the Death Penalty for Espionage?*, 70 LA. L. REV. 995, 996 (2010).

[14] Michael R. *Gordon, Israel Sells Arms to China, U.S. Says*, N.Y. TIMES, Oct. 13, 1993; Bryant Jordan, *Report: Israel Passes U.S. Military Technology to China*, MILITARY.COM (Dec. 24, 2013), http://defensetech.org/2013/12/24/report-israel-passes-u-s-military-technology-to-china/.

[15] *See* Michael D. Beck & Seema Gahlout, *Introduction to Nonproliferation Export Controls*, *in* TO SUPPLY OR DENY: COMPARING NONPROLIFERATION EXPORT CONTROLS IN FIVE KEY COUNTRIES 1, 2 (Michael D. Beck, Seema Gahlout & Scott A. Jones eds., 2003).

[16] *China Controls Seek to Prevent Terrorism* (Feb. 17, 2007), http://newsok.com/china-controls-seek-to-prevent-terrorism/article/3014775.

[17] Thomas Graham, *ISIS' Worst Nightmare: The U.S. and Russia Teaming Up on Terrorism*, THE NAT'L INTEREST, Feb. 10, 2015.

[18] Christopher Harress, *ISIS Weapons Growing In Number, Sophistication: A Soviet, Balkan And American Mix, But The Group Can't Use All Of Them*, INT'L

Haram acquires some weapons through theft or capture and others through convoluted sales arrangements, but some reports suggest that it also acquires weapons directly from bribed officers in the Nigerian military.[19] The harms inflicted on innocent persons by these and other organizations do not bear repeating. Information from the United Nations High Commission on Refugees suggests that increasing numbers of people flee such violence every year, and that globally more than forty-five million people may currently be displaced in the face of this type of violence.[20]

Two distinct groups of people, therefore, may be harmed by abrogation of the rules. One group consists of persons resident in a polity threatened by another polity. The other group consists of innocent people anywhere who might be harmed by groups or polities that embrace mayhem. While this paper does provide real examples of harms caused by abrogation of these rules, this paper is careful not to directly state that any particular firm in the defense industry pays bribes in order to avoid regulation.

The case that bribes could be paid for such a purpose, however, is easily made. The military industry has a troubled history with the payment of bribes for the purpose of obtaining contracts from or making sales to governments. The payment of bribes to a government official for purposes of self-enrichment by definition involves a violation of rules. Numerous studies have found that the payment – or even merely the observation of the payment – of bribes by members of a firm erodes the "ethical climate" within that firm.[21] Persons within such firms tend to be more opportunistic and to violate other rules.[22] It is a very small and

---

BUS. TIMES (Aug. 15, 2014), http://www.ibtimes.com/isis-weapons-growing-number-sophistication-soviet-balkan-american-mix-group-cant-use-all-1659176.

[19] Clement Ejiofo, *Boko Haram's Source of Weapons Revealed*, NAIJ (June 2014), http://www.naij.com/66368.html.

[20] UNITED NATIONS HIGH COMMISSION ON REFUGEES, MID-YEAR TRENDS 2014. at 21 (2014).

[21] *See* Nichols, *supra* note 6, at 342 (discussing studies).

[22] Willa Bruce, *Ethical People Are Productive People*, 17 PUB. PRODUCTIVITY & MGMT. REV. 241, 248 (1994); William A. Weeks et al., *The Role of Mere Exposure Effect on Ethical Tolerance: A Two-Study Approach*, 58 J. BUS. ETHICS 281, 282 (2005).

possibly inevitable step from paying a bribe for the purpose of selling a product to paying a bribe for the purpose of *being allowed* to sell a product.

III. Defenses by the Defense Industry

The defense industry does not, of course, speak with a single voice. Defenses of structures and conduct that lead to corruption, however, tend to coalesce around three tropes. Perhaps the most frequent defense turns the distorted market observation on its head. Defense industries point out that the market is indeed distorted, and argue that they could not survive in this market without engaging in questionable behavior. These firms often argue that they have a responsibility to the people who depend on them for salaries, to contribute to the overall wealth of the nations in which they are located, or most often that they have a responsibility to enhance the wealth of investors.

Defense industry firms also suggest that they provide a net benefit to society by providing society with the means of defending itself. They point out the many dangers in the world today, the security provided by military devices, and the high costs of developing those devices. Sales made through corrupt means, or sales that violate rules in other ways, subsidize the production of military devices that provide this safety.

It is interesting to note that both this cluster of defenses and the cluster mentioned previously are teleological in nature. These defenses do not take account of rights. As is true of any teleological argument, these defenses rely on empirical claims regarding the conditions of the world and the consequences of discrete actions. A thorough evaluation of these claims would require a level of investigation that would probably violate rules regarding national security and secrecy, and that quite possibly would make individual firms uncomfortable. The argument seems to be offered, therefore, more as a claim than as an actual fact.

A third set of defenses clusters around the notion that “someone else, probably worse, would have done the same thing.” There are many actors in the defense industry, who follow rules in differing degrees. Some firms follow few rules at all. Military industry firms more oriented toward obeying the rules

sometimes suggest that for many reasons it is "better" that firms like themselves make the sale than less rule oriented firms. In addition to accruing the benefits of making these sales, rule-oriented firms suggest that the world would be a more dangerous place if firms with disregard for rules were allowed to flourish.

This is a subtle but interesting argument. In some ways the argument can be compared to the economic doctrine of second best: that if a market distortion cannot be removed then it might be most productive to introduce another market distortion.[23] This argument, as is the case with the preceding arguments, also relies on empirical claims easily made but difficult to verify. The argument also raises troubling questions about self-regulation, and about entrusting firms to break the rules only to an extent that in some way increases – or minimally decreases – overall well-being.

IV. To Whom Does the Defense Industry Owe Duties

A preliminary question is whether defense industry firms, as firms, are moral agents capable of having duties. Numerous business ethicists suggest that business firms are in fact moral agents, to whom moral responsibility and blame can be assigned. Tom Donaldson, for example, notes that business firms are "capable of controlling the structure of [their] policies and rules" and thus bear moral responsibility for the decisions made through them.[24] Eric Posner & Adrian Vermeule suggest two broad arguments for thinking of business firms as moral agents: one set of arguments deemphasizes strict individualism and allows for the assignment of blame to collections of individuals; the other simply treats business firms as individual actors for moral purposes, much the same way that blame is assigned to business firms (and many other entities, such as nations, or unions, or

---

[23] *See* Alan O. Sykes, The Doctrine of Commercial Impracticability in a Second-Best World, 19 J. Legal Stud. 43, 44-45 (1990) (describing theory).

[24] Thomas Donaldson, Corporations and Morality 30 (1982); *see also* Patricia H. Werhae, Persons, Rights, and Corporations 59 (1985) (stating that because business firms structure the rules and processes for the "secondary actions" taken by their agents those firms "are and should be held morally responsible for actions within their control when . . . they could have acted otherwise").

sports teams) in everyday language.[25] This paper recognizes that not everyone agrees that business firms are moral actors to whom duties may be assigned.[26] This paper, however, is not the forum for resolving that debate and proceeds as if business firms or the collection of persons making decisions for and acting on behalf of business firms can be assigned duties.

Many large defense industry firms are publicly traded. Publicly traded firms do have responsibilities to shareholders. But that, of course, cannot be the sum total of the parties to whom these firms owe duties. The discipline of business ethics is replete with arguments that a firm's duties do not end with the observation that a publicly traded firm has responsibilities to shareholders. At a minimum, for example, firms are obligated to obey law, at least to the extent that the laws are meant to be followed.[27] Firms also clearly have a duty not to harm, and outside of the rarified debates of legal scholars most people believe that firms clearly have a duty to rescue.[28] This paper argues that military industry firms do in fact have a special duty to the three groups of persons likely to be harmed through bribery in the defense industry: users of the products and services of that industry, persons defended by the use of those products and services, and victims of groups that embrace and inflict mayhem.

Defense industry firms operate in an inherently flawed market. It is precisely the flaws to the market that create conditions that contribute to bribery within the industry. It is very important to recognize, however, that defense

---

[25] Eric A. Posner & Adrian Vermeule, *Reparations for Slavery and Other Historical Injustices*, 103 COLUM. L. REV. 689, 703-04 (2003).

[26] *See, e.g.*, Amy Sepinwall, *Citizens United and the Ineluctable Question of Corporate Citizenship*, 44 CONN. L. REV. 575, 605 (2012) (arguing that regardless of whether business firms are moral agents, they "are not expected to participate in the central institutions of citizenship").

[27] Thomas A. Uebler, *Shareholder Police Power: Shareholder's Ability to Hold Directors Accountable for Intentional Violations of Law*, 33 DEL. J. CORP. L. 199, 211 (2008).

[28] *See* MARTIN SANDBU, JUST BUSINESS: ARGUMENTS IN BUSINESS ETHICS (2012) (providing deep analysis of the debate and attitudes outside of law); Lynn A. Stout, *Bad and Not-so-Bad Arguments for Shareholder Primacy*, 75 S. CAL. L REV. 1189, 1204 (2002) (summarizing legal arguments).

industry firms benefit rather than are harmed by these market flaws. Indeed, these flaws are allowed to exist so that defense industry firms *can* exist and operate.

The market is a social construct that serves several purposes. Those purposes, however, are socially-oriented and intended to enhance overall well-being. A well-functioning market disciplines or creatively destroys firms that produce unwanted goods or services, that shift rents rather than creating value, that act in ways inimical to society. To the extent that the market does not do so, society regulates activities either through its governance/legal functions or through coordinated social efforts. Market regulation and social regulation, however, are difficult when firms cannot compete, when transactions cannot be disclosed, or when firms of necessity must form close relationships with governments.

Society willingly allows defense industry firms to operate outside the discipline of markets and of regulation. The defense industry is not as lucrative as some business sectors, but has nonetheless managed to accrue substantial income and other benefits from its operations.[29] In turn, society asks that defense industry firms produce functioning goods and services that actually contribute to the defense of that society. Whether through operation of a specific social contract, or through a more general principle of reciprocity, defense industry firms therefore owe a duty to society to perform in that way.

The people against whom defense industry products are used by groups that embrace mayhem are also owed a duty, although arguably in a different way than those owed to society in general. The defense industry might argue that defense industry firms themselves do not directly harm those people, nor do they even make the decision to inflict harm on those people, Their duty, however, may

---

[29] *See* pwc, Aerospace and Defense: 2013 Year in Review and 2014 Forecast (2014), *available at* http://www.pwc.com/en_US/us/industrial-products/assets/pwc-aerospace-defense-2013-year-in-review-and-2014-forecast.pdf;
Richard Clough, *U.S. Defense Industry's Profits Soaring Along With Global Tensions: Lockheed, Northrop, Raytheon and General Dynamics are Reaping Record Rewards for Shareholders*, Bloomberg News (Sept. 25, 2014), http://www.pressherald.com/2014/09/25/u-s-defense-industrys-profits-soaring-along-with-global-tensions/.

lie in theories of complicity. With respect to legal theories, international law assigns culpability to firms that work with bad international actors if three conditions are met:

> (1) there is a strong and interdependent business relationship between the [firm] and the host government (i.e., the [firm] hires the security forces or contracts for their services); (2) the MNC is aware of the human rights violations; and (3) the [firm] . . . continues to perform under contractual arrangements, particularly in furtherance of a collaborative project or endeavor.[30]

Relying on this doctrine, Human Rights Watch has encouraged litigation against defense industry firms that provide devices to malfeasant polities, stating that such a firm "facilitates or participates in government human rights violations. Facilitation includes the company's provision of material or financial support for states' security forces which then commit human rights violations that benefit the company."[31]

As a moral concept, theories of complicity tend to examine the degree of proximity between the actively wrong actor and the putatively complicit actor.[32] Complexity theory teaches that most actions have many effects: a butterfly flapping its wings in New York affects the weather in Tokyo.[33] The butterfly, however, is hardly either spatially or temporally proximate to the effects in Tokyo, and as a moral matter would bear little culpability in any harms caused by inclement weather. A difficult question, and one that does not have an algorithmic answer, is the degree of proximity at which moral responsibility ceases to exist.

The degree of proximity between defense firms that pay bribes to escape regulation and the infliction of damage by groups that embrace mayhem would

---

[30] Anita Ramasastry, *Corporate Complicity: From Nuremberg to Rangoon : An Examination of Forced Labor Cases and Their Impact on the Liability of Multinational Corporations*, 20 BERKELEY J. INT'L L. 91, 103 (2002).

[31] Human Rights Watch, The Enron Corporation: Corporate Complicity in Human Rights Violations (1999), available at http://www.hrw.org/reports/1999/enron/

[32] Kent Greenawalt, *Refusals of Conscience: What Are They and When Should They Be Accommodated?*, 9 AVE MARIA L. REV. 47, 57 (2010).

[33] Steven M. Manson, *Simplifying Complexity: A Review of Complexity Theory*, 32 GEOFORUM 405, 407 (2001).

seem to be close enough to warrant blame. These are not really groups that engage in deliberation or choice; by definition they use military devices to inflict harm. The Clarion Project, a non-aligned organization that promotes dialogue, describes Jama'atu Ahlis Sunna Lidda'awati wal-Jihad – better known as Boko Haram – as "follow[ing] a doctrine of unrestrained warfare, making no distinction between non-combatants and combatants; civilians and soldier; females or males," and notes that its leader has proclaimed that when its followers meet people of other ideologies "'there is no[t] any talk except hitting of the neck.'"[34] To provide weapons to Boko Haram, or to Ansaru, or Epanastatikos Agonas, or Kach Chai, or Kahane Chai, or Lashkar-e-Jhangvi, or Lashkar-e-Taiba, or any of dozens of similar groups, is to *know* that those devices are intended to be used to hurt people. Moreover, the very fact that a bribe would be paid to avoid regulations that prohibit the provision of goods or services to those organizations suggests a strong relationship between the provider of military devices and the group. Both legal and moral responsibility would be assigned to any firm that did so.

CONCLUSION

Defense industry firms operate in an environment in which secrecy is often as much an objective of the parties as is providing or obtaining the most appropriate good or service at the most appropriate price. Not only does this constitute an imperfect market, it also creates conditions that lead to the payment of bribes. Bribery does in fact occur more often in the defense industry than in many other business sectors.

Bribery and other corruption have observable effects. Bribery tends to degrade the quality of goods and services, to degrade the quality of management and decisionmaking, and to be used to avoid regulation. With respect to the defense industry these effects are likely to cause harm to at least three distinct

[34] Ryan Mauro, *Boko Haram* 7 (Clarion Group Fact Sheet 2014), *available at* http://www.clarionproject.org/sites/default/files/ClarionProject_FactSheet%20-%20BOKO%20HARAM.pdf.

groups of people: people who use military devices, people intended to be protected by the goods and services produced by defense industry firms, and the victims of groups that embrace mayhem.

Defense industry firms have a duty not to directly or complicitly harm people within these groups by paying bribes. The market failures that encourage corruption are known and tolerated by society, because those failures are considered necessary for the operation of firms that contribute to safety and security. Defense industry firms are substantially rewarded for their legitimate activities. In exchange for being allowed to benefit from operating without the discipline of markets, society may impose special duties on defense industry firms. That includes a duty not to pay bribes.

A Corruption, Military Procurement and FDI Nexus?

Nancy Hite-Rubin
The Fletcher School
Tufts University

Abstract

Since the end of the Cold War, the levels of both international arms trade and military procurement are increasing exponentially in the developing world. Given that military procurement is seriously prone to corruption (Willett 2009; Auriol 2006; Gupta, de Mello and Sharan 2001), and corruption is more prevalent in lower-income countries, this gives academics and policy analysts some pause. This chapter builds off of previous research showing that countries that are perceived to be corrupt actually attract more foreign direct investment (FDI) when they spend more on their military (Drezner and Hite-Rubin 2014). Using this analysis, I also demonstrate that arms procurement corresponds to higher FDI at an increasing rate along the axis of corruption. Both findings are critical, and elicit further discussion as to the mechanism that underlies these empirical facts. One hypothesis put forward in this paper is that military offsets commonly associated with the purchase of major arms act as a springboard for broader foreign investment into corrupt markets. Questions over market efficiency, as well as, ethical ramifications of this trend, are still very much up for debate.

Chapter 9 in Forthcoming- Susan Rose-Ackerman and Paul Lagunes, ed. *Greed, Corruption, and the Modern State: Essays in Political Economy* (Edward Elgar)

********** Do not Cite or Circulate, comments welcome ☺ **********

Corruption in military procurement is a very serious problem (see, e.g., Willett 2009; Auriol 2006; Gupta, de Mello and Sharan 2001),[1] particularly for developing economies that have experienced the greatest increase in military spending since the Cold War. Corruption of any form arguably stifles economic development. Yet, a recent paper by Daniel Drezner and Nancy Hite-Rubin (2014) provides a possible refutation of this notion. In their global analysis of post–Cold War military spending, they find that countries that are perceived to be corrupt actually attract more foreign direct investment (FDI) when they spend more on their military. The authors attribute their robust empirical finding to the geo-economic favoritism hypothesis. This is the idea that military spending signals to foreign investors that FDI property rights are more secure. Could it also be the case that military procurement, a key component of military spending, stimulates FDI?

Drezner and Hite-Rubin's finding that military spending attracts foreign capital only into corrupt economies is worth further discussion. In this chapter, I explore the relationship between corruption and FDI with an emphasis on how corruption may play a role in arms procurement. I build off of Drezner and Hite-Rubin's previous finding that aggregate military spending leads to higher FDI, and look more closely at the relationship between major arms transfers and subsequent FDI in corrupt states. I show that the purchase of major arms on the international market is also linked to greater FDI, even when controlling for total military spending. This is important, as it means that both the level of overall military spending and the composition of that spending each help to determine foreign investment.In this chapter I explore the possibility that military contracting creates rent-seeking opportunities that actually encourage the flow of foreign capital into corrupt states.

Military procurement is highly prone to corruption for several reasons. First, for security reasons, governments tend to be least transparent in their spending on defense. This alone creates opportunities for rent seeking and project misallocation. Furthermore, military equipment is usually highly specialized, which reduces market entry and competition among suppliers as well as buyers. Finally, because major arms are expensive and complicated, prices vary highly and thus provide a window for corruption. The highly specialized nature of military goods, large profit margins and lack of market competition sets the stage for bribe-taking, collusion and misallocation. Indeed, research using firm-level data indicates that purchases of military equipment are more prone to corruption, and that bribes usurp nearly twice the contract value of any other sector (Cole and Tran 2011). Certainly, corruption in military spending results in losses and is market-distorting. How,

[1] Transparency International (TI) has also done extensive work on this issue, including issuing a Government Defence Anti-corruption Index (Cover et al. 2013). See also "Defence and Security," Transparency International, accessed September 17, 2014, http://www.transparency.org/topic/detail/defence_security.

then, can it be the case that military spending in relatively corrupt markets actually corresponds to higher investment?

The following section reviews literature on corruption and foreign direct investment, discussing how the Drezner and Hite-Rubin article contributes to this debate. I then provide an overview of trends in military spending and arms transfers in the post–Cold War era. Here, I describe the phenomenon of military offset agreements and how they have become increasingly more common, especially in connection with the sale of major arms from wealthy to developing countries. The empirical section of this chapter establishes two findings. First, when corrupt countries spend more on their military they attract foreign capital, whereas non-corrupt countries that spend more do not. Second, arms procurement from foreign sources also significantly attracts FDI, even when controlling for total military spending. This empirical evidence sheds light on the curious triangular relationship between military procurement, foreign capital investment and corruption. The chapter concludes with a discussion on the role of corruption in military procurement, and how it may distort the composition of investment at the same time as it attracts larger dollar totals.

1. Corruption, institutional quality and FDI

Many influential studies have demonstrated that corruption stifles foreign investment and thus growth (Mauro 1995; Keefer and Knack 1997; Wei 2000; Habib and Zurawicki 2002; Dreher and Herzfeld 2005; Hsu 2008; Castro and Nunes 2013). This is based on the idea that the institutional quality of the host country is the paramount factor determining the riskiness, and ultimately the profitability, of foreign investment. As Raymond Vernon (1971) observed more than four decades ago, the "obsolescing bargain" of FDI means that companies must be concerned about the ability of host countries to credibly commit when it comes to maintaining the foreign investment climate. A country's ability to signal to investors that its commitments are credible is inversely related to the degree that it is perceived as being corrupt.

The attractiveness of a host country to foreign investors is deeply intertwined with institutional quality. For example, in recent years a fair amount of empirical research has been devoted to examining the effect that investment-specific institutions, such as bilateral investment treaties and preferential trade agreements, have on FDI (Tobin and Rose-Ackerman 2005; Neumeyer and Spess 2005; Kerner 2009; Büthe and Milner 2008). Neumeyer and Spess ran an empirical analysis looking at the relationship between BITs and foreign direct investment inflows and found a robust, positive correlation. They contend that BITs can function as a substitute for poor institutional quality. Alternatively, Tobin and Rose-Ackerman are more cautious in interpreting this correlation. They find that this BIT-FDI relationship is only robust for countries that already have a stable institutional

environment, and caution against asserting any substituting function. Kerner adds to the debate by providing a more refined model, asserting that BITs attract FDI through indirect channels. Finally Büthe and Milner investigate the empirical relationship with FDI inflows across a multitude of international political institutions, contending that these international institutional agreements (including BITs) allow host governments to make more credible commitments and thus attract more investment. All of these papers share an implicit assumption that corruption is a sign of institutional shortcomings, which sends negative signals to foreign investors.

In addition to exploring the role of international agreements, other scholars argue that due to their inherent institutional checks, democracies are more capable of committing credibly to investors and thus attracting greater FDI. States with democratic regimes are perceived to be more likely to honor their contracts (North and Weingast 1989; Schultz and Weingast 2003; Besley and Persson 2007; Acemoğlu and Robinson 2012). Relatedly, foreign investors are thought to be more vulnerable to the development of "extractive," non-democratic political institutions where politically powerful actors can exploit the coercive apparatus of the state to reward members of the selectorate with private goods, rather than providing the general population with the public goods necessary to attract inward capital flows (Bueno de Mesquita et al. 2003). As Daron Acemoğlu and James Robinson (2012) have observed, countries that rely on extractive institutions are more likely to possess comparatively more sclerotic economies. Finally, Nathan Jensen (2006) argues that because of the higher "domestic audience costs" of democratic institutions, democratic leaders are more geared to policies that facilitate the operations of multinationals.

Although most scholars view corruption as an institutional problem, there is not an overwhelming consensus that such corruption deters foreign direct investment. Egger and Winner argue that corruption is actually a stimulus for FDI (Egger and Winner 2005). They base this claim on their empirical analysis of 73 countries between 1995-1999, wherein they find a strong statistical correlation between positive corruption levels and FDI. From this evidence they assert that corruption is associated with more direct investment in low-income economies, due to its being utilized as a means to circumvent bureaucratic inefficiencies and obstacles. Egger and Winner's paper complements the "efficient grease" view of corruption under which it facilitates rather than deters economic activities (Kaufmann and Wei 1999; Méon and Weill 2009).

Egger and Winner's empirical strategy is, however, seriously flawed. First and foremost, the mere existence of a robust statistical correlation does not provide sufficient grounds to make causal claims. In this chapter, I utilize cross-sectional time series data from 90 countries (1990-2008) and also find that the correlation between corruption and FDI inflows is significant and positive (across a multitude of similarly conservative

specifications). However, I attribute this global relationship to the fact that since the end of the Cold War, the most rapid growth in the world economy has occurred in developing markets. The Global South is also significantly more corrupt than the Global North. Therefore, a cross-sectional empirical model – even one using lags and country-fixed effects as Egger and Winner did – would likely still produce a significant beta coefficient for corruption as a predictor of FDI (due to cross-sectional variation). This does not mean that FDI will increase if corruption levels rise within an individual country, nor does it explain the growth in foreign investment in any particular country. Indeed, when I split the sample of countries between "corrupt" and "non-corrupt" states, the statistical correspondence between corruption and FDI vanishes.[2] In other words, if the corruption level in the Philippines (and similarly "corrupt" countries) is perceived to rise or fall from one year to the next, this change does not affect expected FDI.

Our recent paper on military spending and foreign direct investment demonstrates that military spending is linked to foreign direct investment, but more importantly this link is contingent upon corruption levels (Drezner and Hite-Rubin 2014). We are not suggesting that corruption causes a particular change in FDI. There are numerous factors that correspond with corruption levels that would make the investment climate and political economy of a host country distinct. For this reason, I use the rather simple technique of sample splitting the countries in terms of their corruption levels.[3] In doing so I hope to advance the debate on whether corruption helps or hinders FDI, by showing that military spending only attracts investment into corrupt countries. The purpose of this chapter is to explore why that is the case.

"Military spending" is a measure of all spending on state defense, which includes maintenance, personnel, domestic production of military equipment, and the purchase of major weapons from foreign entities. The measure for "arms transfers" is but one component of military spending, and arguably the only component that involves purchases in the international market. When I analyze the relationship between military spending (excluding arms imports) and FDI, military spending alone is still strongly linked to FDI. I attribute this to the geo-economic favoritism mechanism, whereby domestic investment in security signals to foreign investors that the institutional environment is secure.

---

[2] See the empirical analysis presented in Tables 1, 3 and 4, wherein I split the sample according to level of corruption. The impact of corruption thus vanishes. This is because the significance of the coefficient picks up on differences across the Global South and North, rather than how volatility of an individual country's corruption score predicts FDI. Although fixed effects helps to correct for this problem (by estimating individual intercepts for each country), it is not sufficient. Simply splitting the sample enables an empirical analyst to check for these differentials in the impact of corruption on FDI.

[3] We can learn a lot more from doing this, than running more elaborate models which require implausible assumptions. However it is also important to justify the dimensions of by which to split categories and not split into very small groups.

In this chapter, I pay close attention to an auxiliary finding from our previous article; namely, that the volume of major arms transfers into corrupt countries appears to increase FDI. The relationship between arms procurement and the attraction of foreign capital is statistically independent of the relationship between overall military spending and FDI. Whereas the tendency of aggregate military spending to attract FDI is explained by the logic of geo-economic favoritism as stated earlier (Drezner and Hite-Rubin 2014), the nature of military procurement in international markets merits further consideration. The following section explores trends in military expenditures, focusing on arms transfers. The purpose here is to begin a discussion on whether military procurement in corrupt countries can actually be beneficial to these economies. Alternatively, is there something about military purchases and offset agreements that could distort local markets, while still resulting in a net increase in FDI inflows?

2. Military spending, procurement and offset agreements

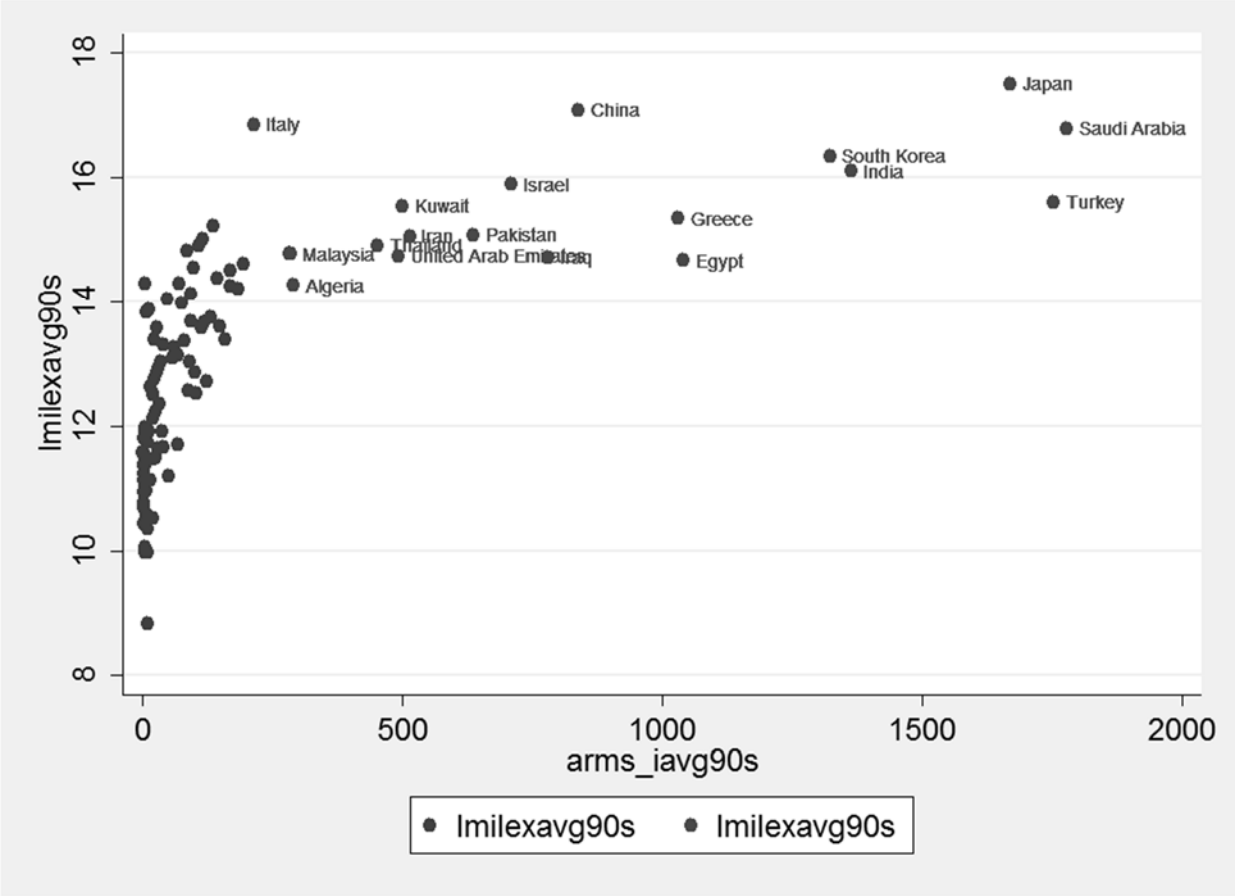
Global military expenditures are currently at an all-time high, estimated to be 1.7 trillion US dollars per year (Archer and Willi 2012). Although the United States still outspends the rest of the world, its relative share is diminishing as other countries (mostly middle-income) are quickly catching up. Although North America and Western and Central Europe have scaled back military spending since 2004, spending has more than doubled (even quadrupled) in many countries throughout the rest of the world (Perlo-Freeman and Solmirano 2014, 6). Much of this increase is attributable to major weapons purchases in the world market. According to the Stockholm International Peace Research Institute (SIPRI), the volume of international arms trade has increased considerably in the last ten years. The world's top importers of major weapons are India, China, Pakistan, the UAE and Saudi Arabia. SIPRI identified over 150 countries that imported weapons since 2009, and finds that sales are growing everywhere except for European states (Perlo-Freeman and Solmirano 2014).

The following two figures illustrate which countries, spent the most on their militaries and imported the highest volumes of major weapons per year. Figure 1 covers the period from the post–Cold war era through 1999, and Figure 2 covers trends in the 2000s. The sample has been censored to only include "corrupt" countries,[4] purposely excluding countries such as the US and Western European countries in which the link between military spending and attracting FDI does not apply. During the 1990s, the greatest quantities of arms were transferred to countries in the Middle East, northern Africa and Asia. Saudi Arabia had the highest annual level of transfers during the 1990s, closely

[4] This means the chart is censored to only include countries that are considered to be corrupt. In this case, I used a PRS score of under 4 to make this determination.

followed by Turkey and Japan. No Latin American countries stood out, nor did any of the sub-Saharan African states have major weapons transfers that were above average at that time.

Figure 1: Military Spending and Weapons Transfers into Corrupt Countries, 1990-1999

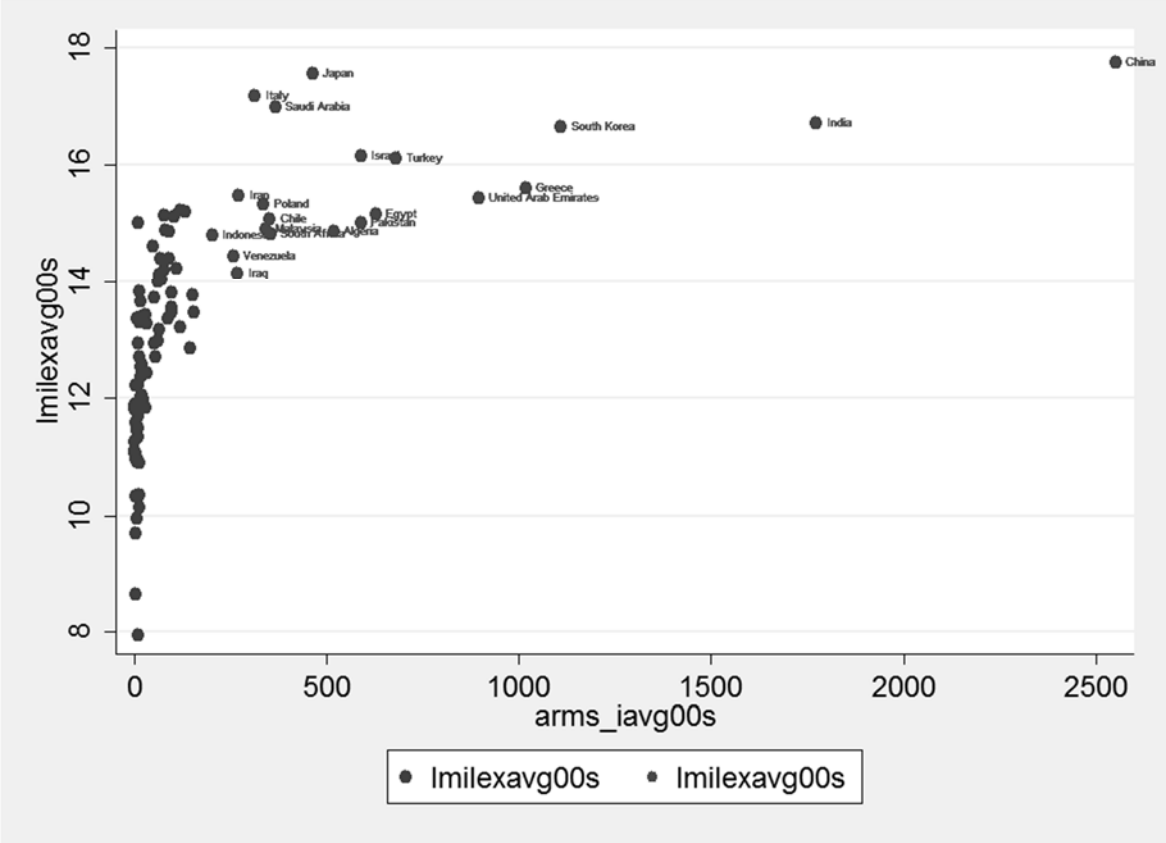


Notes: The scatter plot depicts logged military expenditures on the y-axis and average arms spending (between 2000 and 2008) on the x-axis. "Corrupt" countries that acquired major weapons at markedly high rates are labeled within the plot. These countries, from order of highest import to lowest are Saudi Arabia, Turkey, Japan, India, South Korea, Egypt, Greece, China, Iraq, Israel, Pakistan, Iran, Kuwait, the United Arab Emirates, Thailand, Algeria, Malaysia and Italy.

Between 2000 and 2008 the international sale volume of major arms nearly doubled, as evidenced by the country averages in Figure 2. Comparing across the two charts illustrates several important points. First, the composition of arms transfers has changed considerably. From the Cold War until the 1990s, there was a shift away from Western

Europe. This shift continued into the 2000s and, in fact, there was even more of a pivot towards developing states. Latin American countries such as Chile and Venezuela imported major arms at unprecedented rates, and South Africa became a major player. During the 2000s, arms production and military service companies found profitable consumer bases throughout the developing world. China has dramatically increased its defense spending as well as its importation of major arms, more than quadrupling the former and more than tripling the latter during this decade. Since the end of the Cold War, there has been a marked rise in military spending, as well as, arms procurement by countries with lower institutional credibility and political stability.

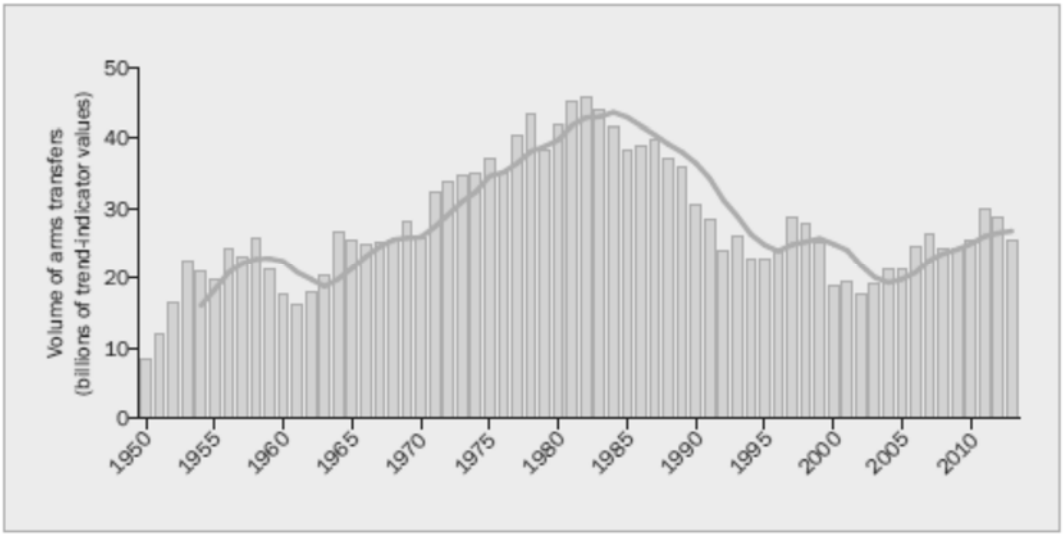
Figure 2: Military Spending and Weapons Transfers into Corrupt Countries, 2000-2008



Notes: The scatter plot depicts logged military expenditures on the y-axis and average arms spending (between 2000 and 2008) on the x-axis. Corrupt countries that acquired major weapons at markedly high rates are labeled in the plot. These countries, from order of highest import to lowest are: China, India, South Korea, Greece, United Arab Emirates, Turkey, Egypt, Israel, Pakistan, Algeria, Japan, Saudi Arabia, South Africa, Chile, Malaysia, Poland, Italy, Iran, Iraq, Venezuela and Indonesia.

The SIPRI measure of arms transfers is an annual, country-level estimate of the volume of military weapons purchased (or transferred) on the international market. The values displayed in Figure 3 show the aggregate volume of "major conventional weapons and components" that are tracked by SIPRI. This includes expensive and complicated items such as missiles, reconnaissance satellites, ships and large artillery (both new and old).[5] The measure does not account for major weapons transferred or sold to non-state actors, nor does it cover smaller items such as trucks, guns and life vests. SIPRI collects its information directly from arms suppliers and indirectly from the US Congressional Research Service's (CRS) annual report, *Conventional Arms Transfers to Developing Nations*. SIPRI claims to receive data regarding arms transfers from non-US countries from CRS sources (Holtom, Bromley and Simmel 2012); however, it is not entirely clear how complete this information is because many of the details are classified.[6]

Figure 3: The trend in international transfers of major weapons, 1950-2013



Source: Wezeman and Wezeman (2014: 1).

The sale of defense equipment has been notoriously associated with corruption (Willett 2009; Auriol 2006; Gupta, de Mello and Sharan 2001).[7] Such corruption ranges from bribes

[5] "Coverage," SIPRI Arms Transfers Database, accessed September 17, 2014, http://www.sipri.org/databases/armstransfers/background/coverage/.

[6] For example, CSR reports rely only on unclassified information and estimated data (see Grimmett and Kerr 2012, 1, 69–75; Holtom, Bromley and Simmel 2012, 4; Federation of American Scientists 1991).

[7] Transparency International (TI) has also done extensive work on this issue, including issuing a Government Defence Anti-corruption Index (Cover et al. 2013). See also "Defence and Security,"

deposited into personal offshore accounts to generally opaque and non-competitive procurement contracts. Military purchases are particularly non-transparent because government defense ministries can invoke national security as a plausible excuse to prevent oversight. Military procurement is prone to rent seeking for economic reasons. Namely, major arms are difficult to price fairly because of product complexity, uniqueness and variation in size. Additionally, the market for international defense equipment is extremely opaque, due in part to national security considerations. Finally, since the end of the Cold War arms procurement has become a "buyers' market," meaning that arms sellers clamor to sell equipment and generate elaborate schemes to win contracts. The phenomenon of military offsets in procurement contracts, increasingly prevalent in the wake of the Cold War, is arguably the result of the shadowy incentives of this arms economy.

A military offset is a reciprocal economic agreement associated with large arms and/or infrastructure purchases from foreign countries. They are the result of negotiations between large suppliers and governments and a typical part of such agreements (Economist Intelligence Unit 2013).[8] According to the US Defense Procurement and Acquisition Policy, the term "offset" refers to:

> . . . the entire range of industrial and commercial benefits provided to foreign governments as an inducement or condition to purchase military goods or services, including benefits such as co-production, licensed production, subcontracting, technology transfer, in-county procurement, marketing and financial assistance, and joint ventures. (Defense Offsets Disclosure Act of 1999, Pub. L. 106-113, section 1243(3))[9]

The broad definition reflects the general diversity that exists across offset arrangements, as well as the fact that little systematic information exists. There are two types of offsets: direct offsets relating to the primary military arms transactions, and indirect offsets, which can be entirely unrelated to security (Ungaro 2013). Another classification relates to whether offset contracts entail "countertrade", "local content requirements" or "bundling" (Markowski and Hall 2006). A "countertrade" provision in an offset agreement refers to the major arms supplier being compensated with goods from the purchasing nation; for example, if part of the contract for military jets is financed with

---

Transparency International, accessed September 17, 2014, http://www.transparency.org/topic/detail/defence_security.

[8] For further information on countertrade and offsets, see "FAQs" issued by the Global Offset and Countertrade Association at http://www.globaloffset.org/faqs.php or read about offsets on the EPICOS website at http://www.epicos.com/Portal/Main/AerospaceDefence/ICOffset/Pages/default.aspx.

[9] For more information about the US law, see "Offsets of Foreign Military Sales: FMS Offsets and Other Issues Affecting FMS Procurements Frequently Asked Questions (FAQs)," Defense Procurement and Acquisition Policy (DPAP), accessed September 18, 2014, http://www.acq.osd.mil/dpap/cpic/ic/offsets_of_foreign_military_sales.html.

palm oil. Such arrangements are argued to be beneficial to host countries because they are export-creating. "Local content requirements" refer to offset stipulations whereby the arms supplier sub-contracts, licenses production or directly finances activities according to the preferences of the arms-importing country. Finally, Markowski and Hall refer to "bundling" as supplying products and services that represent bonuses to the primary arms acquisition. This often takes the form of technology transfers.

Some argue that offset agreements facilitate trade and spill over positively in other sectors unrelated to security (Taylor 2011; Grieve n.d.; Khaitan 2013). Many governments explicitly require offset agreements for all military procurement. In some countries, such as India, the general culture embraces offsets as a means of developing local capacities through technology transfer, creating export markets, and even stimulating foreign investment (Khaitan 2013).

The U.S. Department of Commerce Bureau of Industry and Security (BIS) reports that American defense firms entered into defense export sales contracts worth $122.67 billion from 1993 to 2011. Of these contracts, associated offset agreements were valued at $83.73 billion (approximately 68 percent of all contract value) (BIS 2013). The majority of global sales of arms originate from U.S. suppliers. According to a 2012 Congressional Research Service Report, between 2004 and 2011 U.S.-origin conventional arms transfers totaled $145.2 million. This was twice the amount of arms transfers from the next highest supplier country (Russia, which contracted for $72.5 million), and nearly six times the amount of transfers from the following two suppliers (France and the United Kingdom, at $25.7 and $23.2 million, respectively) (Grimmett and Kerr 2012, 41).[10]

Importantly, offsets agreements are not illegal bribes, and the act of offsetting military spending does not explicitly defy international law[11] or anti-corruption regimes. Despite criticisms, offsets do not necessarily entail bribery. However, the negotiations involved in order to arrive at an offset agreement may provide avenues for corrupt rent seeking. According to a Transparency International research report, offset agreements are particularly prone to corruption in three specific channels (Muravska et. al. 2010). The lucrative incentives presented in offset packages may influence leaders to procure arms that they would otherwise not. Second, officials involved in the offset negotiation and competition may exploit their influence for personal gain. Third, private sector corruption may also play a nefarious role if private companies collude with the arms supplier to

[10] Interestingly, the US supply of offset contracts especially took off between 2008 and 2011. Between 2004 and 2007, Russia led the world in supply of offset contracts, nearly doubling those of the US in contract value (Grimmett and Kerr 2012, 40).

[11] According to WTO's Agreement on Government Procurement (GPA) Article XXIII, procurements that the acquiring country views as "necessary for the protection of its essential security interests" are exempt from the GPA general ban on offset agreements. Yet when national security interests are involved, private influence may affect the outcome of procurement decisions (Piga 2011, 146).

unfairly extract gains from the offset provisions. The authors' broad categories for corruption in defense offsets highlight just some of the ways that non-competitive, highly secretive and exceedingly complex market for major arms could be rife with rent seeking.

The following statistical analysis is not able to determine whether offset agreements lead to more corruption than arms procurement that does not involve offsets. Unfortunately, it cannot determine if the counter-trade, local context requirements and procurement bundling provisions in offset packages induce corrupt governments to buy unnecessary equipment. Nor will I show definitively whether the complexity and secrecy of military procurement directly feeds political patronage and generates economic losses. Rather, the analysis does establish that there is an empirical link between major arms procurement and subsequent foreign investment, which is stronger the higher the levels of perceived corruption.

3. Empirical Methods and Data

The analysis presented here extends the earlier empirical strategy, utilizing some of the same model specifications as the previous article (Drezner and Hite-Rubin 2014). I first revisit the correlation between foreign direct investment and military spending to show how the relationship is tied to perceptions of corruption. In addition to looking at military spending, I narrow the focus to arms transfers (a component of military spending). As discussed in the previous section, these arms transfers are often tied to military offset agreements. Such agreements are becoming increasingly more complex, and may in their own right produce avenues for FDI. Through this empirical analysis, I explore the possible connection between arms purchases and FDI.

The data are organized in pooled time-series cross-sectional format (TSCS), covering 92 countries from the end of the Cold War (1990) through 2008. The results presented account for heteroskedasticity, autocorrelation and cross-sectional dependence of the data. All of the variables utilized in this analysis are described in Table 1.

3.1 Corruption

I utilize two independent index measures of corruption. The primary measure (*corr*) is a measure of "corruption within the political system . . . [that is] a threat to foreign investment," determined annually and published as part of the ICRG.[12] This indicator

[12] The *ICRG Methodology* explains more fully that this is an assessment of corruption within the political system. Such corruption is a threat to foreign investment for several reasons: it distorts the economic and financial environment; it reduces the efficiency of government and business by enabling people to assume positions of power through patronage rather than ability; and, last but not least, it introduces an inherent

measures country-level corruption on a 0–6 relative scale: 6 is considered a perfect score and 0 is considered extremely corrupt. To insure robustness the analysis is retested using Transparency International's Corruption Perceptions Index (TI's CPI) as an alternative measure (*ti_cpi*). The two corruption indices have a correlation coefficient of .837. The ICRG measure is arguably a more appropriate measure for this analysis, because of its balance with respect to the data set and focus on foreign investor incentives.[13]

3.2 FDI inflows

The dependent variable is a measure of net FDI inflows into the host country in a given year, measured in current US dollars. There are two measures of FDI inflows: one relying on Political Risk Services (PRS) Group data, and one relying on World Bank data. The PRS Group's International Country Risk Guide (ICRG) is a subscription-based service that provides data on foreign investment and country-specific political and economic factors.[14] Both sources utilize the same definition and measure for FDI inflows, with the two sources co-varying at over 90 percent.

3. 3 Military spending

Military expenditure data are from the National Material Capabilities (NMC) data set, which is part of the Correlates of War Project at the University of Michigan. Its variable *milex* is a country-year measure of military expenditures, measured in current US dollars. This project utilizes the most recent version (4.0) that covers 158 countries from 1990 to 2007.

3.4 Arms purchases (from abroad)

This logged variable utilizes SIPRI's five-year moving average of arms transfers, a measure that aims to account for year-to-year fluctuations in arms delivery given the often significant variation in total annual transfers (Wezeman and Wezeman 2013, 1). The value is a trend indicator value, designed by SIPRI as a roughly equivalent in estimate of the current dollar value of arms import volumes. The value is not to be confused as an exact

---

instability into the political process. (PRS Group 2014) The *ICRG Methodology* also contains maximum points for these variable and related formulas for calculating risk.

[13] "Balance" refers to the consistency in coverage of country-year observations over the post–Cold War data set. The PRS Group provides data as an investment-focused consumer service. The data it covers are most complete for middle income and emerging market countries.

[14] More information about PRS Group's data is available at http://www.prsgroup.com/ICRG.aspx and http://www.prsgroup.com/CountryData.aspx.

value, and thus relative comparisons are more meaningful than absolute figures. Notice in Table 1, that both logged military expenditures (lmilex) and arms imports (larms_i_) are both negatively associated with corruption. This descriptive statistic indicates that both arms imports and military spending tend to be higher in less corrupt countries. Similarly, the raw correlation test statistic across FDI and corruption is also negative and significant. FDI inflows are lower on average the more corrupt a country is perceived to be.

[INSERT TABLE 1]

3.5 Core political and economic controls

Many institutional, economic and political factors account for changes in FDI inflows from one year to the next. The data set is constructed to comprehensively control for these competing explanations, ensuring that relationships between military spending and FDI inflows are not spurious. The following measures are utilized throughout the findings section. Later, the number of controls is increased in order to verify the robustness of the findings.

Economic Controls. I use two measures control for market size. Logged population (*lpop*) is taken from the Composite Index of National Capability (CINC)[15] version 4.0, which is based on the NMC data set. In addition, CINC's measure for logged primary energy consumption (*lpec*) provides a fairly good proxy for the size of the domestic market within a country in a given year. This energy consumption variable is measured in thousand coal-tons by country-year. In additional to market size, level of economic development is another key control and is measured here as the log of GDP per capita in constant, 2005 US dollars (*lgdp_percap*). This measure is calculated by taking the log of GDP (*gdppcwb05*). The control for economic growth is the annual change in estimated GDP, at constant 1990 prices (*gdp_grow*). Finally, a measure from the Penn World Tables (*pst_gsg*) controls for the role of government size in attracting foreign capital, measuring total government spending as a percentage of GDP.

Political risk. The PRS Group's ICRG political risk measures are also used as control variables. The ICRG collects political and economic information and converts these into annual "risk points," or indexed assessments of financial risk in a given country, along several dimensions. Five of these dimensions are used in the data set. The first is corruption (*corr*), which the ICRG measures annually on a 0–6 scale. Another dimension is foreign

[15] This data set is part of the Correlates of War Project, established in 1963 by J. David Singer, a political scientist at the University of Michigan. The Project's goal has been "the systematic accumulation of scientific knowledge about war." See "Project History," Correlates of War, accessed September 17, 2014, http://www.correlatesofwar.org. The CINC covers the period from 1816 to 2007 and is "the most widely used indicator of national capability" (see "Available Data Sets" on the Project's website).

debt (*f_debt_gdp*), an annual measure of gross foreign debt expressed as a percentage of GDP. The third dimension is an annual measure of government budget balance (*bb_gdp*), expressed as a percentage of GDP. Fourth, the ICRG provides a 6-point index measure of "law and order"[16] (*law_o_*). The ICRG calculates this risk point based on a combined score that measures the strength and impartiality of the legal system, along with an assessment of the observance of law in practice. Finally, the ICRG's combined economic risk rating (*riskr_*) rates investor risk for each country yearly from 0 (highest risk) to 50 (least risk).[17]

International organizations and treaties. Another major factor that can explain FDI flows is bilateral investment treaties (BITs) (Tobin and Rose-Ackerman 2011, 2005). In order to control for the role of bilateral investment treaties, I generated a unique variable *bit*, which, is a country-year measure of the number of active BITs a particular country has with other countries. The intuition behind the measure is that the greater the number of active BITs a country has in a given year, the more capital investment is likely to follow. The variable is constructed with 4,199 country-year observations, with countries averaging 14 treaties in any given year. The model specifications also include two control variables to account for the role of institutionalization upon both attracting FDI and (possibly) stimulating military spending. Formal membership in GATT or WTO is an independent variable to control for the effect of trade alliances. This measure (*GATTWTO*) comes from the Ulfelder International Organizations database. This is a dichotomous measure, coded as a 1 for every year that a given country is a member of either GATT or WTO. In addition, Ulfelder's measure for NATO membership accounts for the possible role of security alliances. *NATO* is a categorical variable, also country-year level of analysis, coded as 0 (neither a member nor formally invited to join), 1 (formally invited to join but not a member), or 2 (member). Both of these control variables cover 160 countries over the 1990–2008 timeframe.

Institutional environment. In addition to political risk factors and international relations variables, I include additional controls for the domestic institutional environment. One such control is the size of government (pwt_gsp), a measure of aggregate government

[16] These two measures comprise one risk component, with each sub-component equaling half of the total. The "law" sub-component assesses the strength and impartiality of the legal system, and the "order" sub-component assesses popular observance of the law. (Refer to ICRG Methodology regarding maximum points for these variable and related formulas for calculating risk.)

[17] "Economic risk rating" is a means of assessing a country's current economic strengths and weaknesses. In general, where strengths outweigh weaknesses a country will show low risk, and where weaknesses outweigh strengths the economic risk will be high. To ensure comparability between countries, risk components are based on accepted ratios between the measured data within the national economic/financial structure, and then the ratios are compared rather than the data. Risk points are assessed for each of the component factors of GDP per head of population, real annual GDP growth, annual inflation rate, budget balance as a percentage of GDP, and current account balance as a percentage of GDP. Risk ratings range from a high of 50 (least risk) to a low of 0 (highest risk), though the lowest de facto ratings are generally near 15.

spending as a percentage of GDP. The logic behind this being that official government spending tends to be rather low in more corrupt countries, and military spending (and thus arms procurement spending) is but one component of the overall government budget. I control for size of government, so to avoid spuriously attributing the impact of increasing the size of the public sector to the effects at hand. Similarly, I also control for net development aid (wdi_aid), a measure of foreign financial assistance from abroad. I also employ the Freedom House democracy score (fh_polity2) and two measures of political stability (ucdp_count, p_durability). The ucdp_count is a measure of the number of conflicts a country is involved in, and p_durability is a count of the number of years since a country had undergone a regime change. Unsurprisingly, on table 1, we see that more "corrupt" countries have significantly lower democracy scores, less durable regimes and have experienced more conflicts during the time (1990-2008) time frame.

4. Military spending and FDI in "corrupt countries"

The analysis shows that countries riddled by corruption tend to attract greater foreign capital when their military spending rises. Although a link between military spending and FDI does not hold in less corrupt economies, the relationship is positive and significant for the emerging market economies (EMEs) in the sample. I demonstrate this by first testing for the relationship among all countries in the global sample and then "splitting" the analysis by corruption levels.

Table 2: Military spending and FDI, by level of corruption

Net FDI Inflows (PRS)	ALL	Low Corruption	Corrupt
	Model 1	Model 2	Model 3
lmilex_percap	0.271**	-0.235**	0.322**
	0.104	0.0923	0.117
lgdp_pc	1.952***	3.458***	1.819***
	0.267	0.367	0.446
gdp_grow_	0.0485***	0.0474***	0.0454**
	0.0149	0.0106	0.0175
bit_	0.0219***	0.0167***	0.0333***
	0.004	0.00473	0.00626
corr_	-0.069	-0.0252	-0.0449
	0.0624	0.0841	0.104
riskr_	0.0316***	0.012	0.0276**

	0.00868	0.0124	0.0107
f_debt_gdp_	-0.00291***	-0.000417	-0.00431***
	0.000752	0.00196	0.00143
bb_gdp_	0.00724	0.0150**	0.00715
	0.0049	0.00602	0.00478
lpec	0.17	-0.402	0.287*
	0.114	0.311	0.15
law_o_	0.104**	0.0704	0.114*
	0.0487	0.0545	0.0625
NATO	0.147*	0.0484	0.423***
	0.0709	0.0884	0.0831
GATTWTO	0.330**	0.950***	0.202
	0.121	0.226	0.142
pwt_gsg	-0.00319***	-0.00367	-0.00276**
	0.000965	0.00399	0.00103
Constant	-22.21***	-28.32***	-21.86***
	2.387	4.827	3.644
Observations	1,362	503	859
Number of groups	88	55	74

Notes: Split analysis of military spending and FDI inflows, over corruption level. Estimation of pooled OLS/WLS and fixed effects (within) regression models with Driscoll and Kraay (1998) standard errors. *** p<0.01, ** p<0.05, * p<0.1. Note that the number of groups refers to the number of countries in the model specification. Since corruption scores vary from year to year, the "low corruption" and "corrupt" country groups overlap.

The results presented in Table 2 demonstrate that the relationship across FDI and military spending hinges significantly upon perceptions of corruption. Here, I split the sample by corruption measure to see if military spending relates to FDI differently for corrupt states. The ICRG measures corruption annually with a relative scale, assigning 75 percent of countries to a score of 4.0 or lower. I coded countries with a score of 4.5 or higher as "Low Corruption" and countries scoring 4.0 or lower as "Corrupt." The split analysis above compares countries that are perceived as corrupt (model 3) to those not perceived by international investors as being corrupt (model 2). What is striking in this analysis is that the relationship between military spending (*lmilex*)[18] and FDI is significant

[18] This logged variable utilizes SIPRI's military expenditure data. This data aggregates (where possible) all current and capital expenditure on

- the armed forces, including peacekeeping forces,
- defence ministries and other government agencies engaged in defense projects,
- paramilitary forces, when judged to be trained and equipped for military operations, and
- military space activities.

Such expenditure should include

and negative for the subsample of non-corrupt states. This negative relationship for non-corrupt countries is striking in comparison to the robust positive relationship seen in corrupt countries. In countries where corruption does not detract from investor confidence, perhaps military spending is a signal of waste. The relationship for country-year observations that fall at or below 4.0 on the corruption scale is robust and positive, in the same manner as the full sample[19].

One possible explanation for why countries with higher levels of corruption benefit from military spending is that it may signal to international investors that their assets are more secure. This interpretation comports with the geo-economic favoritism hypothesis that military spending attracts foreign investment. Countries that are corrupt have inherently insecure institutional environments, and thus require the expensive signal of military spending to demonstrate to investors that the risk of seizure or conflict is minimized. The primary analysis in Figure 1 supports the claim that military spending may send a favorable signal to foreign investors in such environments. Yet, is it possible that another factor may explain this divergence?

To address the relationship across military procurement, corruption and FDI, I need to "unpack" the measure of military spending. In doing so, I investigate whether military procurement, a component of aggregate military spending, explains the FDI increases in corrupt economies. I look at the potential role of corruption as a factor independently resulting in kickbacks and offsets that may increase the level of FDI. In the preceding analysis, I utilized a measure for aggregate military spending, which is seen to reflect military *power* and thus enables testing of the geo-economic favoritism hypothesis. I find support for geo-economic favoritism only in countries with moderate to high levels of corruption. The question at hand, then, is twofold. First, is it possible that military offsets are driving the finding? In other words, when military procurement costs are removed from the aggregate military spending measure, do the initial results still hold? Second, in addition to testing for the robustness of the geo-economic favoritism interpretation I analyse the role of arms transfers alone. Here, I ask whether military purchases on the international market correspond to higher FDI.

- military and civil personnel, including retirement pensions of military personnel and social services for personnel,
- operations and maintenance,
- procurement, military research and development, and
- military aid (in the military expenditure of the donor country. (Perlo-Freeman and Solmirano 2014, 8).

[19] Note that the cut off point of 4, is selected as a conceptual benchmark in line with the ICRG's 75 percentile ranking. In our forthcoming article, we employ marginal-effects analysis to demonstrate that the relationship is insensitive to this arbitrary cut-off.

	FULL SAMPLE	Lowest Corruption	Medium Corruption	Highest Corruption
	Model 1	Model 2	Model 3	Model 4
lmilex	0.233**	-0.393*	0.347**	0.208**
	0.106	0.208	0.121	0.0972
larms_imports	0.0422	-0.00988	0.121*	0.183**
	0.0281	0.028	0.0591	0.0783
corr_	-0.062	0.0282	0.00586	0.0695
	0.0512	0.102	0.12	0.109
lgdp	1.973***	3.115***	2.072***	2.878***
	0.231	0.478	0.426	0.411
ltpop	1.751***	-1.420*	1.710**	3.344***
	0.517	0.772	0.67	0.939
bit_	0.0215***	0.0193***	0.0223**	-0.0209***
	0.00433	0.00463	0.0079	0.00533
riskr_	0.0180*	0.0226	0.0162	0.00859
	0.01	0.0162	0.0101	0.0141
f_debt_gdp_	-0.000999	0.00371	-0.00124	0.000383
	0.00195	0.00385	0.00233	0.00166
bb_gdp_	0.0311***	0.0194*	0.0318***	0.0256**
	0.00646	0.0095	0.0106	0.00957
lpec	-0.652***	-0.557	-0.515	-0.392
	0.201	0.398	0.359	0.304
law_o_	0.0473	0.0662	0.0289	0.0328
	0.0314	0.0473	0.0408	0.0515
Constant	-51.96***	-35.11***	-57.03***	-89.03***
	5.468	4.585	7.775	8.143
Observations	1,091	455	547	289
Number of groups	86	51	68	53

Notes: Estimation of pooled OLS/WLS and fixed effects (within) regression models with Driscoll and Kraay standard errors. *** p<0.01, ** p<0.05, * p<0.1

The regressions presented in Table 3 are consistent with the preceding analysis. The inclusion of arms imports as a control variable appears to bolster, rather than challenge, the main finding. Increased military spending is associated with higher FDI for corrupt states and lower FDI for non-corrupt states.[20] The analysis in Table 3 therefore supports the geo-economic favoritism hypothesis that an increase in aggregate military spending signals to foreign investors that the country is more capable of protecting the assets of foreign investors. However, the results also strikingly show that, while the core finding remains robust, arms imports also appear to predict FDI inflows. Notice that this relationship is only significant for the subsample of countries that are "corrupt." Specifically, arms imports (*larms_i_*)[21] are positively and significantly associated with FDI for countries that are perceived as moderately to very corrupt. In other words, the more corrupt a country is perceived to be, the higher the likelihood that an increase in arms imports corresponds to an increase in FDI inflows. This empirical finding may provide a first glimpse at the prevalence of military offsets and kickbacks associated with arms purchases.

[INSERT TABLE 4]

	FULL SAMPLE	Lowest Corruption	Medium Corruption	Highest Corruption
	Model 1	Model 2	Model 3	Model 4
larms_i_	0.0643	-0.0871**	0.181***	0.321***
	0.0417	0.0364	0.0599	0.0617
corr_	0.0288	0.258*	0.029	0.0595
	-0.0713	-0.129	-0.0805	-0.13
lgdp	1.628***	0.920*	2.371***	2.911**
	-0.42	-0.43	-0.716	-1.123
ltpop	2.074*	0.632	1.325	2.273**
	-0.983	-1.293	-0.958	-0.897
bit_	0.0274***	0.0183*	0.0266**	-0.0171
	-0.00449	-0.00907	-0.0121	-0.0134
riskr_	0.0222**	0.0144	0.0124	0.00724
	-0.00932	-0.0137	-0.01	-0.0184
f_debt_gdp_	-0.00545**	0.000561	-0.00754**	-0.00343**
	-0.00197	-0.00338	-0.00313	-0.00149
bb_gdp_	0.0233*	0.0500***	0.00719	-0.0263
	-0.0122	-0.015	-0.0147	-0.0176

[20] One could simply subtract arms imports from aggregate military spending, but SIPRI advises against combining these two measures into one factor because the data for the two measures are unbalanced.
[21] This logged variable utilizes SIPRI's five-year moving average of arms transfers, a measure which aims to account for year-to-year fluctuations in arms delivery given the often significant variation in total annual transfers (Wezeman and Wezeman 2013, 1).

lpec	-0.701***	-0.374	-0.388	-0.306
	-0.147	-0.32	-0.297	-0.622
law_o_	0.126**	0.0878	0.115	0.0689
	-0.0506	-0.0788	-0.0687	-0.0736
NATO	0.274*	-0.0779	0.603**	-0.575***
	-0.141	-0.109	-0.249	-0.133
GATTWTO	-0.378**	1.380***	-0.494***	-0.897***
	-0.148	-0.29	-0.156	-0.199
pwt_gsg	0.000345	0.0131**	0.000339	0.000344
	-0.000516	-0.0061	-0.000759	-0.00104
wdi_aid	2.25e-10***	1.75e-10***	2.40e-10***	1.67e-10***
	0	-5.31E-11	-7.07E-11	0
ucdp_count	0.145**	0.0797	0.158***	0.155***
	-0.0557	-0.362	-0.045	-0.0375
fh_polity2	0.0619	0.633***	0.0273	-0.0567
	-0.073	-0.195	-0.0676	-0.0768
p_durable	-0.0028	0.0824**	-0.0223	0.0136
	-0.0131	-0.0279	-0.0189	-0.0218
Constant	-45.80***	-28.81**	-54.88***	-76.93***
	-4.984	-10.97	-7.757	-16.54
Observations	593	143	397	207
Number	61	30	58	43

To further explore the relationship between arms procurement in corrupt countries and FDI, I have excluded military spending and expanded the model specifications. Table 4 presents the results after extending the analysis to control for conflict-related factors, and isolating the relationship between arms imports and net foreign direct investment inflows. The relationship across arms imports and FDI is quite similar to the relationship across military expenditures and FDI. However, there is one key distinction: arms sales appear to more strongly predict FDI the more corrupt the country is perceived to be. In addition to the core set of controls, I also included measures for international organization membership (NATO, GATTWTO), size of government (pwt_gsp), net development aid (wdi_aid), democracy score (fh_polity2), and two measures of political stability (ucdp_count, p_durability)[22]. The relationship between the controls and the dependent variable (net FDI

[22] These controls were also utilized in (Drezner and Hite-Rubin) as part of additional robustness checks and specifications for testing the relationship across aggregate military spending and FDI. The findings

inflows) are interesting in their own right and warrant further consideration beyond this chapter. What is perhaps most striking is that the number of conflicts a corrupt state has been involved in since the Cold War (ucdp_count) positively predicts FDI inflows. Also, relative democracy level (fh_polity2) among corrupt and very corrupt states doesn't seem to make a difference when it comes to attracting FDI. Net development aid flowing into countries corresponds to higher FDI, regardless of corruption level. Most importantly, the inclusion of these controls shows us that the volume of arms transfers corresponds to higher FDI, when holding a multitude of important political and economic factors constant.

5. Conclusion

The findings present us with an empirical puzzle that inspires more questions than answers. How can it be the case that for countries such as the Philippines or South Africa, or even the Democratic Republic of Congo, tend to acquire an influx of foreign investment following major military purchases?

An optimistic take on this could be that the offset agreements are making it possible for foreign investors to enter markets that were deemed too risky. In other words, we see that the increase in FDI associated with arms procurement is higher the more corrupt the state is. The observed bump in FDI inflows could be a function of contract "bundling", as well as, spill over from opening new streams for foreign investment. Consider for example, a scenario wherein a company such as Pepsi invests in Indonesia as part of the offset package for purchasing fighter jets from Lockheed, an American company. Lockheed distributes some of the expected profits to Pepsi, and all colluding parties profit on both the supplier and purchasing end. The success of this contract inspires other MNCs to invest in Indonesia, and thus FDI further increases.

Unfortunately, the rosy scenario is likely to be incomplete. First, we do not know if the Indonesian government would have bought fighter jets, but for the offset package inducements. Second, it may also be unclear if the winning contract was most beneficial to the Indonesian government and economy, or if there were side payments involved. Finally, even if the sale of major weapons to Indonesia corresponds to a boost in FDI, it is not obvious that this is welfare enhancing. In other words, foreign investment for a "bridge to nowhere" could register as FDI but actually undermine the host country's development prospects and international profile.

The preceding analysis demonstrates that a robust correlation exists across arms procurement and FDI, while controlling for economic, geo-political and institutional factors. The finding that arms procurement corresponds to higher FDI, at an increasing

---

from both analyses discussed in this chapter and the related paper are robust to additional controls and alternative regression estimators.

rate on the axis of corruption, is critical. The question for future research is *why*? One interpretation is that the purchase of major arms, and associated military offsets, may act a springboard for opening broader foreign investment into corrupt markets. The economic, political and security implications of this cannot be understated

References

Acemoğlu, Daron, and James A. Robinson. 2012. *Why Nations Fail: The Origins of Power, Prosperity, and Poverty.* New York: Crown.

Aizenman, Joshua, and Reuven Glick. 2006. "Military Expenditure, Threats, and Growth." *Journal of International Trade and Economic Development* 15 (2): 129–155.

Archer, Colin, and Annette Willi. 2012. "Opportunity Costs: Military Spending and the UN's Development Agenda." Geneva: International Peace Bureau. http://www.ipb.org/uploads/tbl_noticies_web/169/documents/Opportunity%20Costs_text%20only.pdf.

Auriol, Emmanuelle. 2006. "Corruption in Procurement and Public Purchase." *International Journal of Industrial Organization* 24 (5): 867–885.

Azam, Muhammad, and Siti Aznor Ahmad. 2013. "The Effects of Corruption on Foreign Direct Investment: Some Empirical Evidence from Less Developed Countries." *Journal of Applied Sciences Research* 9 (6): 3462–3467.

Baek, Kyeonghi, and Xingwan Qian. 2011. "An Analysis on Political Risks and the Flow of Foreign Direct Investment in Developing and Industrialized Economies." *Economics, Management, and Financial Markets* 6 (4): 60–91.

Besley, Timothy, and Torsten Persson. 2007. "The Origins of State Capacity: Property Rights, Taxation, and Politics." NBER Working Paper, no. 13028, April.

BIS. 2013. "Offsets in Defense Trade: Seventeenth Study." Conducted pursuant to section 723 of the Defense Production Act of 1950, as amended (February). https://www.bis.doc.gov/index.php/forms-documents/doc_view/687-seventeenth-report-to-congress.

BIS. 2012. "Offsets in Defense Trade: Sixteenth Study." Conducted pursuant to section 723 of the Defense Production Act of 1950, as amended (January). https://www.bis.doc.gov/index.php/forms-documents/doc_view/396-offsets-in-defense-trade-sixteenth-study.

Bueno de Mesquita, Bruce, Alistair Smith, Randolph M. Siverson and James D. Morrow. 2003. *The Logic of Political Survival*. Cambridge: MIT Press.

Büthe, Tim, and Helen V. Milner. 2008. "The Politics of Foreign Direct Investment into Developing Countries: Increasing FDI through International Trade Agreements?" *American Journal of Political Science* 52 (4): 741–762.

Castro, Conceição, and Pedro Nunes. 2013. "Does Corruption Inhibit Foreign Direct Investment?" *Política* 51 (1): 61–83.

Cole, Shawn, and Anh Tran. 2011. "Evidence from the Firm: A New Approach to Understanding Corruption." In *International Handbook on the Economics of Corruption: Volume Two*, edited by Susan Rose-Ackerman and Tina Søreide, 408–427. Cheltenham, UK, and Northampton, MA, US: Edward Elgar.

Cooray, Arusha, and Friedrich Scheider. 2013. "How Does Corruption Affect Public Debt? An Empirical Analysis." Johannes Kepler University of Linz, Department of Economics Working Paper No. 1322. http://www.econ.jku.at/papers/2013/wp1322.pdf.

Corruption Watch. n.d. "The Arms Deal—What You Need to Know." http://www.corruptionwatch.org.za/content/arms-deal-what-you-need-know.

Cover, Oliver, Tehmina Abbas, Leah Wawro and Anne-Christine Wegener. 2013. *Government Defence Anti-corruption Index 2013*. London: Transparency International UK.

d'Agostino Giorgio, J. Paul Dunne and Luca Pieroni. 2012. "Corruption, Military Spending and Growth." *Defence and Peace Economics* 23 (6): 591–604.

Dreher, Axel, and Thomas Herzfeld. 2005. "The Economic Costs of Corruption: A Survey and New Evidence." Social Science Research Network working paper. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=734184.

Drezner, Daniel W., and Nancy Hite-Rubin. 2014. "Does Military Spending Attract (Corrupt) Foreign Investment? An Empirical Investigation." Working paper prepared for presentation at the American Political Science Association annual meeting, Washington, DC, August.

Driscoll, John C., and Aart C. Kraay. 1998. "Consistent Covariance Matrix Estimation with Spatially Dependent Panel Data." *Review of Economics and Statistics* 80 (4): 549–560.

Dumludag, Devrim. 2012. "How Does Corruption Affect Foreign Direct Investment in Developing Economies?" *Talkin' Business* (September 21). http://www.talkinbusiness.net/2012/09/how-does-corruption-affect-foreign-direct-investment-in-developing-economies/.

Economist Intelligence Unit. 2013. "The Defence Industry: Guns and Sugar." *Economist Intelligence Unit* (May 25). http://www.economist.com/news/business/21578400-more-governments-are-insisting-weapons-sellers-invest-side-deals-help-them-develop.

Egger, Peter, and Hannes Winner. 2005. "Evidence on Corruption as an Incentive for Foreign Direct Investment." *European Journal of Political Economy* 21: 932–952.

Federation of American Scientists. 1991. "Literature Review: CRS' Conventional Arms Transfers to the Third World." *Arms Sales Monitor* 6 (August).

GAO (US General Accounting Office). 2003. *Report and Recommendations of the Defense Offsets Commission Still Pending*. GAO-03-649 (May). Washington, DC: GAO.

Grieve, Chuck. n.d. "Why It's Good to Switch on to Offsets." *Defence* 53–56. http://www.offsets2000.com/wp-content/uploads/2013/07/Offsets-2000-Roger-Bulgin-Defence-Interview.pdf.

Grimmett, Richard E., and Paul K. Kerr. 2012. *Conventional Arms Transfers to Developing Nations, 2004–2011*. US Library of Congress, CSR Report R42678, August 24. Washington, DC: Congressional Research Service.

Gupta, Sanjeev, Luiz de Mello and Raju Sharan. 2001. "Corruption and Military Spending," *European Journal of Political Economy* 17 (4): 749–777.

Habib, Mohsin, and Leon Zurawicki. 2002. "Corruption and Foreign Direct Investment." *Journal of International Business Studies* 33 (2): 291–307.

Holtom, Paul, Mark Bromley and Verena Simmel. 2012. "Measuring International Arms Transfers." SIPRI Fact Sheet (December). http://books.sipri.org/product_info?c_product_id=450.

Hsu, Yuan-Ho. 2008. "Is Corruption a Grabbing Hand? A Panel Data Study of FDI." Program for Encouraging Academic Research, National Cheng Kung University, Tainan, Taiwan.

Jensen, Nathan M. 2006. *Nation States and the Multinational Corporation: A Political Economy of Foreign Direct Investment*. Princeton, NJ: Princeton University Press.

Kaufmann, Daniel, and Shang-Jin Wei. 1999. "Does 'Grease Money' Speed Up the Wheels of Commerce?" NBER Working Paper 7093. Washington, DC: National Bureau of Economic Research. http://www.nber.org/papers/w7093.

Keefer, Philip, and Stephen Knack. 1997. "Why Don't Poor Countries Catch Up: A Cross-national Test of an Institutional Explanation." *Economic Inquiry* 35 (3): 590–602.

Kerner, Andrew. 2009. "Why Should I Believe You? The Costs and Consequences of Bilateral Investment Treaties." *International Studies Quarterly* 53 (1): 73–102.

Khaitan, Rajiv. 2013. "Indian Defence Industry and Defence Offset." Seminar on Practical Aspects of Doing Business with India, Hotel Herods, Tel Aviv, February 14. http://www.indembassy.co.il/adminpart/resimages/68090Indian%20Defence%20Industry%20and%20Defence%20Offset%20-%20Khaitan%20(14%20February%202013).pdf.

Kimla, Dominik. 2013. "Military Offsets and In-country Industrialisation: Top 20 Military Offsets Markets." Market Insight presentation by Frost and Sullivan, March.

Marshall, Shana. 2010. "The Modernization of Bribery: The Arms Trade in the Arab Gulf." Jadaliyya (December 22). http://www.jadaliyya.com/pages/index/413/the-modernization-of-bribery_the-arms-trade-in-the.

Marshall, Shana. 2009. "Money for Nothing? Offsets in the U.S.–Middle East Defense Trade." *International Journal of Middle East Studies* 41 (4): 551–553.

Mauro, Paolo. 1995. "Corruption and Growth." *Quarterly Journal of Economics* 110 (3): 681–712.

Méon, Pierre-Guillaume, and Laurent Weill. 2009. "Is Corruption and Efficient Grease?" *World Development* 38 (3): 244–259.

Metzger, Robert S. 2013. "Offsets Loom Large as Defense Firms Sell More Abroad." *Law360* (September 30). http://www.rjo.com/PDF/OffsetsLoom_093013.pdf.

Muravska, Julia, Mark Pyman and Francisco Vihena da Cunha. 2010. "Corruption Risks in Defence Offset Contracts" presentation for Global Revolution V Conference. Copenhagen, September 9-10, 2010

Neumayer, Eric, and Laura Spess. 2005. "Do Bilateral Investment Treaties Increase Foreign Direct Investment to Developing Countries?" *World Development* 33 (10): 1567–1585.

North, Douglass, and Barry Weingast. 1989. "Constitutions and Commitment: The Evolution of Institutions Governing Public Choice in Seventeenth Century England." *Journal of Economic History* 49 (4): 803–832.

Perlo-Freeman, Sam, and Carina Solmirano. 2014. "Trends in World Military Expenditure, 2013." SIPRI Fact Sheet (April). http://books.sipri.org/files/FS/SIPRIFS1404.pdf.

Perlo-Freeman, Sam, and Pieter D. Wezeman. 2014. “The SIPRI Top 100 Arms-producing and Military Services Companies, 2012.” SIPRI Fact Sheet (January). http://books.sipri.org/files/FS/SIPRIFS1401.pdf.

Piga, Gustavo. “A Fighting Chance against Corruption in Public Procurement?” In *International Handbook on the Economics of Corruption: Volume Two*, edited by Susan Rose-Ackerman and Tina Søreide, 141–181. Cheltenham, UK, and Northampton, MA, US: Edward Elgar.

PRS Group. 2014. *IGRG Methodology*. East Syracuse, NY: PRS Group. http://www.prsgroup.com/wp-content/uploads/2014/08/icrgmethodology.pdf.

Russin, Richard J. 1995. “Offsets in International Military Procurement.” *DISAM Journal* 17 (4): 105–121.

Schultz, Kenneth, and Barry Weingast. 2003. “The Democratic Advantage: Institutional Foundations of Financial Power in International Competition.” *International Organization* 57 (1): 3–42.

Slijper, Frank. 2013. *Guns, Debt and Corruption: Military Spending and the EU Crisis*. Amsterdam: Transnational Institute. http://www.tni.org/files/download/eu_milspending_crisis.pdf.

Taylor, Travis K. 2011. “Countertrade Offsets in International Procurement: Theory and Evidence.” In *Designing Public Procurement Policy in Developing Countries: How to Foster Technology Transfer and Industrialization in the Global Economy*, edited by Murat A. Yülek and Travis K. Taylor, 15–34. New York, Dordrecht, Heidelberg and London: Springer.

Tobin, Jennifer, and Susan Rose-Ackerman. 2011. “When BITs Have Some Bite: The Political-Economic Environment for Bilateral Investment Treaties?” *Review of International Organizations* 6 (1): 1–32.

———. 2005. “Foreign Direct Investment and the Business Environment in Developing Countries: The Impact of Bilateral Investment Treaties.” Yale Law School Center for Law, Economics and Public Policy Research Paper No. 293. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=557121.

Tokunova, Svetlana. 2014. “A Comparative Study on the Effects of Corruption on FDI.” Master’s thesis, Erasmus School of Economics, Rotterdam.

TRACE International. 2014. *Global Enforcement Report (GER) 2013*. Annapolis, Dubai and Manila: TRACE International. http://www.traceinternational.org/Knowledge/ger2013.html.

Ungaro, Alessandro R. 2013. “Trends in the Defence Offsets Market.” 17th Annual International Conference on Economics and Security (ICES), SIPRI, Stockholm, June 14–15. http://www.sipri.org/research/armaments/milex/ICES2013/papers/archive/ungaro-trends-in-the-defence-offsets-market.

US International Trade Commission (USITC). 1985. “Assessment of the Effects of Barter and Countertrade Transactions on U.S. Industries.” Report on Investigation No. 332-185 under Section 332 of the Tariff Act of 1930, USITC Publication 1766, October. Washington, DC: USITC.

Vernon, Raymond. 1971. *Sovereignty at Bay.* Boston: Longman.

Wei, Shang-Jin. 2000. “Local Corruption and Global Capital Flows.” Brookings Papers on Economic Activity 2: 303–346.

———. 1997. “Why is Corruption So Much More Taxing than Tax? Arbitrariness Kills.” NBER Working Paper No. 6255. Washington, DC: National Bureau of Economic Research.

Wezeman, Siemon T., and Pieter D. Wezeman. 2014. “Trends in International Arms Transfers, 2013.” SIPRI Fact Sheet (March). http://books.sipri.org/files/FS/SIPRIFS1403.pdf.

Willett, Susan. 2009. “Defence Expenditures, Arms Procurement and Corruption in Sub-Saharan Africa.” *Review of African Political Economy* 36 (121): 335–351.

Zorluoglu, Habib Izzet, Fehrettin Tezcan and Turker Cakir. 2008. “Offset Implementation for Turkey’s International Defense Acquisitions.” MBA professional report, Naval Postgraduate School, Monterey, California, December.

Center for Ethics and the Rule of Law
Ethical Dilemmas in the Global Defense Industry
April 16, 2015
DRAFT PAPER

The Compliance Mentoring Program: Improving Ethics and Compliance in Small Government Contractors

By Jessica Tillipman & Vijaya Surampudi[1]

I. Introduction

Over the past decade, the anti-corruption, ethics and compliance landscape has changed dramatically. This is a direct consequence of a robust anti-corruption enforcement effort by the United States and other countries. The increase in enforcement has also been spurred by the passage of several multilateral anti-corruption agreements, such as the Organization for Economic Co-operation and Development Anti-Bribery Convention ("OECD Anti-Bribery Convention") and the United Nations Convention Against Corruption ("UNCAC"), which prohibit, among other things, the bribery of foreign government officials. They also require companies to dedicate resources to maintaining robust internal controls.

The increase in anti-corruption enforcement has had a profound impact on large, multinational corporations. Many of these companies have responded to this increase in

[1] Jessica Tillipman is the Assistant Dean for Field Placement and a Professorial Lecturer in Law at The George Washington University Law School where she co-teaches an Anti-Corruption & Compliance seminar. She is also a Senior Editor of the FCPA Blog. Vijaya Surampudi is a third-year law student at The George Washington University Law School. She will graduate in May, 2015.

enforcement by investing heavily in sophisticated compliance programs designed to prevent or mitigate liability for anti-corruption violations. This development has been most pronounced in the defense industry where large, U.S. defense contractors have developed rigorous compliance programs.

Unlike their large counterparts, many small government contractors are largely unable to keep up with the rapidly evolving trends and best practices in ethics and compliance. Their inattention to this critical area leaves them at risk for compliance failures, fraud and corruption. As a result, small contractors are more likely to be debarred from the U.S. procurement system than their large counterparts. Despite the harsh consequences that stem from these compliance deficiencies, few small contractors dedicate resources to the development of vital compliance policies and internal controls. This has resulted in a critical gap in the defense industry supply chain, as many large contractors regularly partner with small companies that lack the sophistication and resources necessary to ensure compliance with the many government contracts compliance requirements.

One possible solution to this growing problem is to incentivize large government contractors to work with their small partners to help develop their compliance programs. To be effective, the incentives must be substantial so that large contractors are willing to share their confidential and proprietary programs with other companies. Fortunately, a model for this type of arrangement exists in the U.S. procurement system. The U.S. "mentor-protégé" program is designed to assist small businesses with the navigation of the immense government contracts regulatory system. Under this program, the larger, more experienced contractor serves as a "mentor" to the smaller contractor (the "protégé"). Among other things, the mentor guides the protégé through the complex procurement regime by sharing expertise and resources. In return,

the mentor is provided with contractual opportunities and incentives. This model could be beneficial in the area of compliance by providing a mechanism where information could be exchanged between two contracting parties to ensure transparency throughout all levels of the procurement regime.

II. Global Shift in Anti-Corruption Enforcement & Compliance

Over the past decade, there has been a global shift in perceptions and approaches towards public corruption. Enforcement has increased dramatically, the sharing of information and resources among governments has improved, and global best practices in corporate anti-corruption compliance have emerged.[2] Dozens of countries have made multilateral commitments to combat corruption and have enacted anti-corruption legislation to fight bribery and foster a new era of corporate anti-corruption compliance.[3]

Anti-bribery enforcement agencies, non-governmental organizations and civil society organizations have developed compliance guidance to assist companies with the prevention and deterrence of corruption. In addition, large, multinational companies have been incentivized to invest in ethics and compliance programs in an effort to avoid expensive anti-corruption enforcement actions and the long-term reputational harm that may result from public knowledge of their misconduct.

a. Relevant Corruption Laws, Treaties and Conventions

Enacted in 1977, the FCPA has provided the foundation for today's global anti-corruption enforcement activities. The U.S. statute criminalizes the bribery of foreign government officials and requires persons and entities to maintain accurate books and records

[2] *2014 Year-End FCPA Update*, Gibson Dunn Publications (January 5, 2015) available at http://www.gibsondunn.com/publications/pages/2014-Year-End-FCPA-Update.aspx
[3] *Infra* text accompanying notes 13-16

and robust internal controls.[4] Working in tandem, the two pillars of the FCPA not only combat bribery, but also ensure that companies and individuals do not hide bribes and improper transactions in off-book accounts and slush funds.[5] FCPA enforcement has increased dramatically over the past decade, resulting in hundreds of enforcement actions –a significant increase from the previous two decades of enforcement.[6]

While the FCPA is famous for its broad jurisdiction, often ensnaring both U.S. and foreign companies that run afoul of its prohibitions–it is equally feared because of its broad knowledge standard, which has resulted in significant fines and penalties for companies that rely on third parties and suppliers to help them develop business opportunities abroad.[7] The statute's knowledge standard "is designed to ensure that companies do not hide behind their agents or other third parties to avoid liability for the bribery of foreign government officials."[8] Indeed, the vast majority of FCPA cases were triggered by third parties that have bribed government officials on behalf of a particular company.[9] To reduce the risk of liability that may result from the actions of third parties and suppliers, companies have developed robust due diligence and oversight procedures for the selection and monitoring of their business partners.[10] Companies that ignore bribery "red flags" in the vetting or monitoring of third parties proceed at their own

[4] 15 U.S.C. §§ 78dd-1, et. seq. (2010).
[5] 15 U.S.C. §§ 78dd-1, et. seq. (2010).
[6] *2014 Year-End FCPA Update*, Gibson Dunn Publications (January 5, 2015) available at http://www.gibsondunn.com/publications/pages/2014-Year-End-FCPA-Update.aspx
[7] 15 U.S.C. §§ 78dd-1, et. seq. (2010); *see also 2014 Year-End FCPA Update*, Gibson Dunn Publications (January 5, 2015) available at http://www.gibsondunn.com/publications/pages/2014-Year-End-FCPA-Update.aspx
[8] Tillipman, Jessica, Gifts, Hospitality & the Government Contractor (June 1, 2014). Briefing Papers No. 14-7, June 2014 at 15.
[9] *Id.*
[10] *Id.*

peril.[11]

While the United States remained alone for 25 years in its fight against the bribery of government officials in international business transactions, the anti-corruption landscape began to change in the late 1990s.[12] "In less than a decade, dozens of countries [had] signed on to treaties requiring them to criminalize transnational bribery of foreign officials in similar terms to the antibribery prohibition of the FCPA, requiring criminalization of money laundering where the predicate offense is a corrupt practice, and requiring cooperation with other counties in investigations and enforcement."[13] Moreover, multilateral agreements, such as the OECD Anti-Bribery Convention and UNCAC, have spawned implementing legislation across the globe designed to, among other things, combat bribery in international business.[14]

Signed in 1997, the OECD Anti-Bribery Convention is aimed at reducing corruption in developing countries by encouraging sanctions against bribery in international business transactions.[15] The convention largely mirrors the provisions of the FCPA, prohibiting the bribery of foreign government officials and requiring companies to maintain stringent internal

---

[11] *See, e.g.*, TRACE International, *Trace Due Diligence Guidebook: Doing Business With Intermediaries Internationally*, 19 (2010), http://www.traceinternational.org/data/public/The2010TRACEDueDiligenceGuidebook-65418-1.pdf. This guidebook contains a helpful list of common bribery red flags that should signal the need for caution and additional investigation.

[12] Lucinda Low, *The United Nations Convention Against Corruption: The Globalization of Anticorruption Standards* (2006), *available at http://www.steptoe.com/assets/attachments/2599.pdf*.

[13] *Id.* (detailing the numerous regional anti-corruption treaties that were also passed during this time period).

[14] United Nations Convention Against Corruption, (Sept. 2004), V.04-56160, *available at* https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf; Organization for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, (2011), *available at http://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf*.

[15] http://issuu.com/oecd.publishing/docs/reporttoministers

controls. As of March 2015, thirty-four OECD member countries and seven non-member countries have adopted the convention.[16] The OECD Working Group on Bribery monitors the implementation of anti-corruption legislation and assesses anti-corruption law enforcement efforts.[17] Over the past decade, active implementation of the OECD has led to the criminal sanctioning of 333 individuals and 111 entities for foreign bribery. [18]

The UNCAC requires states to implement a variety of anti-corruption measures, which affect their laws, institutions and practices. The UNCAC provides a holistic approach to combatting corruption, focusing not only on traditional law enforcement techniques, but also on methods of enhancing international co-operation and preventative measures directed at both the public and private sectors.[19] Similar to the OECD Anti-Bribery Convention, the UNCAC requires states to impose "civil, administrative or criminal penalties" on individuals or companies that engage in acts of corruption to dissuade other entities from propelling or encouraging similar patterns of corruption.[20] Its provisions also address the "promotion of corporate codes of conduct, best practices, and compliance programs for business and the professions, [and] measures to promote corporate transparency."[21]

---

[16] *OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* http://www.oecd.org/corruption/oecdantibriberyconvention.htm (last visited April 2, 2015).
[17] *Id.*
[18] *Annual Report of the OECD Working Group on Bribery 2014*, Organization for Economic Cooperation and Development (2014) at 15, *available at http://www.oecd.org/daf/anti-bribery/AntiBriberyAnnRep2012.pdf.*
[19] http://www.unodc.org/unodc/en/treaties/CAC/ (requiring each state to "develop and implement or maintain effective, coordinated anti-corruption policies that promote the participation of society and reflect the principles of the rule of law, proper management of public affairs and public property, integrity, transparency and accountability.") at 9
[20] *Id.* at 14.
[21] Lucinda Low, *The United Nations Convention Against Corruption: The Globalization of Anticorruption Standards* (2006), *available at http://www.steptoe.com/assets/attachments/2599.pdf.*

b. Robust Anti-Corruption Enforcement Ushers in a New Era of Compliance

The dramatic increase in anti-corruption enforcement by the United States and (increasingly) other countries, demonstrates a growing global commitment to combatting corruption. Many household company names have run afoul of the FCPA, resulting in time-consuming, expensive and embarrassing enforcement actions.[22] Not surprisingly, the negative consequences stemming from these enforcement actions have incentivized large, multinational companies to invest in compliance programs that will detect, prevent and deter illicit activities.[23] Moreover, governments, international organizations and civil society have also championed the role of ethics and compliance in helping to prevent and mitigate corporate corruption.

In fact, the U.S. Department of Justice ("DOJ") has publicly recognized and rewarded companies that implement robust compliance programs even when allegations of corruption arise. For example, in 2011, Johnson & Johnson entered into a Deferred Prosecution Agreement with the DOJ to resolve corruption allegations. The government made clear that it had reduced the company's criminal penalty to $21.4 million "due to J&J's pre-existing compliance and ethics programs, extensive remediation and improvement of its compliance systems and internal controls."[24] In 2012, the DOJ took an unprecedented step of publicly announcing that it had

[22] *See* Richard L. Cassin, *With Alstom, three French Companies are now in the FCPA top ten*, The FCPA Blog (December 23, 2014 at 9:45AM) available at http://www.fcpablog.com/blog/2014/12/23/with-alstom-three-french-companies-are-now-in-the-fcpa-top-t.html (establishing many household companies settled FCPA violations with DOJ including Siemens ($800 million in 2008), Alstom ($772 million in 2014), KBR/Halliburton ($579 million in 2009) BAE ($400 million in 2010)).

[23] Claudia J. Dumas, Fritz Heimann, Shruti Shah, *Verification of Anti-Corruption Compliance Programs*, Transparency International-USA Report, at p. 9 (2014)

[24] *Johnson & Johnson Agrees to Pay 21.4 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act and Oil for Food Investigations*, Department of Justice Office of Public Affairs Press Release (April 8, 2011) available at http://www.justice.gov/opa/pr/johnson-johnson-agrees-pay-214-million-criminal-penalty-resolve-foreign-corrupt-practices-act

declined to prosecute Morgan Stanley for the bribery of a Chinese government official because of the company's strong, pre-existing compliance program.[25] Instead, DOJ limited its prosecution to the "rogue" employee that committed the wrongdoing.[26]

Over the past decade, an international consensus has developed regarding best practices in corporate ethics and compliance programs.[27] Several government enforcement agencies, non-governmental anti-corruption organizations, industry groups, and civil society organizations have released compliance "best practices" guides that provide guidance to companies designing risk-based, anti-corruption compliance programs.[28] For example, in 2010, the OECD published anti-corruption compliance guidance, titled *Good Practice Guidance on Internal Controls, Ethics and Compliance*, providing a framework for companies to assist them with the design of their compliance programs.[29] In 2012, the U.S. Department of Justice published *A Resource Guide to*

[25] *See Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA*, Department of Justice Office of Public Affairs Press Release (April 25, 2012) ("After considering all the available facts and circumstances, including that Morgan Stanley constructed and maintained a system of internal controls, which provided reasonable assurances that its employees were not bribing government officials, the Department of Justice declined to bring any enforcement action.").

[26] *Id.* The DOJ's publicly pronouncements regarding the importance of compliance are not limited to FCPA enforcement. *See generally* Brent Snyder, *Compliance is a Culture, Not Just a Policy*, Remarks as Prepared for the International Chamber of Commerce/ United States Council of International Business Joint Antitrust Compliance Workshop (September 9, 2014), *available at http://www.justice.gov/atr/public/speeches/308494.pdf.*

[27] *Infra* text accompanying notes 24-28.

[28] *See* Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act, 14 November 2012, available at http://www. sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf; *see also* OECD Council, "Good Practice Guidance on Internal Controls, Ethics and Compliance," Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transaction, 18 February 2010, available at http://www.oecd.org/investment/anti-bribery/anti-briberyconvention/44884389.pdf; *see also* The World Bank Group, Summary of World Bank Group Integrity Compliance Guidelines, available at http://siteresources.
worldbank.org/INTDOII/Resources/IntegrityComplianceGuidelines_2_1_11web.pdf.)

[29] OECD, Good Practice Guidance on Internal Controls, Ethics, and Compliance (Feb. 18, 2010),

the U.S. Foreign Corrupt Practices Act, designed to outline both the government's policies regarding FCPA enforcement[30] and "the hallmarks of an effective corporate compliance program."[31] Similarly, the United Nations Office on Drugs and Crime ("UNDOC"), published *An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide*, that outlines policy guidelines for developing company preventative measures to detect and deter foreign bribery during international business transactions.[32]

In each guide, companies are encouraged to employ measures designed to prevent and detect misconduct.[33] Although the recommendations are designed to be flexible and tailored to each company's particular risks and resources, they provide similar recommendations, applicable to all companies, regardless of size, industry or risk.[34] For example, most guides consider the following to be necessary components of an effective ethics and compliance program: visible commitments from senior management, a clear corporate policy prohibiting bribery and

---

available at http:// www.oecd.org/investment/anti-bribery/ **233/** anti-briberyconvention/44884389.pdf

[30] *Foreign Corrupt Practices Act (FCPA) Guidance*, United States Department of Justice Fraud Section Website, http://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf (last visited January 6th, 2015).

[31] *Id.*

[32] See The World Bank Group, Summary of World Bank Group Integrity Compliance Guidelines, available at http://siteresources.

[33] *See* Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act, 14 November 2012, available at http://www. sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf; *see also* OECD Council, "Good Practice Guidance on Internal Controls, Ethics and Compliance," Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transaction, 18 February 2010, available at http://www.oecd.org/investment/anti-bribery/anti-briberyconvention/44884389.pdf; *see also* The World Bank Group, Summary of World Bank Group Integrity Compliance Guidelines, available at http://siteresources. worldbank.org/INTDOII/Resources/IntegrityComplianceGuidelines_2_1_11web.pdf.)

[34] Claudia J. Dumas, Fritz Heimann, Shruti Shah, *Verification of Anti-Corruption Compliance Programs*, Transparency International-USA Report, at p. 16-17 (2014)

misconduct, a code of conduct, risk-tailored compliance policies and procedures, risk assessments, robust due diligence and oversight of third parties, confidential reporting and internal investigation procedures, dedication of sufficient resources to the implementation and oversight of the compliance program, ongoing training for employees and relevant third parties, transparent financial and accounting procedures, effective communication and documentation, periodic review and testing of internal controls, and incentives and disciplinary measures for violations of company policies and the law.[35]

In light of the numerous compliance resources available to companies, government regulators and enforcement agencies have little sympathy for companies that claim ignorance about the necessity of an effective compliance program.[36] "They are equally harsh with companies that do compliance "on the cheap" –downloading and adopting the policies and codes of conduct found on the internet, dedicating little to no resources to compliance activities, failing to provide ethics and compliance training to employees, or ignoring red flags of corruption or unethical behavior."[37] Companies that fail to invest in compliance or merely maintain a "paper" compliance program will eventually violate a law—resulting in huge fines, penalties, investigative costs, reputational damage and other related consequences.[38]

c. Compliance Developments in the U.S. Government Procurement System

[35] *Foreign Corrupt Practices Act (FCPA) Guidance*, United States Department of Justice Fraud Section Website, http://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf (last visited January 6th, 2015) at 9-12; Anti Corruption Ethics and Compliance Handbook for Business, OECD, UNODC, The World Bank (2013); An Anti-Corruption Ethics and Compliance for Business- A Practical Guide, United Nations Office on Drugs and Crime (2013).
[36] Tillipman, Jessica, Gifts, Hospitality & the Government Contractor (June 1, 2014). Briefing Papers No. 14-7, June 2014 at 20.
[37] *Id.*
[38] *Id*

The development and implementation of ethics and compliance best practices requires significant resources and political will.[39] While state-of-the-art compliance programs are increasingly prevalent in the commercial sector, robust compliance policies and procedures have always been critical for U.S. government contractors given the myriad laws applicable to their government procurement activities.[40] A contractor's failure to comply with these requirements and obligations can have a devastating impact on the company's reputation and government revenue streams.[41] Not only does a contractor risk the termination of its current contracts, it also faces a multitude of administrative remedies and civil or criminal penalties.[42] Given the staggering consequences of non-compliance, it is no surprise that the United States' largest contractors have invested heavily in developing robust and effective ethics and compliance programs.[43] Indeed, some of the country's largest contractors have been leaders in the development of robust and innovative anti-corruption policies and procedures.[44]

In light of their significant compliance obligations, the comprehensive compliance guides are a significant resource for contractors designing, implementing and refining their internal

[39] Stacey English, Susannah Hammond, *Cost of Compliance* 2014, Thomson Reuters Accelus' Annual Cost of Compliance Survey (2014) at 6.
[40] John D. Altenburg, *Winding Down War Zone Contracts*, National Defense & Technology Magazine (Nov. 2013), *available at http://www.nationaldefensemagazine.org/archive/2013/November/Pages/WindingDownWarZoneContracts.aspx.*
[41] Stacey English, Susannah Hammond, *Cost of Compliance* 2014, Thomson Reuters Accelus' Annual Cost of Compliance Survey (2014) at 6.
[42] *See* 48 C.F.R. §§ 9.406-9.407; *see also* The Foreign Corrupt Practices Act and Global Anti-Corruption Law, Association of Corporate Counsel and Morrison and Foerster FCPA & Anti Corruption Task Force Report (Dec. 2010) at p. 61-67.
[43] Claudia J. Dumas, Fritz Heimann, Shruti Shah, *Verification of Anti-Corruption Compliance Programs*, Transparency International-USA Report, at p. 11-12 (2014)
[44] U.S. Government Accountability Office Report to Congressional Committees, *Defense Contracting Integrity: Opportunities Exist to Improve DOD Oversight of Contractor's Ethics Programs*, GAO-09-591 (2009)(finding that 55 out of 57 defense contracts had ethics programs that are currently standard for compliance prior to the promulgation of the FAR rules) at 3.

compliance programs.[45] They are of particular importance because most government contractors are legally obligated to implement a "Contractor Code of Business Ethics and Conduct."[46] This requirement is designed to ensure that contractors "conduct themselves with the highest degree of integrity and honesty" and maintain a written code of business ethics and conduct.[47] To promote compliance with these policies, the Federal Acquisition Regulations ("FAR") requires contractors to employ an "ethics and compliance training program and an internal control system" that is "(1) suitable to the size of the company and extent of its involvement in Government contracting; (2) Facilitate[s] timely discovery and disclosure of improper conduct in connection with Government contracts; and (3) Ensure[s] corrective measures are promptly instituted and carried out."[48]

The implementation of these "best practices" guidelines and ensuring a comprehensive compliance and ethics program requires substantial integration throughout all levels of the company. Large contractors often have a dedicated ethics and compliance staff that can oversee internal investigations and ensure that internal controls are functioning properly.[49] Firms are under significant pressure to ensure that they have dedicated ample resources and staffing to their compliance department or face "tough questions" from regulators.[50] Further, companies must

---

[45] *See* Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act, 14 November 2012; *see also* OECD Council, "Good Practice Guidance on Internal Controls, Ethics and Compliance," Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transaction, 18 February 2010; *see also* The World Bank Group, Summary of World Bank Group Integrity Compliance Guidelines.
[46] *See generally* FAR 3.10; 52.2013-13.
[47] *See* FAR 3.1002.
[48] FAR 3.1002.
[49] Greg Bingham, John T. Jones, *Costs of Mandatory Ethics and Compliance Programs*, General Dynamics and The Kendrich Group LLC Joint Report (January 2009) p.6; .
[50] Stacey English, Susannah Hammond, *Cost of Compliance* 2014, Thomson Reuters Accelus' Annual Cost of Compliance Survey (2014) at 6.

invest a significant number of hours providing ethics training to employees to ensure that all employees understand the company's legal obligations, as well as its commitment to ethics and compliance. For example, "a typical aerospace and defense employee receives several hours of training each year on ethics and compliance with government contract requirements"—often more than what is typically required of the employees of commercial companies.[51] Training alone can easily cost a defense contractor tens of millions of dollars annually to ensure that all employees have a sufficient understanding of the interplay between government regulations and the daily operations of the business.[52]

While many of the U.S. government's largest contractors have invested heavily in developing robust and sophisticated compliance programs, the government's smallest contractors have lagged far behind.[53] Small businesses may be contractually required by FAR 52.203-13 to maintain a "code of business ethics and conduct" but are exempt from establishing a "a compliance program and an internal controls system."[54] While it is "recommended" that small businesses invest in these important compliance and internal control systems, the small business exemption is in recognition of the burden this requirement places on small businesses.[55] Specifically, unlike larger companies, small businesses "lack the financial resources or even the

[51] Greg Bingham, John T. Jones, *Costs of Mandatory Ethics and Compliance Programs*, General Dynamics and The Kendrich Group LLC Joint Report (January 2009) p.6.
[52] Greg Bingham, John T. Jones, *Costs of Mandatory Ethics and Compliance Programs*, General Dynamics and The Kendrich Group LLC Joint Report (January 2009) p.6.
[53] 2014 Anti-Bribery and Corruption Benchmarking Report: Untangling the Web of Risk and Compliance (2014) at 9 available at http://www.kroll.com/media/pdf/reports/2014_kroll_abc_report.pdf
[54] FAR 52.203-13(c). *See also* See Joseph D. West, et al., "Contractor Business Ethics Compliance Program & Disclosure Requirements, 09-5 Briefing. Papers 1 (Apr. 2009).
[55] See Joseph D. West, et al., "Contractor Business Ethics Compliance Program & Disclosure Requirements, 09-5 Briefing. Papers 1 (Apr. 2009).

market power to enforce the kind of zero tolerance policies" towards corruption.[56] Compared to larger companies, small businesses have far less capital and smaller profit margins to implement compliance programs. As a consequence, some small businesses may feel more pressure to take shortcuts or engage in corrupt practices to obtain greater profit margins.[57] While exempting small businesses from these compliance obligations is understandable given the resources these systems require, the exclusion continues to perpetuate weaknesses in the procurement system.

A 2007 report by UNDOC found that the failure of small and medium-sized ("SMEs") businesses to invest in ethics and compliance signals a significant failure in the system.[58] In contrast to their larger counterparts, SMEs have been much slower to implement or even acknowledge developing best practices in anti-corruption ethics and compliance programs.[59] The most common (and obvious) reason for the lack of SME commitment to compliance is cost.[60] Most small businesses spend their resources just trying to survive. Many view compliance as a luxury—not as an essential aspect of doing business.[61] In 2010, the Small Business Administration reported that small firms with less than 20 employees paid $10,585 per employee to comply with all federal regulations and firms with 20-499 employees paid $7,454 per

[56] Corruption Prevention to Foster Small and Medium Sized Enterprise Development Vol. II, United Nations Industrial Development Organization & United Nations Office on Drugs and Crime Joint Report (2012) at 13.
[57] Corruption Prevention to Foster Small and Medium Sized Enterprise Development Vol. II, United Nations Industrial Development Organization & United Nations Office on Drugs and Crime Joint Report (2012) at 14.
[58] Corruption Prevention to Foster Small and Medium Sized Enterprise Development, United Nations Industrial Development Organization and United Nations Office on Drugs and Crime, Vienna, 2007.
[59] *Id.*
[60] *Id.*
[61] Nicole V. Crain and W. Mark Crain, The Impact of Regulatory Costs on Small Firms, Small Business Administration Office of Advocacy, available at https://www.sba.gov/sites/default/files/The%20Impact%20of%20Regulatory%20Costs%20on%20Small%20Firms%20%28Full%29.pdf.

employee.[62] Given the high cost of compliance, many small businesses have found that working outside regulatory requirements to be more profitable.[63] Indeed, "corruption in business is an economic issue and it will continue as long as the gains from corrupt behavior exceed the expected losses that are in turn closely connected to the probability of being caught."[64]

The failure of small companies to design and implement successful compliance programs may also be attributed to the complexity of the current compliance guidelines.[65] The "hallmarks" of effective compliance programs are often designed with large, multinational companies in mind.[66] While all of the guides make clear that policies and procedures should be tailored to the risks and resources of each particular company, the guidance can be overwhelming to resource-strapped SMEs.[67] The guidance is also decidedly less helpful to small businesses that lack the resources and sophistication necessary to meet these aspirational standards.[68] Many best practices are simply not feasible because the costs required to implement them are too high for resource-constrained entities.[69] Yet, regardless of the financial burden and

---

[62] *Id.*
[63] Tonoyon, Strohmeyer, Habib, Perlitz, *How Formal and Informal Institutions Shape Small Firm Behavior in Mature and Emerging Market Economies*, (2006).
[64] Corruption Prevention to Foster Small and Medium Sized Enterprise Development, United Nations Industrial Development Organization and United Nations Office on Drugs and Crime, Vienna, 2007.
[65] Jane Moscowitz, *Compliance Programs for Small Businesses*, 48 No. 5 Prac. Law. 25 (2002).
[66] *Foreign Corrupt Practices Act (FCPA) Guidance*, United States Department of Justice Fraud Section Website, http://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf (last visited January 6th, 2015) at 9-12; Anti Corruption Ethics and Compliance Handbook for Business, OECD, UNODC, The World Bank (2013); An Anti-Corruption Ethics and Compliance for Business- A Practical Guide, United Nations Office on Drugs and Crime (2013).
[67] *Id.*
[68] 014 Anti-Bribery and Corruption Benchmarking Report: Untangling the Web of Risk and Compliance (2014) at 9 available at http://www.kroll.com/media/pdf/reports/2014_kroll_abc_report.pdf
[69] Greg Bingham, John T. Jones, *Costs of Mandatory Ethics and Compliance Programs*, General Dynamics and The Kendrich Group LLC Joint Report (January 2009) at 9 (finding that a robust

infeasibility of implementing a robust compliance program, the legal risks remain the same. Thus, many small businesses face the same corruption and compliance risks as their large counterparts, but do so without the same level of protection.

While the compliance deficiencies of small businesses are bound to create problems for the small business industry, their failure to invest in ethics and compliance creates significant risks for large companies as well.[70] This is particularly true in the defense industry, where large, multinational contractors depend on small businesses to perform contracts overseas. Although large companies may value and invest in expensive compliance programs, these efforts may be moot when a small company in their supply chain does not have the resources, knowledge or even willingness to invest in compliance.[71]

II. The Risks of Contracting with Small Businesses

While commercial companies may be inclined to avoid risky small businesses that do not invest in ethics and compliance, large government contractors do not have the same luxury.[72] The U.S. government has injected socio-economic policies into its procurement system in an effort to aid in the development of small businesses.[73] Indeed, Congress has made it clear it is the responsibility of the procurement system[74] to protect and promote the interests of small

compliance program even for a small business could amount to $2,000,000 per year to ensure satisfactory ethics, training and internal controls).

[70] Corruption Prevention to Foster Small and Medium Sized Enterprise Development, United Nations Industrial Development Organization and United Nations Office on Drugs and Crime, Vienna, 2007.

[71] *Id.*

[72] *Infra* text accompanying notes 72-83.

[73] *See* Major Patrick E. Tolan Jr., *Government Contracting with Small Business in the Wake of the Federal Acquisition Reform Act, And Adarand: Small Business As Usual*, 44 A.F.L. Rev. 75 (1998); *see also* Andrew George Sakallaris*, Questioning the Sacred Cow: Reexamining the Justifications for Small Business Set Asides*, 36 Pub. Cont. L.J. 685, 687 (Summer 2007).

[74] Small Business Act of 1953, Pub. L. No. 83-163, 67 Stat. 232.

businesses.[75] Through the Small Business Act of 1953, Congress dedicated an entire agency—the Small Business Administration ("SBA")—to the implementation and encouragement of policies that "aid, counsel, assist and protect… the interest of small business concerns in order to preserve free competitive enterprises, to ensure a fair proportion of the total purchases or contracts and subcontracts for property and services for the Government."[76] More importantly, Congress memorialized their support for small businesses by requiring agencies to meet small business contracting goals—targets designed to ensure that a fair proportion of federal contracts are issued to small businesses.[77] Specifically, Congress requires that all agencies must ensure that 25 % of all contracts and that 35.9% of all contract dollars are issued to small business.[78] To meet these goals, contracting officers are required to reserve a certain percentage of total contracts so only small businesses may bid on the opportunities.[79] Typically, a contracting officer must determine whether two or more small business exists offering proposals that do not exceed the market price, quality and delivery.[80] If the CO determines that this is the case, they must "set-aside" the contract for small businesses.[81]

In addition to prime contract set-asides, under certain circumstances, large prime contractors must also preference small businesses as their subcontractors.[82] Specifically, under

[75] Mirit Eyal-Cohen, *Why Is Small Business The Chief Business of Congress*, 43 Rutgers L.J. 1, 3 (Fall 2011/Winter 2012).
[76] 15 U.S.C. § 631(a) (2006).
[77] See Arthur Miller & W. Theodore Pierson Jr., Observations on the Consistency of Federal Procurement Policies with Other Government Policies, 29 Law & Contemp. Probs. 277, 296 (1964).
[78] Government Efficiency through Small Business Contracting Act of 2012, H.R. 3850, §2.
[79] An Act to Amend the Small Business Act and the Small Business Investment Act of 1958, P.L. 95-507, §221, 92 Stat. 1771 (October 24, 1978) (codified at 15 U.S.C. §644(g)(2)).
[80] FAR 19.502-2(b).
[81] FAR 19.501(a).
[82]FAR 19.702.

certain circumstances, prime contractors must "agree in the contract that small business, veteran-owned small business (VOSB), service-disabled veteran-owned small business (SVOSB), Historically Utilized Business (HUBZone) small business, small disadvantaged business (SDB) and women-owned small business (WOSB) concerns will have the maximum practicable opportunity to participate in contract performance consistent with its efficient performance."[83]

Defense contractors have enhanced small business obligations under the Defense Federal Acquisition Regulation Supplement ("DFARS").[84] Further, the Department of Defense ("DoD") is required to ensure that certain techniques such as "bundling,"[85] which may preclude small businesses from bidding on a particular contract, are minimized.[86] While there is a perception that the defense industry excludes small business contractors from the market, in reality, the industry has an affirmative obligation to work with small firms.

a. Impact of Small Business Compliance Failures on the Supply Chain

Despite the important role that small businesses play in the procurement system, their compliance failures can undermine the integrity of the entire system, create liability for their

[83] Office of Navy Research, Science and Technology, "Small Business Subcontracting Plans," available at http://www.onr.navy.mil/en/contracts-grants/small-business/subcontracting-plans.aspx (last visited April 3, 2015).
[84] See, e.g., DFARS 219.502-2.
[85] "Bundling" means—(1) Consolidating two or more requirements for supplies or services, previously provided or performed under separate smaller contracts, into a solicitation for a single contract that is likely to be unsuitable for award to a small business concern…." FAR 2.101.
[86] DFARS 205.205-70; see also Acquisition Process: Task and Delivery Order Contracts, Bundling, 78 Fed. Reg. 191 (October 2, 2013) (finding new regulations are need to ensure that small business as both prime and subcontractors can be considered in rather than excluded from multiple award contracts and acquisitions that are consolidated through bundling); see also U.S. Government Accountability Office Report on Small Business Contracting, Updated Guidance and Reporting Needed for Consolidated Contracts, GAO-14-36 (November 2013) available at http://www.gao.gov/assets/660/659254.pdf; *see also* http://washingtontechnology.com/articles/2010/07/13/bundled-contract-sole-source-reporting.aspx

large-contractor partners, and result in their exclusion from the procurement system. Although the U.S. government does not collect data on the number of small businesses excluded each year due to compliance failures, it is well-known in the industry that small business are more susceptible to debarment because of their limited knowledge of regulatory requirements and "less developed compliance and ethics programs."[87] Moreover, when misconduct is discovered, small businesses "often lack the resources to respond to and remediate harm."[88] When the U.S. government has attempted to reverse this trend by proposing enhancements to small business compliance programs and internal controls, the government contracts industry has pushed back vehemently arguing that the costs would be too burdensome for the small companies.[89]

While small businesses bear the brunt of negative consequences that stem from their compliance deficiencies, they do not operate in a vacuum. Compliance deficiencies can impact the entire supply chain and create significant risks for the large, prime contractors that partner with small firms.[90] Thus, in an effort to minimize risks stemming from compliance deficiencies in their supply chains, many sophisticated contractors dedicate significant resources to the monitoring and oversight of their subcontractors.[91] Large contractors may also invest in ethics and compliance training for some of their small subcontractors to ensure that their business

[87] Dietrich Knauth, *5 Areas of Growing Debarment Risk for Contractors*, Law360, New York (January 13, 2014, 10:49 PM ET) available at http://www.crowell.com/files/5-Areas-Of-Growing-Debarment-Risk-For-Contractors.pdf

[88] Tillipman, Jessica, A House of Cards Falls: Why 'Too Big to Debar' is All Slogan and Little Substance (January 13, 2012). Fordham Law Review Res Gestae, Vol. 80, No. 49, 2012.

[89] FAR Case 2007-006: Contractor Business Ethics Compliance Program and Disclosure Requirements, 73 Fed. Reg. 67064, 67087 (Nov. 12, 2008).

[90] PriceWaterhouseCoopers, *How to Fortify Your Supply Chain Through Collaborative Risk Management* (January 20009), at http://www.pwc.com/us/en/aerospace-defense/assets/pwc-aerospace-scrm-012008.pdf ("A compliance failure at a supplier based anywhere in the world could become a major problem for a contractor".).

[91] FAR Case 2007-006: Contractor Business Ethics Compliance Program and Disclosure Requirements, 73 Fed. Reg. 67064, 67087 (Nov. 12, 2008).

partners are aware of the extensive compliance obligations required under their subcontracts.[92] Unfortunately, oversight and training is not enough to prevent compliance failures—especially where subcontractors have failed to invest time or resources in developing their own compliance programs. This is source of great concern for prime contractors, which may be held liable for the actions of their subcontractors.[93]

Although large contractors continue to work with small businesses in order to meet statutory goals, it is rare that a large company's commitment to small businesses extends beyond their minimum requirements.[94] Indeed, many large corporations have typically "shied away from small suppliers because of the sense that they are untested, less reliable and more likely to go out of business."[95] This not only undermines the government's long-term strategic goals of enhancing opportunities for small businesses, it handicaps opportunities for large businesses to partner with new and potentially more innovative firms.

b. Sharing Compliance Best Practices

The defense industry has made very visible commitments to elevating ethics and compliance in the industry. Many of the world's largest defense contractors are making great strides in establishing global ethics and compliance standards through their participation in organizations and forums dedicated to these issues.[96] For the past five years, the aerospace and

---

[92] Aaron Grieser, *The Outer Limit of Global Compliance Programs: Emerging Legal & Reputational Liability in Corporate Supply Chains*, 10 Or. Rev. Int'l L. 285, 312 (2008).
[93] *Id.*
[94] Lockheed Martin is the only large defense contractor to provide direct assistance and use of internal corporate ethics resources to their suppliers. http://www.lockheedmartin.com/us/suppliers/ethics.html
[95] Mark Foggin, *Breaking into the Corporate Supply Chain* at 16, a*vailable at* https://nycfuture.org/pdf/Breaking_into_the_Corporate_Supply_Chain.pdf.
[96] *See*, e.g., Defense Industry Initiative,www.DII.org, United Nations Global Compact and International Forum on Business Ethical Conduct for the Aerospace and Defence Industry, http://ifbec.info.

defense industries have held an annual conference attended by industry members, government representatives, and non-governmental organizations in an effort to share compliance "best practices" and to "promote trust and integrity."[97] Further, the Defense Industry Initiative ("DII") Working Group[98] has hosted an annual forum of over "300 industry professionals and U.S. Government officials to share best practices and discuss current issues related to ethics and compliance."[99] The DII Working Group has also developed a "model supplier code of conduct" designed to articulate the "expectations" DII holds for suppliers throughout the industry.[100] It also serves as a resource for small and medium-sized contractors "seeking to streamline the processes by which they agreed to individual contractors' codes of conduct when doing business with other DII members."[101] DII has also developed a "supplier toolkit" that has been "designed to give SMEs the necessary guidance on creating effective ethics and compliance programs."[102] These examples make clear that defense industry members are actively collaborating with each other to share anti-corruption, ethics and compliance best practices.

While these forums and public initiatives certainly convey a willingness to share information about ethics and compliance practices, the specific details of company compliance programs are not always publicly available. A 2012 Transparency International U.K. Defence

[97] International Forum on Business Ethical Conduct for the Aerospace and Defence Industry 5th Annual Conference Report [hereinafter "IFBEC Report"] at 1.
[98] The Defense Industry initiative is a non-profit organization with "seventy-seven signatory companies comprising the top U.S. defense and security companies. . . [the organization seeks]the continued promotion and advancement of a culture of ethical conduct in every company that provides products and services to the United States Armed Forces." See http://www.dii.org/about-us.
[99] *Id.* at 3.
[100] DII Model Supplier Code of Conduct, *available at* *http://www.dii.org/resources/dii-model-supplier-code-conduct.*
[101] IFBEC Report at 3.
[102] *Id.*

and Security Programme report noted that over half of companies involved in the organization's study had not shared information publicly about their anti-corruption policies or even whether their ethics programs meet the industry best practices.[103] Additionally, although the defense industry regularly hosts ethics and compliance conferences and forums, the events are generally closed to the public.

The hesitancy to share this information publicly is understandable given the significant investment large contractors make in designing and implementing their ethics and compliance programs. Some of the largest contractors are unwilling to share detailed information about their sophisticated programs because they view their programs as proprietary and confidential. Many contractors (understandably) fear that competitors will exploit this information if they share it publicly. Yet, by depriving small businesses of access to this information, the large contractors may ultimately be harmed if their suppliers suffer from compliance deficiencies or failures.

II. Incentivizing the Sharing of Resources and Guidance

The entire supply chain benefits when contractors at all tiers view ethics and compliance as a critical component of their business. While enhanced supply chain integrity may incentivize some large businesses to share compliance best practices with their suppliers, many large contractors continue to keep this information confidential. Although the defense industry is increasingly committed to sharing guidance and resources with small businesses and suppliers, the amount and type of information shared varies greatly among industry members.

Some of the largest government contractors have decided to invest significant time and resources into helping elevate the ethics and compliance programs of their suppliers. For

[103] Mark Pyman, Tiffany Clark, Saad Mustafa and Gareth Somerset, Defence Companies Anti-Corruption Index 2012, Transparency International UK Defence and Security Programme, London, U.K. (October 2012)

example, Lockheed Martin has created an "Ethics Supplier Mentoring Program" as a means to ensure that the company's suppliers maintain similarly robust ethics and compliance programs.[104] Per Lockheed's website, the goal of the program is to share "best practices, resources, and experiences, all with the aim of creating a more robust ethics program throughout the supply chain."[105] The program "includes an objective review of the supplier's existing Ethics & Business Conduct program, and recommendations for improvement. Each company is partnered with one or more Ethics Officers, who is available as a resource throughout the program."[106]

Lockheed's attempt to enhance the ethics and compliance programs of its suppliers not only reduces the risk of a compliance failure in the supply chain; it also enhances the overall integrity of the procurement system. If other large and sophisticated contractors were to implement a similar program, it could have a dramatic impact on the integrity of the U.S. government contracts regime. Unfortunately, not all contractors are willing to spend the time and resources necessary to mentor their suppliers on ethics and compliance best practices. It is clear that additional incentives are necessary to foster increased information sharing among the companies. Fortunately, a template for incentivized information sharing already exists in the U.S. procurement system: the "mentor-protégé program." If implemented in the ethics and compliance context, this model could provide lasting benefits to the entire procurement system.

a. The Model: Federal Mentor Protégé Programs

[104] *See* http://www.lockheedmartin.com/us/suppliers/ethics.html.
[105] *Id.*
[106] *Id.*

In 1991, the FAR Council created mentor-protégé assistance programs to provide small businesses with resources and support in the federal procurement sector.[107]

> A mentor-protégé program is an arrangement in which mentors—businesses, typically experienced prime contractors—provide technical, managerial, and other business development assistance to eligible small businesses, or protégés. In return, the programs provide incentives for mentor participation, such as credit toward subcontracting goals, additional evaluation points toward the awarding of contracts, an annual award to the mentor providing the most effective developmental support to a protégé, and in some cases, cost reimbursement. [108]

Ideally, mentors and protégées work in conjunction "to create a developmental assistance agreement."[109] The purpose of the agreement is to ensure that the large business trains the smaller business on industry specific subjects,[110] provides assistance in obtaining required federal contract certifications, advises on issues related to contract administration and guides the smaller company on general business and organizational management skills.[111] Through these initiatives, the U.S. government hopes to develop and produce businesses that are able to function independently in the federal contracting system.[112]

The mentor-protégé program depends on the willingness of experienced and sophisticated contractors to serve as mentors to smaller companies. Thus, the U.S. government provides

[107] U.S. Government Accountability Office, Implementation of the Pilot Mentor-Protégée Program, GAO/NSLAD-94-101 (February 1994).
[108] Letter to the Honorable Mary L. Landrieu, Committee on Small Business and Entrepreneurship, *Mentor-Protégé Programs Have Policies That Aim to Benefit Participants but Do Not Require Post agreement Tracking*, U.S. Government Accountability Office, GAO-11-548R (July 15, 2011)
[109] *Id.*
[110] U.S. Government Accountability Office, Implementation of the Pilot Mentor-Protégée Program, GAO/NSLAD-94-101 (February 1994) (including production, quality control, manufacturing, engineering, and computer hardware and software).
[111] U.S. Government Accountability Office, Implementation of the Pilot Mentor-Protégée Program, GAO/NSLAD-94-101 (February 1994).
[112] Keir X. Bancroft, *Regulating Information Security in the Government Contracting Industry*, 62 Am. U. L. Rev. 1145, 1192 (2013).

various incentives to encourage large businesses to participate in the program.[113] The incentives are typically financial and contractual advantages that may be used to obtain or enhance procurement opportunities.[114] This may include credit towards a prime contractor's mandatory subcontracting goals,[115] additional evaluation points that increase a prime's likelihood of winning a contract, or an annual monetary award to mentors who prove that their development support has been beneficial to the protégé.[116]

Other agencies may provide additional incentives. For example, DoD allows prime contractor mentors to collect reimbursements for certain costs that are incurred while providing mentorship to their protégés.[117] The Departments of Energy, Homeland Security and NASA provide prime contractors with award fees[118] in recognition of successful mentor protégé developments.[119] Additionally, the Small Business Administration's program permits large companies to work on contracts that are specifically set-aside for small businesses if they serve

[113] Letter to the Honorable Mary L. Landrieu, Committee on Small Business and Entrepreneurship, *Mentor-Protégé Programs Have Policies That Aim to Benefit Participants but Do Not Require Post agreement Tracking*, U.S. Government Accountability Office, GAO-11-548R (July 15, 2011)

[114] *Id.*

[115] A credit allows prime contractors to count costs incurred during mentorship as if they were incurred in a subcontract awarded to their protégé. *See Evaluating Federal Mentor-Protégé Programs: Assessment, Case Studies and Recommendations*, National Women's Business Council Advisors to the President, Congress and the SBA, p. 7 (April 2011). This allows large businesses to better meet their subcontracting goals. *Id.*

[116] *Id.*

[117] DFARS I-109(d) (permitting mentors to seek reimbursement of costs up to $1,000,000 for costs of assistance furnished to a protégé firm each fiscal year).

[118] An award fee functions as a monetary bonus for any costs that are saved or for performance that is beyond satisfactory and is used to motivate the contractor to provide optimum performance in critical areas. *See* U.S. Department of Air Force Award Fee Guide (2008) available at http://www.acq.osd.mil/dpap/ccap/cc/jcchb/Files/Topical/1Restricted/award.fee.oct08.pdf

[119] 48 C.F.R. 919.7006(a) (March 26, 2015)); see also 48 C.F.R. 1819.7201(b) (March 26, 2015)); see also 48 C.F.R. 819.7105(d) (March 26, 2015).

as a mentor to the small business in the contract.[120] These incentives are designed to provide prime contractors with opportunities that are normally barred by other federal contracting policies to sweeten the deal for providing assistance to these small businesses. The ultimate advantage of these special arrangements is that "mentors benefit from a strengthened cadre of subcontractors and [the agency] benefits from a resultant robust and competitive supplier base."[121]

b. The Compliance Mentor-Mentee Program

The existing mentor-protégé program provides a template that could help narrow the compliance gap that currently plagues the procurement system. This model of information sharing in exchange for financial and contractual incentives is a proven concept that could be implemented in the compliance context with modest effort and resources. The application of this program in the ethics and compliance setting could encourage the sharing of expertise and resources by large contractors with their small, less sophisticated counterparts.

This template could benefit both small and large companies for several reasons. First, the mentee will benefit from the compliance guidance and resources shared by the mentor. By sharing resources and offering guidance, the mentor can help elevate the mentee's ethics and compliance program to better reflect industry best practices. It will also help the mentee identify potential areas of corruption risk –a task that will likely benefit the entire supply chain. While specific ethics and compliance goals would be established at the outset of the program, mentors would be expected to help the protégé (1) design a compliance program tailored to the protégé's

[120] 13 C.F.R. § 124.50 (2010) (granting a SBA mentor and protégé relationship authority to enter a joint venture as a small business for any government prime contract or subcontract including those set aside for companies who meet certain small business size standards).
[121] GAO Report 01-767

specific size, industry and risk profile, (2) develop a comprehensive and effective training program, and (3) draft tailored policies and procedures. Mentors would also be expected to share resources and guidance on an ongoing basis, thus eventually enabling the mentee to maintain an effective, internal compliance program.

In addition to the benefits afforded to the mentee firms, mentors would also be rewarded for the time and energy spent guiding the mentee. In addition to the incentives inherent in reducing risks in the supply chain, the program will provide mentors with significant financial and contractual incentives, such as award fees and access to certain set-aside contracts. This will allow large companies to benefit from additional contracting opportunities while simultaneously promoting a more ethical and compliant procurement process. This could be particularly profitable for large companies given the significant resources they allocate to their compliance functions. While the costs of sharing best practices would be minimal, the financial incentives and enhanced market access could be quite lucrative.

Developments in the defense industry suggest that this approach could be embraced as a positive movement towards a more collaborative and transparent system. As previously noted, Lockheed Martin has developed a similar model in order to ensure ethics and compliance best practices are implemented throughout the company's supply chains.[122] Lockheed's "Ethics Supplier Mentoring Program" demonstrates the significant strides that could be made if large contractors regularly partnered with small contractors to help them enhance their ethics and compliance programs. According to Lockheed's website, their program provides, among other things, (1) an objective review of the supplier's existing ethics program, (2) recommendations

[122] 2014 Supplier Ethics Letter, Ethics Supplier Mentoring Program available at http://www.lockheedmartin.com/us/suppliers/ethics.html

for improvements (3) a direct mentor from their Office of Ethics and Business Conduct to train the supplier for six months, (4) access to internal Lockheed Martin ethics resources, and (5) the opportunity to benchmark the company's compliance program against Lockheed's program.[123] This comprehensive system demonstrates that tangible benefits that a small business may derive from its "ethics and compliance" partnership with a large and sophisticated contractor.

To maximize the proposed program's effectiveness, it will be necessary for the government to dedicate resources to ensuring that the mentor-firm is providing sufficient guidance and assistance to the mentee. It is also critical that mentors are properly screened to ensure that they are joining the program to further the program's policy goals—not to exploit the incentives at the expense of the mentee firms. While no government program is immune from abuse, safeguards will be necessary to prevent and deter the potential manipulation of the program.

Fortunately, lessons may be drawn from audits of the existing mentor-protégé program. For example, a 2007 audit of the DoD Mentor-Protégé Program indicates that in some instances, mentors have benefited from the program's procurement and financial incentives, but have failed to provide adequate procurement guidance to their protégé.[124] Dissatisfied protégé firms have pointed to a "lack of mentor commitment to the program, [the] mentor's failure to meet the objectives of mentor-protégé agreements and costs that exceeded the return for participation."[125] While some concerns with the existing mentor-protégé program exist, the audit also found that

[123] 2014 Supplier Ethics Letter, Ethics Supplier Mentoring Program available at http://www.lockheedmartin.com/us/suppliers/ethics.html
[124] United States Gov't Accountability Office Report: Contract Management Protégés Value DOD's Mentor Protégé Program, but Annual Reporting to Congress Needs Improvement, GAO-07-151 (Jan. 31, 2007).
[125] *Id.*

DoD's mentor-protégé program enhanced the overall capabilities of 93% of the 48 protégés involved in the program.[126]

The lessons learned from past experiences in the mentor-protégé program, coupled with developments in industry "ethics and compliance mentoring programs," demonstrate that this model could be extremely beneficial in the ethics and compliance setting, so long as sufficient safeguards are put in place.[127] Not only would front-end screening of prospective participants be an essential component of the program, the government would need to install a back-end verification process to ensure all parties have maintained their commitments. With screening and oversight mechanisms in place, the impact of this program on small business ethics and compliance programs could be significant.

III. Conclusion

A "compliance mentor-mentee program" could successfully foster the development of small business ethics and compliance programs. With appropriate safeguards in place, the potential improvements to the overall integrity of the procurement system could be significant. The program could greatly reduce supply chain risks and enhance the overall ethics and compliance practices of a chronically weak segment of the procurement system. By incentivizing ethics and compliance at all levels of the supply chain, a "compliance mentor-mentee program" could substantially enhance the U.S. procurement system by ensuring that the government's business partners, large and small, are responsible, ethical and compliant.

[126] *Id.*
[127] *Id.*

Mandatory Disclosure: A Case Study in How Anti-Corruption Measures Can Affect Competition in Defense Markets

Christopher R. Yukins

Lynn David Research Professor in Government Procurement Law and
Co-Director, Government Procurement Law Program,
The George Washington University Law School

A paper to be presented at the conference,
"Ethical Dilemmas in the Global Defense Industry,"
University of Pennsylvania Law School
April 16, 2015

ABSTRACT: In the U.S. defense procurement market, regulators require contractors to make "mandatory disclosures" if principals at those firms determine, after due review, that there is credible evidence that the firms engaged in certain crimes (fraud, bribery or gratuities), civil fraud, or significant overpayment by the government. Failure to make such a mandatory disclosure, required by clause and by regulation, can lead to (among other things) the debarment of the contractor -- a potentially devastating result. Mandatory disclosure is a natural extension of a separate requirement, that contractors maintain effective corporate compliance and ethics systems, and the Defense Department's largest prime contractors, with sophisticated compliance systems in place, have been able to accommodate the mandatory disclosure requirement. This paper asks whether this disclosure requirement in effect favors those largest contractors, and decreases competition in a already highly concentrated defense market, either by creating substantial legal risks for firms too small or inexperienced to institute effective compliance and disclosure systems, or by discouraging competition from other companies in the commercial sector. The paper concludes that the mandatory disclosure rule can impair competition in defense procurement, and recommends that regulators carefully shape any disclosure requirements, and perhaps reconsider relying on voluntary disclosure, mindful of the need to reduce costs and enhance competition in defense procurement markets.

I. Introduction

In U.S. defense contracting, an increasingly important tool in fighting corruption is "mandatory disclosure" -- the requirement that when managers at a contracting firm discover that the firm has been engaged in certain wrongdoing, they must disclose that wrongdoing to the government.[1] Mandatory disclosure plays an especially prominent role in defense contracting,

[1] The clause at Federal Acquisition Regulation (FAR) 52.203-13, 48 C.F.R. § 52.203-13, *Contractor Code of Business Ethics and Conduct*, requires that a contractor, as part of its system of internal controls, make:

Footnote continued on next page

both because of the relative size of the defense spending in overall federal procurement, and because a handful of very large prime contractors, with extraordinarily strong compliance and disclosure systems, dominate the U.S. defense marketplace. In part because those large contractors set a high norm for disclosure, which other contractors have difficulty matching, the U.S. defense market raises an interesting quandary: does mandatory disclosure, an important anti-corruption tool, in effect dampen competition in a procurement market?

This brief paper addresses that question in several steps. Part II of the paper reviews the history of mandatory disclosure in federal contracting, and explains how mandatory disclosure is tied to broader compliance requirements in U.S. contracting. Part III discusses some of the anti-competitive effects of mandatory disclosure, and Part IV assesses possible remedies. Part V concludes by suggesting that mandatory disclosure, like other anti-corruption efforts, should be carefully structured to reduce its negative effects on competition.

II. Mandatory Disclosure -- Background

Mandatory disclosure in federal contracting grew out of two separate initiatives: an effort to find a replacement for *voluntary* disclosures (which had largely failed in defense contracting), and a broader effort to establish *compliance systems* for federal contractors.[2]

Footnote continued from previous page

> (F) Timely disclosure, in writing, to the agency OIG [Office of Inspector General], with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of any Government contract performed by the Contractor or a subcontractor thereunder, the Contractor has credible evidence that a principal, employee, agent or subcontractor of the Contractor has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violation of the civil False Claims Act (31 U.S.C. 3729-3733).

Under FAR 9.406-2(b)(vi), 48 C.F.R. § 9.406-2(b)(vi), *Causes for Debarment*, a debarring official may debar a contractor, based upon a preponderance of the evidence, for:

> Knowing failure by a principal, until 3 years after final payment on any Government contract awarded to the contractor, to timely disclose to the Government, in connection with the award, performance, or closeout of the contract or a subcontract thereunder, credible evidence of—
>
> (A) Violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code;
>
> (B) Violation of the civil False Claims Act (31 U.S.C. 3729-3733); or
>
> (C) Significant overpayment(s) on the contract, other than overpayments resulting from contract financing payments . . . .

[2] For a widely respected monograph on the contractor compliance and mandatory disclosure requirements, see *Guide to the Mandatory Disclosure Rule: Issues, Guidelines, and Best Practices* (Frederic M. Levy & Robert F. Huffman, eds., American Bar Association 2010).

The predecessor to mandatory disclosure -- the Voluntary Disclosure Program -- was launched by the federal government in July 1986,[3] shortly before the "Illwind" procurement scandals which swept up many major defense contractors.[4] The Voluntary Disclosure Program reflected an attempt to formalize, and thus open to a broader set of contractors, a practice of informal, voluntary disclosures which the major defense contractors were already making.[5]

Voluntary disclosure under the formal program was a very cumbersome process, with uncertain benefits for those that made disclosures; the Justice Department, the Defense Department and other enforcement entities retained substantial discretion to decide what impact, if any, a voluntary disclosure would have on a contractor's eventual punishment, and voluntary disclosure risked triggering additional liability from whistleblowers (or "relators") under the federal False Claims Act.[6] The Voluntary Disclosure Program declined in popularity. When the mandatory disclosure rule was proposed at the Justice Department's request in 2007, therefore, the Justice Department's core goal was to replace the fraud and corruption cases which were no longer emerging through the Voluntary Disclosure Program.[7]

It should be stressed, however, that when the proposed rule requiring mandatory disclosure rule was published in November 2007, it came as something of a surprise to the federal contracting community.[8] The Federal Acquisition Regulation (FAR) councils had earlier published a proposed rule, in February 2007, which addressed contractor compliance requirements alone, and built on earlier, agency-specific requirements for such compliance

[3] *See, e.g.*, Inspector General, U.S. Department of Defense, *The Department of Defense Voluntary Disclosure Program*: *A Description of the Process* (Apr. 1990), *available at* http://www.dodig.mil/iginformation/archives/vdguidelines.pdf.

[4] *See, e.g.*, Timothy M. Cox, *Is the Procurement Integrity Act "Important" Enough for the Mandatory Disclosure Rule? A Case for Inclusion*, 40 Pub. Cont. L.J. 347, 371-74 (2011); *In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569, 570 (8th Cir. 1988) (discussing broad "Illwind" investigation disclosed by search warrants executed on over 40 locations on June 14, 1988).

[5] *See* Letter of Deputy Secretary of Defense William H. Taft, IV, July 24, 1986 ("a number of major Defense contractors have adopted a policy of voluntarily disclosing problems affecting their corporate contractual relationship with the Department of Defense"), *reproduced in The Department of Defense Voluntary Disclosure Program*: *A Description of the Process*, *supra* note 3, App. A.

[6] *See generally* Robert S. Ryland, *The Government Contractor's Dilemma: Voluntary Disclosures As the Source of Qui Tam Litigation*, 22 Pub. Cont. L.J. 764 (1993).

[7] 72 Fed. Reg. 64019, 64020 (Nov. 14, 2007) ("According to DoJ, the requirement for mandatory disclosure is necessary because few companies have actually responded to the invitation of DoD that they report or voluntarily disclose suspected instance of violations of Federal criminal law relating to the contract or subcontract.").

[8] For a discussion of how the mandatory disclosure rule emerged in the government's rulemaking process, see, for example, Brian D. Miller, *The Federal Acquisition Regulation Mandatory Disclosure Rule Program at the U.S. General Services Administration Office of Inspector General*, at 2-4 (updated June 2012), *available at* http://www.gsaig.gov.

systems.[9] The compliance systems requirement was not a surprise; as many commentators outside the government had noted, corporate compliance systems were already called for by the U.S. Sentencing Commission's organizational sentencing guidelines, and so extending those requirements to contractors was a predictable next step.[10] In response to the request from the Justice Department, however, the FAR councils in November 2007 published a broader proposed rule, which called for both contractor compliance systems *and* mandatory disclosure.[11] The mandatory disclosure requirement became part of the final combined rule in November 2008, and that final rule took effect on December 12, 2008.[12]

While it applied to contracts awarded by all agencies (not just the Defense Department), the new mandatory disclosure rule drew on many elements of the prior voluntary disclosure program. Disclosures under the mandatory compliance rule are to be processed through the contracting agency, which is to report violations, as appropriate, to the appropriate enforcement authorities, including suspension and debarment officials. As with the voluntary disclosure program, disclosures and enforcement are to turn on whether there is "credible evidence" of a bad act.[13] The mandatory disclosure rule calls for disclosures of *specific bad acts*, and the new rule leaves it to the *contractor*, after due investigation (potentially under an attorney-client privilege), to determine in the first instance whether there is credible evidence of the enumerated bad acts. The mandatory disclosure rule notably does *not* require disclosure of *other*, non-enumerated forms of bad acts, such as violations of the Procurement Integrity Act -- even though that law was born of the same procurement scandals which emerged alongside the voluntary disclosure rule.[14]

The mandatory disclosure rule, unlike its predecessor, does not explicitly incentivize disclosure; a contractor will not necessarily win a reduced sentence by making a mandatory disclosure. But if a contractor *fails* to make a mandatory disclosure -- *i.e.*, if a contractor's principals have credible evidence of an enumerated bad act and the contractor fails to disclose that information -- the contractor may be suspended or debarred, on that ground alone.[15]

---

[9] 72 Fed. Reg. 7588 (Feb. 16, 2007).

[10] *See, e.g.*, Christopher R. Yukins, *Ethics in Procurement: New Challenges After A Decade of Reform*, Procurement Law., Spring 2003, at 3.

[11] 72 Fed. Reg. 64019 (Nov. 14, 2007).

[12] 73 Fed. Reg. 67064 (Nov. 12, 2008).

[13] *Compare The Department of Defense Voluntary Disclosure Program*, *supra* note 3, at 3, *with* 73 Fed. Reg. at 67073 (discussion of adoption of "credible evidence" standard in final rule, per Justice Department input).

[14] *See generally* Timothy M. Cox, *supra* note 4 (discussing omission of the Procurement Integrity Act from list of enumerated statutes).

[15] Applicable regulations are set forth in footnote 1, *supra*. The standards for potential suspension parallel those for debarment, which are set forth in the footnote.

It is important to stress how mandatory disclosure is intertwined with the corporate compliance requirements, which were made part of the same rule. The mandatory disclosure rule assumes that a contractor's compliance system will survey for, and detect, bad acts, and that those bad acts were will be reported up through the firm so that the bad acts can be assessed and then, as appropriate, reported to the government. The mandatory disclosure rule thus arguably rests on an assumption that contractors will have an effective compliance system in place.

Experience under the mandatory disclosure rule has been mixed. While some contractors have tried to mitigate risk by reporting many possible violations to the government -- from petty to major violations -- other contractors have reportedly taken a much narrower approach to disclosure under the rule.[16] What is clear, however, is that mandatory disclosure is taken very seriously by mature defense contractors, including, especially, the handful of large prime contractors at the core of the defense market, and that those contractors cognizant of the requirement take careful steps to integrate disclosure into their broader compliance efforts.[17]

The mandatory disclosure requirements for contractors also can be read against the backdrop of disclosures required of publicly traded companies, under the securities law reforms enacted in the early 1930s. The mandatory disclosures required by those laws were intended to reshape the balance of power between shareholders and managers in publicly traded firms, by forcing managers to open corporate governance by broadening shareholders' access to information. These disclosure requirements under the securities laws were born of unique cultural, historical and political circumstances in the United States, which favored disclosure to support the common investor in the wake of the financial crash of 1929.[18]

Viewed in this light, the mandatory disclosure requirements under the FAR can be seen as an analogous effort to redraw the agency relationship, not between managers and shareholders, but instead between the government and its contractors.[19] There is a natural

---

[16] *See, e.g.*, David Robbins, *Embracing Mandatory Disclosure Can Save Contractors Time, Trouble and Legal Fees*, National Defense, June 2014, *available at* http://www.nationaldefensemagazine.org/archive/2014/June/Pages/EmbracingMandatoryDisclosureCanSaveContractorsTime,TroubleandLegalFees.aspx.

[17] For a practical discussion of the tactical concerns that drive contractors' disclosure decisions, see Frederic Levy & Todd Canni, McKenna Long & Aldridge, *Suspension or Debarment: Are They in Your Future? Government Contractor Compliance Risk Areas for 2013, available at* https://www.mckennalong.com/publications-advisories-3211.html.

[18] *See, e.g.*, James A. Fanto, *The Absence of Cross-Cultural Communication: SEC Mandatory Disclosure and Foreign Corporate Governance*, 17 Nw. J. Int'l L. & Bus. 119, 137-39 (1996) (citing Paul G. Mahoney, *Mandatory Disclosure As A Solution to Agency Problems*, 62 U. Chi. L. Rev. 1047 (1995)).

[19] *See generally* Christopher R. Yukins, *A Versatile Prism: Assessing Procurement Law Through the Principal-Agent Model*, 40 Pub. Cont. L.J. 63 (2010), http://ssrn.com/abstract=1776295.

asymmetry of information between the government and its contractors, which opens the door for strategic behavior -- including, potentially, fraudulent and corrupt behavior -- by the contractors. By forcing mandatory disclosure of information on bad acts, the government has broken down that asymmetrical relationship, at least in part.

This leads, in turn, to a number of important questions. Why, for example, did the government choose *these* bad acts -- why not require disclosure, for example, of all production failures (even if they do not constitute fraud), or of violations of other important anti-corruption measures, such as the Procurement Integrity Act, the Anti-Kickback Act or the covenant against contingent fees? More broadly for our purposes here, how and why does *this* system of mandatory disclosure affect competition in procurement markets (most specifically, the defense market), and what can be done to ease its potentially anticompetitive effects?

III. Anti-Competitive Effects of Mandatory Disclosure

As noted, changes to the securities laws of the 1930s forced new mandatory disclosures in financial markets, in order to *radically reshape* agency relationships between management and shareholders, by reducing the informational advantage that managers held. In contrast, as was described above, the mandatory disclosure rule imposed on contractors in 2008 was arguably an *evolutionary* measure, which did not reorder but instead reinforced existing competitive advantages held by the Defense Department's largest contractors, and bolstered existing reputational bonds between the Defense Department and those large firms. This section assesses those practical effects of the mandatory disclosure rule, and their potentially anti-competitive effects.

A. Mandatory Disclosures Depend on Effective Compliance Systems -- Which the Largest Contractors Have Been Building for Decades

To understand mandatory disclosure's potential anti-competitive effect, it is important to stress that mandatory disclosure depends, first, on an *effective compliance system*. Without an effective compliance system, information on apparent violations -- the stuff of mandatory disclosures -- typically will not "bubble up" to management's attention, except by accident. Put another way, without an effective compliance system in place, a contractor runs material risk of *not* being able to meet its mandatory disclosure obligation if, indeed, the firm engages in one of the prohibited acts (criminal or civil fraud, bribery, etc.).

The standards for compliance systems are remarkable uniform across borders,[20] both inside and outside procurement markets. As the following chart illustrates, countries and

[20] For different perspectives on these common international standards, see, for example, Thomas Fox, *What Are the Essential Elements of a Corporate Compliance Program?* (May 23, 2013), *available at* http://www.lexisnexis.com/legalnewsroom/corporate/b/fcpa-compliance/archive/2013/05/23/what-are-the-essential-

Footnote continued on next page

standards-setting organizations across the world require the same basic elements -- including a code of conduct, training, etc. -- in corporate compliance systems:

CORPORATE COMPLIANCE: INTERNATIONAL HARMONIZATION					
Elements of Corporate Compliance Systems	**U.S. Sentencing Commission: Organizational Sentencing Guidelines**	**U.S. Federal Acquisition Regulation (FAR): Contractor Compliance Requirements**	**UK Ministry of Justice: Compliance Under UK Bribery Act**	**Organisation for Economic Cooperation & Development (OECD)**	**International Chamber of Commerce (ICC)**
Standards and procedures	√	√	√	√	√
Knowledgeable leadership	√		√	√	√
Exclude risky personnel	√	√	√	√	√
Training	√	√	√	√	√
Monitor, evaluate, reporting hotline	√	√	√	√	√
Incentives and discipline	√	√	√	√	√
Adjust program to risk	√	√	√	√	√

Although these harmonized standards mean that multinational firms bear lower costs of compliance across borders, the costs of *establishing and maintaining* an effective compliance and ethics system (however uniform) should not be underestimated.[21]

Footnote continued from previous page
elements-of-a-corporate-compliance-program.aspx (discussing presentation of Paul McNulty & Stephen Martin, Baker & McKenzie).

[21] *See, e.g.*, Stacey English & Susannah Hammond, *Cost of Compliance 2014 Survey* (Thomson Reuters Accelus), *available at* http://accelus.thomsonreuters.com/sites/default/files/GRC00814.pdf. For an interesting alternative viewpoint, on how small businesses can establish ethics and compliance systems at almost no cost, see Joseph E.

Footnote continued on next page

Though corporate compliance systems were first mandated in federal contracting in 2008, major contractors began to implement compliance systems (also known as corporate integrity systems) many years earlier, driven in important part by the defense industry's corruption scandals (laid bare by the Justice Department's "Illwind" investigation) of the 1980s.[22] The large contractors that had embraced corporate compliance and ethics programs therefore were well-prepared for the compliance requirements mandated by regulation in 2008, and for the mandatory disclosure requirements that flowed from those compliance requirements. As a practical matter, however, it is widely believed in the federal procurement community that hundreds, if not thousands, of small- and medium-sized defense contractors did not have (and do not have) effective compliance and ethics systems in place, and thus cannot readily meet the mandatory disclosure requirements of the law.[23]

The risks of *not* having an effective compliance system are magnified by the unique anti-fraud/anti-corruption laws governing federal contracting -- many of which trigger the mandatory disclosure rule. For example, when the rule requires disclosure of any violation of "Federal criminal law involving fraud, conflict of interest, bribery or gratuity violations found in Title 18 of the United States Code," this sweeps up personal conflicts of interest under 18 U.S.C. § 208,

---

Footnote continued from previous page
Murphy, *A Compliance & Ethics Program on a Dollar a Day: How Small Companies Can Have Effective Program*s (Aug. 2010), *available at* http://www.corporatecompliance.org/Portals/1/PDF/Resources/CEProgramDollarADay-Murphy.pdf.

[22] *See, e.g.*, Nancy B. Kurland, *The Defense Industry Initiative: Ethics, Self-Regulation, and Accountability*, 12 J. Bus. Ethics 137 (1993). A later report summarized the evolving efforts, through these years, to build compliance programs in the defense industry:

> Large U.S. companies engaged as defense contractors with various branches of the U.S. military continued to be accused of fraudulent practices spawning federal government demands for a more comprehensive ethics and compliance program by many U.S. corporations. These firms revised their code of ethics, created employee ethics training programs and established internal processes for auditing employee practices, particularly with regards to pricing of products to the government. Many of these ethics and compliance program revisions or improvements were in response to the threats by the federal government to terminate all contracts in the future if changes were not made . . . .

James Weber & David M. Wasieleski, *Corporate Ethics and Compliance Programs: A Report, Analysis and Critique*, 112 J. Bus. Ethics Business Ethics 609, 611 (2012).

[23] Although contractors working under smaller contracts (under $5 million) are technically exempt from the compliance system requirements of the contract clause at FAR 52.203-13, *see* FAR 3.1004(a), 48 C.F.R. § 3.1004(a), if a contractor under such a small contract (typically a small business) fails to disclose the covered bad acts (including fraud and corruption), under FAR Subpart 9.4, that contractor risks potential suspension or debarment. In other words, while contractors on smaller procurements bear risk because they must disclose certain bad acts, under the terms of the rule itself those businesses may well *not* have a compliance system in place to screen for and identify those bad acts.

which can be highly technical and difficult to detect, with no *de minimis* exception[24] but with a complex set of regulatory safe harbors.[25] Nor are the civil fraud requirements easy to meet: whereas common law fraud normally requires *intentional* fraud to trigger liability,[26] under the federal false claims act mere *recklessness* is enough.[27] Thus, a firm's aggressive recruiting of retiring government employees (which can be criminal under 18 U.S.C. § 208),[28] or sloppy accounting or production methods (which can constitute reckless fraud), all may trigger liability, and thus an obligation to report under the mandatory disclosure rule. This means, in turn, that a firm without an effective compliance system in place -- a firm, in other words, in the mass of unprepared defense contractors -- is left exposed to potentially disastrous risks, both of substantive violations *and* of failing to make the mandated disclosure of those violations. In sum, the mandatory disclosure rule *exacerbates* the competitive disadvantages borne by small- and medium-sized enterprises which have been too slow to adopt corporate compliance systems.

B. Mandatory Disclosure Reinforces Reputational Bonds Between Contractors and the Defense Department

As the discussion above reflects, mandatory disclosure amplifies the competitive weaknesses borne by the many contractors -- potentially thousands of firms -- in the middle and lower tiers of the defense marketplace which do not have effective compliance systems. The mandatory disclosure rule hurts those small- and mid-sized firms in another way: only the largest firms, with effective and highly public compliance and disclosure systems, can assure the defense department that the reputational capital which those firms share with the government will be carefully protected, through internal enforcement and disclosure.

The U.S. defense industry has become much more concentrated over recent decades,[29] and now a handful of prime contractors dominate that market.[30] While previous studies have

[24] *See* U.S. Office of Governmentwide Ethics, *18 U.S.C. § 208: Acts Affecting a Personal Financial Interest*, http://www.oge.gov/Laws-and-Regulations/Statutes/18-U-S-C--%C2%A7-208--Acts-affecting-a-personal-financial-interest/ ("The criminal prohibition has no de minimis level. That is, it applies where any financial interest exists, no matter how small.").

[25] 5 C.F.R. Part 2640.

[26] *See, e.g., Strategic Diversity, Inc. v. Alchemix Corp.*, 666 F.3d 1197, 1210 n.3 (9th Cir. 2012).

[27] *See, e.g.*, Claire M. Sylvia, The False Claims Act: Fraud Against the Government § 4:38 (2014) (discussing authorities applying recklessness standard under False Claims Act).

[28] *See, e.g., Former Boeing Exec Pleads to Conspiracy Charge*, 18 Andrews Gov't Cont. Litig. Rep. 7 (2004).

[29] *See, e.g.*, F.G. Hayden, Elliot G. Campbell, and Shannon Cummins, *The Ranking of Contractors to the U.S. Department of Defense According to Integrated Power Blocs Among the Contractors*, 44 *J. Econ. Issues* 411, 412-414 (2010) (recent history of consolidation in defense history).

[30] *See, e.g.*, Erik Kopač, *Defense Industry Restructuring: Trends in European and U.S. Defense Companies*, __ Transition Studs. Rev. __ (2006).

suggested that sophisticated contractors may structure themselves to reduce reputational risk to the government and the contractors,[31] there has been little, if any, specific assessment of the mandatory disclosure rule's role in this complex relationship between the Defense Department and its largest contractors.

The starting point for this discussion is a recognition that a government inevitably shares reputational capital with its contractors, especially those prime contractors under its direct control.[32] The debate over private military contractors, for example, has highlighted that shared reputational capital, for those arguing for tighter regulation of PMCs have pointed out that the contractors' actions can impair a government's reputation and legitimacy.[33]

Viewed in this light, the mandatory disclosure rule may be seen as a capstone on a broader government effort to force contractors, through ethics and compliance programs, to control the risks of fraud and corruption -- especially reputational risks -- on behalf of the government. The mandatory disclosure rule notably does *not* focus on performance risks; there is no requirement, for example, to report new obstacles which may slow a project.[34] Instead, as written and implemented, the mandatory disclosure rule serves more as an early warning device for fraud and corruption, to alert the government to potential egregious violations by

[31] One study, by Chong Wang of the Naval Postgraduate School, suggested that the largest, most politically connected contractors may hire politically astute senior retirees from the military establishment so as to curb the contractor's own opportunistic (corrupt or rent-seeking) behavior that would undermine the government's reputation *See, e.g.*, Chong Wang, *Political Connections of the Boards of Directors and Department of Defense Contractors' Excessive Profits*, 14 J. Pub. Proc. 96, 113 (2014) ("DoD contractors may hire . . . politically connected directors and use their experience to serve a benevolent role to the public. For instance, one legitimate use of the political experience is to keep DoD contractors from opportunistic profit-seeking behaviors that could reach or even cross federal government regulatory redlines.")

[32] *See, e.g.*, Douglas P. Beighle, *Defense Contractors - The Next Spotted Owl?*, 24 Nat. Cont. Man. J. 1 (1991) (discussing Congress' and contractors' shared reputational loss due to negative studies and procurement scandals of the previous decade).

[33] *See, e.g.*, Zoe Salzman, *Private Military Contractors and the Taint of a Mercenary Reputation*,40 N.Y.U. J. Int'l L. & Pol. 853 (2007-2008). A study of the use of military law to address contractor criminal misconduct in combat areas pointed out that "[c]ontractor criminal activity can generate significant media interest, adversely impact strategic relationships with host nation governments, and require commanders to swiftly formulate a response when such incidents occur within their areas of operation." Lieutenant Colonel Charles T. Kirchmaier, *Command Authority over Contractors Serving With or Accompanying the Force*, 439 *Army Law.*, Dec. 1, 2009, 35, 37; Nigel D. White & Sorcha MacLeod, *EU Operations and Private Military Contractors: Issues of Corporate and Institutional Responsibility*, 19 Eur. J. Int'l L. 965 (2008).

[34] Disclosure of those performance-based risks are typically dealt with separately, under contractual clauses which require, for example, that contractors report any extraordinary costs which may be chargeable to the government within 30 days.

contractors.[35] While contractors are expected to identify and initially investigate the violations, ultimate enforcement against those violations still rests with the government. From officials' perspective, the government leverages the contractors' compliance and ethics system to gain better visibility into violations, thus multiplying the government's enforcement capacity and -- importantly -- sharply reducing reputational risks from otherwise unpredictable and uncontrolled third-party reports of fraud and corruption, for example from the press and whistleblowers.

In practice, however, this mandatory disclosure model appears to be one which favors large, established contractors, and which in effect bolsters barriers to entry in the defense market. The mandatory disclosure requirements are themselves idiosyncratic -- some crimes are subject to mandatory disclosure, but many are not -- and so demand time and sophistication to integrate into a broader compliance and ethics program. That foundation underlying mandatory disclosure, an effective compliance and ethics program, is also extremely expensive, and while some of those compliance costs may be allowable under cost-reimbursement contracts, a compliance program inevitably causes additional costs (including opportunity costs) which will *not* be absorbed by the government customer.

Nor do the costs end once mandatory disclosure has been integrated into an ethics and compliance program. The compliance system must remain active, gathering, processing and assessing reports of possible violations. When violations may call for mandatory disclosure, those possible violations must be specially assessed, often with input from sophisticated outside counsel. The contractor may undertake an internal investigation, under the protection of an attorney-client privilege, and the contractor ultimately need only disclose those circumstances which present "credible evidence" of an enumerated bad act (bribery, fraud, etc.). Mandatory disclosure is, in other words, a long, costly process, one built on an already expensive system of ethics and compliance -- not a process that favors those new to the market, or short of resources. Mandatory disclosure is, in sum, a rule which can be readily implemented by large, established contractors, but which poses daunting obstacles to those contemplating entering the defense market, and which poses serious risks to competitors that cannot (or care not to) implement it properly.

IV. Easing the Anti-Competitive Effects of Mandatory Disclosure

As the discussion above reflects, the mandatory disclosure rule creates substantial benefits for enforcement officials (by unearthing violations for enforcement) and, more broadly, for the government as a whole by reducing the costs and reputational risks of fraud and

[35] Guidance by the then-Inspector General for the General Services Administration, for example, explained that contractors should give early notification, even before an investigation is concluded, and that the agency would normally await conclusion of the contractor's investigation before taking any action. Brian D. Miller, *supra* note 8, at 10 ("We prefer early notification, and so long as the contractor keeps us informed of its progress, we do not intervene until the contractor has completed its internal review.").

corruption. At the same time, though, the mandatory disclosure rule creates significant costs for contractors, and tends to favor the largest, most deeply established contractors in the market. In a defense market that is already markedly concentrated, those anti-competitive forces are a cause for concern. This section assesses possible ways to ease the rule's inherently anti-competitive effects.[36]

A. Governments Should Facilitate Compliance and Ethics Systems

One obvious measure to enhance competition would be to reduce contractors' costs of administering the corporate compliance and ethics system upon which the mandatory disclosure requirement rests. This can be done, for example, by making model codes of ethics and training freely publicly available, and by using common standards for compliance systems.[37] The important point is one of perspective: in mandating compliance systems among their contractors, governments should recognize that the goal is a one of reducing *agency costs* -- to ensure that the government's rules and principles are conveyed, and complied with, efficiently down through the supply chain. Doing so will reduce hiccups in the supply chain, and will expand the available competition. Viewed in this way, the government has every incentive to cooperate fully with its vendors, large and small, in establishing robust and effective compliance systems.

B. Harmonize Standards for Mandatory Disclosure

Governments' success in harmonizing the standards for compliance systems (discussed above) should be matched in mandatory disclosure requirements: to the extent a government decides to mandate disclosures, those requirements should be harmonized across regulatory regimes. Thus, for example, it makes little sense for the federal government to require:

- *Federal contractors* to make mandatory disclosures once they have *credible evidence* of *enumerated crimes* (bribery or gratuity under Title 18, U.S. Code),

[36] For a general discussion of the legal and policy imperatives for assessing procurement rules' potentially anti-competitive effects, see Christopher R. Yukins & Lt. Col. Jose Cora, *Feature Comment: Considering the Effects of Public Procurement Regulations on Competitive Markets*, 55 Gov. Contractor ¶ 64 (Mar. 6, 2013), *available at* http://ssrn.com/abstract=2230613.

[37] Rather than simply adopt the organizational compliance standards promulgated by the U.S. Sentencing Commission -- a sister federal agency, which maintains what are commonly referred to as the "gold standard" for corporate compliance standards, *see, e.g.*, Paul E. McGreal, *The Amended Organizational Sentencing Guidelines: Top Ten Things Attorneys Should Kno*w, The Houston Lawyer, March/April 2005, *available at http://www.thehoustonlawyer.com/aa_mar05/page10.htm* -- the drafters of the federal procurement rules insisted on creating their own, parallel standards. 73 Fed. Reg. at 67068. Because the FAR compliance standards are largely, but not perfectly, identical to the U.S. Sentencing Commission guidelines (see chart above), the FAR regulators' insistence on drafting their own standards increased contractors' implementation costs, and may mean that the federal procurement standards will lag a step behind, as the U.S. Sentencing Commission's guidelines evolve over time.

civil or criminal fraud under the False Claims Act, or "significant overpayments," while requiring,

- *Federal grantees* to make mandatory disclosures "in a timely manner, in writing to the Federal awarding agency or pass-through entity *all violations of Federal criminal law involving fraud, bribery, or gratuity violations* potentially affecting the Federal award."[38]

Thus, while *contractors* must disclose both *criminal* (intentional) and *civil* (reckless) fraud, the covered grantees need only disclose *criminal* fraud; by the same token, it is not clear what other criminal statutes are covered in the grantees' requirements (is the Anti-Kickback Act, for example, a "Federal criminal law involving . . . bribery"?). There is no ready reason for these standards to differ, especially since federal contractors regularly serve as grantees, as well,[39] and the federal grant rule was explicitly modeled on the contract mandatory disclosure rule.[40] Where, as here, mandatory disclosure requirements vary -- apparently unnecessarily -- private vendors must spend more to implement these varying standards, and other potential competitors are further discouraged from competing for federal contracts or grants.

C. Limit Scope: Target Violations for Which Contractors Have a Clear Informational Advantage, or Which Pose Most Severe Reputational Risks

Because of the costs and potentially anti-competitive effects of mandatory disclosure,[41] it is important that the scope of mandatory disclosure be carefully limited. In principle, because (as noted) regulators' goals here should be to level the informational imbalance between government and its contractors, and to force early (and controlled) disclosures of violations which pose potentially severe reputational risk, logically regulators should craft the mandatory disclosure rule to force disclosure of bad acts:

[38] Section 200.113 of the Office of Management & Budget's "Super Circular" governing federal grants (now known as the "Omni Circular"), 78 Fed. Reg. 78590 (Dec. 26, 2013), which is being implemented by federal grantmaking agencies, provides as follows:

> *§ 200.113 Mandatory disclosures*. The non-Federal entity or applicant for a Federal award must disclose, in a timely manner, in writing to the Federal awarding agency or pass-through entity all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures can result in any of the remedies described in § 200.338 Remedies for noncompliance, including suspension or debarment. (See also 2 CFR Part 180 and 31 U.S.C. 3321)

[39] Data on federal funds received by grantees and contractors are available in a combined database, through www.usaspending.gov.

[40] *See* 78 Fed. Reg. at 78595.

[41] Mandatory disclosure also may implicate broader issues of self-incrimination; these are potentially human rights issues, beyond the scope of this paper, which focuses instead on the economic costs and benefits of a mandatory disclosure regime. *See, e.g.*, Jeremy A. Goldman, Note, *New Far Rule on Compliance Programs and Ethics: A Hidden Assault on the Corporate Attorney-Client Privilege*, 39 Pub. Cont. L.J. 71 (2009).

- For which contractors enjoy a clear informational advantage, and
- Which pose the sharpest reputational risks to the government.

Although the federal mandatory disclosure rule apparently was not crafted with these goals in mind -- instead, it appeared to reflect various enforcement agencies' efforts to include specific bad acts onto the mandatory disclosure list[42] -- the final rule does, in rough terms, reflect these dual goals. The bad acts which must be disclosed are generally those which contractors have an easier time discerning than the government (e.g., bribes, gratuities and fraud), and, again because of complicated reasons of agency,[43] these are precisely the bad acts which are most likely to have deeply corrosive reputational impacts on the government. In other words, although the federal rule is not perfect,[44] it does appear to accommodate these dual policy goals.

D. Allow Contractor Opportunity to Investigate, Under Privilege

Another, relatively simple means of reducing the anti-competitive impact of a mandatory disclosure rule is to allow the contractor time, before making any disclosure, to assess the evidence under the protection of a privileged investigation. The drafters of the federal rule prudently, and explicitly, decided to leave contractors this breathing space before making a mandatory disclosure.[45] Although critics may argue that the rule thus allows contractors time to "bury" troubling evidence, the alternative -- to require contractors to disclose any apparent violation, without due investigation -- would be highly inefficient. A rule demanding immediate disclosure could mean that the government would be flooded with reports which might prove, in the end, to be groundless. Furthermore, a rule which forced *immediate* disclosure of any bad act

[42] For a detailed discussion of this aspect of the administrative history of the mandatory disclosure rule, see, e.g., Brian D. Miller, *supra* note 8, at 3-5.

[43] *See, e.g.*, Susan Rose-Ackerman, *The Law and Economics of Bribery and Extortion*, 6 Ann. Rev. L. & Soc. Sci. 217, 218 (2010) ("Principal-agent relationships are at the heart of any corrupt transaction. An employee or another person acting as an agent for a government body or a private organization accepts a private benefit in return for acting in the payee's interest."); Nico Groenendijk, *A Principal-Agent Model of Corruption*, 27.3-4 Crime, L. & Soc. Change 207 (1997).

[44] The federal rule's open-ended requirement that contractors disclose "significant overpayments" remains uncertain. The provision also may be exploited by contractors which seek to make *some* disclosure, to comply with the rule, but not to report more serious bad acts (such as fraud) ; these contractors instead may simply disclose a "significant overpayment," pending a more detailed internal review. *See* Brian D. Miller, *supra* note 8, at 10.

[45] *See, e.g.*, 73 Fed. Reg. at 67074 ("[T]he [FAR] Councils believe that using the standard of 'credible evidence' . . . will help clarify 'timely' because it implies that the contractor will have the opportunity to take some time for preliminary examination of the evidence to determine its credibility before deciding to disclose to the Government. Until the contractor has determined the evidence to be credible, there can be no 'knowing failure to timely disclose.' This does not impose upon the contractor an obligation to carry out a complex investigation, but only to take reasonable steps that the contractor considers sufficient to determine that the evidence is credible.").

brought to light in a compliance system would, in effect, encourage contractors *not* to have effective corporate compliance systems, but instead to allow news of bad acts to drift into dark silence at the bottom of the firm.

E. Reinvigorate Voluntary Disclosure

The final proposed change to the mandatory disclosure regime may be the most radical, but the most useful: to recognize that mandatory disclosure will probably always be limited (for the reasons outlined above), so that the optimal policy choice instead may be to reinvigorate *voluntary* disclosure, by giving contractors positive incentives, perhaps through reduced enforcement penalties, to come forward with bad acts.[46]

A voluntary disclosure regime, unlike a mandatory one, could cover a much broader array of bad acts and crimes, for it would pose none of the risks (discussed above) that an overbroad mandatory regime carries, of inefficiently forcing disclosures of *too many* bad acts. A system of voluntary disclosure would reduce the costs of implementation, because a voluntary regime means that only those contractors that discover bad acts internally, and seek to make a voluntary disclosure to reduce their exposure, must study and abide by the voluntary disclosure rules. Finally, a voluntary disclosure regime would have a much less damaging effect on competition, for contractors that could not manage disclosure -- the contractors at serious peril in a mandatory regime -- would face no new risks of destruction in a voluntary regime; failing to make a disclosure would simply lose them the leniency they might otherwise enjoy, under a voluntary regime.

As noted, several decades ago the federal government instituted a system of voluntary disclosure to handle fraud in defense procurement, a system which failed largely because of its own cumbersomeness, and because it did not present defense contractors with sufficient incentives for disclosure. A renewed emphasis on voluntary disclosure, perhaps with clearer and stronger incentives for disclosure, and potentially modeled on the World Bank's reportedly

[46] As Susan Rose-Ackerman noted, in discussing the importance of whistleblowing in addressing corruption:

> Successful detection of corruption depends upon insiders to report wrongdoing. Citizens and businesses victimized by extortion demands may report bribery attempts, but they may not be able to offer enough proof for prosecutors to act. Instead, effective law enforcement often requires officials to promise leniency to one of the participants. This creates an important paradox for law enforcement efforts. High expected punishments ought to deter corruption, but a high probability of detection may only be possible if some are promised low penalties.

Susan Rose-Ackerman, *supra* note 43, at 222.

successful system of voluntary disclosures for contractors,[47] might prove a useful way forward. In assessing a new voluntary disclosure system, though, policymakers might wish to weigh the increasingly important role that whistleblowers (often current or former employees) play in revealing fraud and corruption; a system of voluntary contractor disclosure should complement, not disrupt, existing systems to encourage and protect private whistleblowers.

V. Conclusion

The federal government's mandatory disclosure rule provides an interesting case study in how an anti-corruption tool, of good intent, can be quite costly and have anti-competitive effects in an already highly concentrated defense procurement market. To address those problems, a mandatory disclosure rule should be crafted to minimize transaction and opportunity costs, and to focus on the problems at the core of a disclosure rule: the need to remedy the government's informational deficits regarding its contractors' bad acts, to redress fraud and corruption and the reputational damage they can cause the government. Recognizing these broader benefits of disclosure, and the inherent limitations of mandatory disclosure, policymakers may wish to revisit the benefits of incentivizing *voluntary* disclosures by contractors, as a complement to the information on bad acts gained through mandatory disclosures and whistleblowers.

[47] The World Bank publishes extensive materials on its Voluntary Disclosure Program, which incentivizes contractors on World Bank-funded projects to come forward with information on bad acts, to reduce or avoid the risk of sanctions (including potentially debarment) under the World Bank's sanctions system. *See, e.g.*, World Bank, *VDP Guidelines for Participants (2011), http://siteresources.worldbank.org/INTVOLDISPRO/Resources/VDP_Guidelines_2011.pdf;* World Bank, "About the VDP," http://go.worldbank.org/3JOFMN95S0.

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

Defence Integrity Pacts
Identifying the corruption risks in defence and security
Enlisting the defence contractors
Integrity self-assessment by nations
Developing counter-corruption pl

BUILDING INTEGRITY AND COUNTERING CORRUPTION IN DEFENCE & SECURITY

20 PRACTICAL REFORMS

Using metrics and surveys
Involving civil society
Leading Change
Reducing corruption risks in contracts in operations
Educating change leaders
Independent Monitoring
Codes of Conducts, values and behaviours
Military-owned businesses
Build leadership understanding
Diagnosis of Corruption Risks
Strategic and planning considerations for conflict environments
Asset disposal

www.transparency.org

1. IDENTIFYING THE CORRUPTION RISKS IN DEFENCE AND SECURITY

Corruption is a broad term. This Handbook breaks it down into 29 specific defence corruption issues that provide a basis for a country-specific analysis.

There is no generic diagnosis, and therefore no generic plan that will work in every situation. However there are key risk areas and recurring problems across the world. To help diagnose the risks, TI has devised a framework for understanding defence and security corruption that can guide you around the range of possible corruption issues and provide a starting point for your own analysis.

This framework has been used during dialogue with the senior leadership in many nations: with defence ministers, the most senior officials and high-ranking military officers, as well as at public meetings and with civil society.

While neither definitive nor exhaustive, the framework is robust enough to serve as the starting point for most nations. It breaks the generality of defence and security corruption down into five broad headings encompassing different types of corruption. Those areas of defence where corruption is most significant and causes the greatest problems have a subsequent chapter of this handbook devoted to them.

This framework is a good tool to open the debate within a ministry or department or across the armed services. It can identify which issues are relevant and which need to take priority. It can be used to talk to colleagues and identify which issues are significant.

FIGURE 1: FRAMEWORK FOR DEFENCE AND SECURITY CORRUPTION

POLITICAL	PERSONNEL	PROCUREMENT
DEFENCE & SECURITY POLICY	LEADERSHIP BEHAVIOUR	TECHNICAL REQUIREMENTS / SPECIFICATIONS
DEFENCE BUDGETS	PAYROLL, PROMOTIONS, APPOINTMENTS, REWARDS	SINGLE SOURCING
NEXUS OF DEFENCE & NATIONAL ASSETS	CONSCRIPTION	AGENTS/BROKERS
ORGANISED CRIME	SALARY CHAIN	COLLUSIVE BIDDERS
CONTROL OF INTELLIGENCE SERVICES	VALUES AND STANDARDS	FINANCING PACKAGE
EXPORT CONTROLS	SMALL BRIBES	OFFSETS
		CONTRACT AWARD, DELIVERY
FINANCE	**OPERATIONS**	SUBCONTRACTORS
ASSET DISPOSALS	DISREGARD OF CORRUPTION IN COUNTRY	SELLER INFLUENCE
SECRET BUDGETS	CORRUPTION WITHIN MISSION	
MILITARY-OWNED BUSINESSES	CONTRACTING	
ILLEGAL PRIVATE ENTERPRISES	PRIVATE SECURITY COMPANIES	

POLITICAL

If a corrupt individual or group is able to influence defence and security policy (for example, to create a requirement for procurement of fast jets when no such need truly exists), this is high-level corruption. The subsequent procurement process can be largely clean, yet fundamentally flawed.

A **defence** process can be manipulated or overcomplicated in order to hide corrupt decisions and illicit enrichment, for example, if a policy approval procedure is lacking or policy decisions are not published. In the most extreme cases, defence corruption at the highest level might represent 'state capture', if an elite is able to shape state decisions across a much wider area.

Where countries are rich in natural assets, such as oil, timber, minerals or fish, the military or security forces can become closely or improperly connected with their exploitation. This **nexus of defence/security and natural assets** is common in conflict environments (for example, in Sierra Leone with diamonds, Angola with oil), but it also occurs in peacetime circumstances, as in Nigeria or Indonesia. Such linkages can be prime drivers of subsequent conflict.

Organised crime is present in every country and is a growing transnational security threat. Increasingly technology-enabled, it does not respect national or international boundaries and prospers in ungoverned spaces such as fragile states. Motivated by the acquisition of wealth, it is arguably beyond the power of any one agency or nation to contain effectively, and may have penetrated the defence, security and intelligence establishment. In these circumstances counter-corruption strategies will have little chance unless organised crime is prioritised and addressed at the same time.

Corruption within the **intelligence services** has been a significant problem in some countries, notably in post-communist and post-conflict societies. Intelligence services gather information that has potential economic and political leverage. This makes them an attractive target for corrupt behaviour.[1]

Arms export controls are susceptible to the risk of corruption as a vehicle for illegal arms transfers with negative consequences for international humanitarian law, human rights, and sustainable development. Corruption also hinders efforts to combat violent organised crime and terrorism as it undermines the ability of states to control the diversion of weapons from their intended end-users.

FINANCE

Misuse of defence and security budgets is one of the most common problem areas. In the defence sector a culture of secrecy can create an environment in which good financial practices such as auditing by an external division are not employed on the grounds of national security. Yet much public trust is gained by being more transparent. In any organisation or department, sound management of assets, with timely and efficient accounting systems, is one of the most powerful devices for maintaining integrity. The better the systems in place, the less opportunity there will be for corruption. As well as providing opportunity for fraud, a poor and disconnected accounting system makes it easy to conceal irregularities. Even if irregularities are found, poor accounting makes it impossible to identify those responsible, and hold them to account.

Asset disposals are a common category for corrupt management. This can occur through the misappropriation or sale of property portfolios and surplus equipment, particularly where the military is downsizing. Even large assets can be poorly controlled and easy to sell off corruptly or undervalued.

Secret defence and security budgets are a perennially difficult issue. There are valid reasons for secrecy, but these are open to abuse. Several countries have developed innovative ways of addressing the risks. A broader risk is when there are budgets outside defence that are also used by the military or security forces, but not identified as.

In many countries, defence and security establishments maintain income sources separate to their state revenue streams. These include **military-owned businesses**, either civilian businesses or defence companies which are directly or indirectly owned by the defence establishment. These pose obvious integrity risks.

Misuse of assets also extends to **illegal private enterprises**, with individuals gaining an income from state-owned assets. This may be through the payment of exorbitant fees to cronies for consultancy or other services, or the use of service personnel for private work. It can also include bankrolling of the military by private enterprises in return for military protection of their business interests. The development of a system of patronage between the military and private business is highly detrimental; the more profitable it becomes, the more difficult it is to counter.

PERSONNEL

Personnel and recruitment processes are particularly susceptible to corruption, especially if it is endemic throughout a defence establishment.

Corruption to avoid **conscription**, for example, had already been recognised as a problem in Napoleonic times.[2] Box 1 (below) shows how, in the case of conscription in Russia, personnel management in the modern era can be affected by corruption.

This is just one example of how corrupt practices in the personnel sphere can occur. Other examples are given in Figure 3. They range from having non-existent 'ghost soldiers' on the payroll to extorting favours from subordinates.

The most common effect of corruption in personnel is that it undermines the confidence of staff, making them increasingly prone to participating in or condoning corrupt practices.

For top officials and officers themselves, **leadership behaviour** requires committed and visible engagement by strong role models. They, in turn, need feedback through honest and objective assessment, for example, through third parties and opinion surveys.

Many citizens' experience of corruption is likely to be in the payment of **small bribes** in daily life. These might include payments for speeding up administrative procedures, bribes at checkpoints or payments to avoid predatory police. While this Handbook concentrates on large-scale bribery and corruption, policy-makers should note that anti-corruption plans must

BOX 1: CONSCRIPTION IN RUSSIA

Compulsory military service, also known as conscription or draft, can be a cause of pervasive corruption within the armed forces. Such is the case in Russia. In order to avoid conscription, would-be soldiers pay bribes to the military authorities, medical personnel in charge of assessment and officials in draft boards. Such practices are widespread and publicly acknowledged. In July 2010, Russia's nationalist Liberal Democratic Party, led by Vladimir Zhirinovsky, tabled draft legislation which would allow potential conscripts to pay a sum equivalent to US $32,500 to avoid military service. The resulting funds would be channelled toward the costs of the Ministry of Defence (MoD). This measure, aimed at Russia's military commissions, signifies both the great extent of draft corruption in the country and a clear recognition of this reality.

Serious attempts to deal with this issue have been made in recent years by the Russian government. The length of conscript service was shortened by six months in April 2008 to one year, while the list of exemptions from conscriptions has also been made more restrictive.[3] However, the 2004-7 federal government programme designed to trial a transition to fully professional armed forces was largely ineffective, due to poor design and pervasive corruption which prevents full remuneration from reaching the contracted soldiers.[4]

equally address small bribes and petty corruption. A plan that focuses only on high-value corruption is unlikely to succeed; the general public needs to see benefit at a local level.

Leadership of a reform process requires several other competences: presenting persuasive arguments for why change is necessary (Chapter 4), developing a common direction and energy for change across the top leadership (Chapter 5), building a reform plan (Chapter 6), training more leaders of change across the organisation (Chapter 7) and involving third parties (Chapters 9 and 10).

Significant progress can be made by working on an organisation's values (Chapter 8).

The central issues of integrity in personnel are **payroll, promotions, appointments and rewards**. Examples are shown below:

The **salary chain** is the long link from the national treasury right down to payment to an individual soldier. In many corrupt environments those funds are stolen or diverted en route, so that far less of the due amount finally reaches the soldier. This problem is often extreme in conflict environments, but is also common in peacetime.

More broadly, tackling corruption issues requires attention to the **values** and ethical behaviour of troops, officers and officials. Building **a strong ethical culture** of adherence to policies, rules and guidelines minimises corruption risk. This is particularly relevant in defence and security establishments, which traditionally have a strong custom of compliance to written regulations.

FIGURE 3: **CORRUPTIONS RISKS IN PERSONNEL**

PAYROLL	Extracting percentages from total cash for payroll
	Ghost soldiers on payroll
	Cronies on secret payroll
	Skimming from soldiers' salaries
APPOINTMENTS/RECRUITMENT	Nepotism, favouritism and clientelism: preferred postings and pre-term rank promotion
	Sabotaging personnel/other reforms to preserve power and authority in a given sphere
	Conscription: fees to avoid military service Fees to gain participation in peacekeeping forces
	Favours and fraud during the entry process for respected military educational institutions
	Favours or payment in the selection process for peace support operations or international missions
REWARD AND DISCIPLINE	Extorting favours from subordinates
	Payments to avoid disciplinary process or for reinstatement of position
	Use of disciplinary process to remove threats to power
	Use of reward process to endorse supporters

OPERATIONS

The military's image during operations at home and abroad is vital in promoting and retaining public confidence and respect. Operations are the context in which the general population has most face-to-face daily contact with the military and officials. Therefore their conduct is of paramount importance. This applies both to military personnel and to personnel of **private security companies**.

Where international forces intervene in a conflict country, their approach to corruption once in theatre is critical to the success of their mission. **Disregard of corruption in-country** runs a high risk of being seen as complicity in it. In the past, it was sufficient for military doctrine to regard corruption as a purely civilian/governance issue. But recent experience from Afghanistan to Bosnia to Colombia has shown the need for nations to recognise corruption as a major contextual factor in operations.

Sadly, there are too many cases where intervention or peacekeeping forces have themselves been a source of corrupt behaviour, and **corruption within a mission** has occurred. In many countries the military is used to provide internal security, often in circumstances where the police are unable to operate. Border forces and domestic intelligence and security agencies are also often structured as part of the defence ministry and classed as military forces. This increases the importance of considering counter-corruption in operations as a key element of building integrity in defence.

In a conflict environment, the flow of money into a country represented by local **contracting** and logistics – whether aid money or military support – is an important part of helping to develop that country. With all the problems in a conflict situation, it is easy for corrupt contracts to be awarded, and for non-performance to be tolerated.

PROCUREMENT

Of all defence processes, procurement is usually the highest area of corruption risk, with vulnerabilities at every stage.

These are listed opposite according to the procurement phase: both those from the framework above and a number of others are shown. This Handbook does not attempt a comprehensive review of ways to tackle procurement risks. Instead it devotes four chapters (14-17) to new ideas and reforms for addressing the most serious risks in that area.

FIGURE 2: **CORRUPTION RISKS IN THE PROCUREMENT CYCLE**

1. GOVERNMENT POLICY	Privileged defence relations; defence budgets; external financing; manufacturing government pressure on importers
2. CAPABILITY GAP DEFINITION	Military, political & commercial influence
3. REQUIREMENT/CONTRACT DEFINITION	Inadequate/corrupt military/official expertise, anonymous agents; 'justified opacity', excessive use of national secrecy
4. SUPPORT REQUIREMENTS DEFINITION	Costly & complex
5. OUTLINE PROJECT COSTING	Unreliable data
6. TENDER	Single sourcing; bidder collusion; lack of transparency; offset requirements; inadequate timescales
7. BID ASSESSMENT & CONTRACT AWARD	Evaluation manipulation; favoured bidders; offsets bias outcome; lack of transparency; failure to consider value for money
8. MANUFACTURE & DELIVERY	Variation order; lack of official control; incorrect equipment performance and lack of remedial contract measures
9. IN-SERVICE PHASE	Call-off contracts; lack of expertise; lack of long-term oversight (especially for service contracts)

9. ENLISTING DEFENCE CONTRACTORS

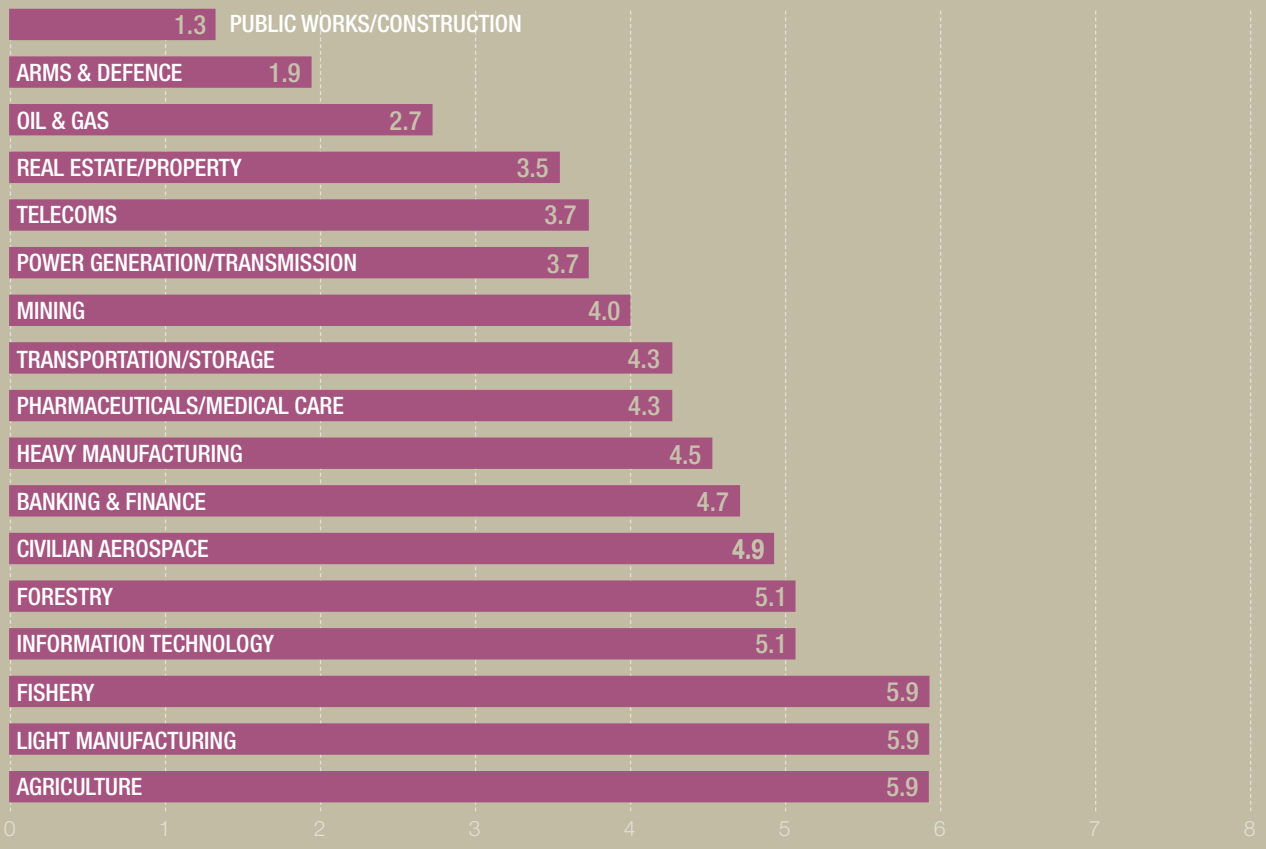
The defence industry has become more willing to engage in counter-corruption reform in the last five years – governments can use this willingness to accelerate their own reforms

This chapter illustrates how governments and companies can feed into each others' efforts to improve defence sector integrity. Governments can do so through supporting a sound business environment and by demanding high standards of integrity from companies they do business with, for example, through prosecution and debarment of corrupt behaviour. Companies can raise standards through better compliance programmes and through collective action, demonstrating that they want to operate in a bribery-free environment.

Several indices suggest the international defence sector is one of the most prone to corruption worldwide. One such index is TI's *Bribe Payer's Index*. In 2002, it ranked Arms and Defence as the industry sector perceived to be the second most corrupt.

In 2006 Control Risks released a survey of international businesses in which a third of defence sector respondents felt they had lost out on a contract in the year before due to bribery by a competitor, and stated this as the number one reason against bidding (Figure 9). As a result, defence companies are avoiding countries which they regard as high-risk, and corruption is given as the foremost reason for such action. This demonstrates that it is in the defence industry's interest to tackle the issue, and offers an opportunity for a defence ministry to collaborate with companies.

FIGURE 8: **TRANSPARENCY INTERNATIONAL'S BRIBE PAYER'S INDEX, 2002**



The scores are average all the responses on a 0 to 10 basis where 0 represents very high levels of corruption, and 10 represents zero perceived level of corruption.

COLLABORATION WITH DEFENCE COMPANIES

Once a defence establishment has the will and the knowledge to tackle corruption, and suitable policies have been put in place, its personnel need to build partnerships in order to control corruption across the entire sector. These relationships are crucial in opening up areas in which corruption traditionally operates discretely.

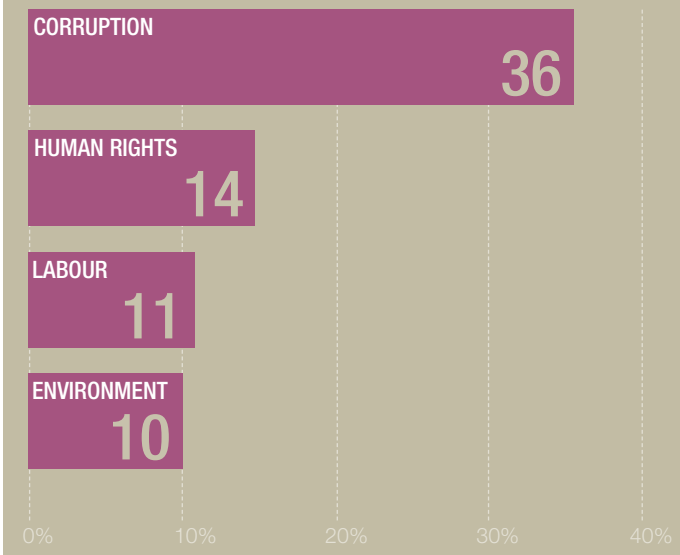
Anti-corruption programmes cannot be effective if designed and implemented in isolation from the contractor community. Active collaboration between governmental defence institutions and the defence industry can help isolate defence sector corruption. Each side can offer mutual cooperation and encouragement in integrity-building measures, and can refuse to do business with an entity perceived as corrupt, whether it is a company or a procuring government agency. One of the biggest concerns for defence establishments is how to attract high-quality suppliers. Clean companies will avoid environments where corruption is endemic, and will have stringent controls to minimise opportunities for corruption originating from their organisations or their agents. This can be a major driver for a ministry's reform.

COLLABORATION AMONG DEFENCE CONTRACTORS

There is much scope for private sector engagement at any stage of the programme to build integrity and reduce corruption risks. Companies can signal clearly to governments that they will not engage in bribery or corrupt practices, and so exert a positive influence over officials and organisations. In sectors such as mineral extraction, water, banking and construction, the private sector's role in raising standards has been crucial. For companies to raise standards within defence establishments, they must also raise standards among themselves. One way the industry can raise standards is by forming an anti-corruption forum and by setting a code of standards.

For example, Europe's defence industry has come together on corruption, coordinated by the AeroSpace and Defence Associations of Europe. Following meetings of major defence firms facilitated by TI, the Associations formed a group to develop a set of Common Industry Standards (CIS) for its member associations and their member firms to follow.

FIGURE 9: **REASONS FOR COMPANIES NOT TO BID IN A TENDER, 2006**
(CONTROL RISKS)



The Common Industry Standards released in 2008 cover:

1. Compliance with laws and regulations
2. Applicability to principal entities, agents and consultants
3. Prohibition of corrupt practices
4. Gifts and hospitality
5. Political donations and contributions
6. Agents, consultants and intermediaries – due diligence, legal provisions, fees, auditing/verification, etc.
7. Integrity programmes
8. Sanctions

Since the CIS were developed in 2007, the French and UK national associations have been engaged in efforts to develop national anti-corruption forums to implement them. There is also a much larger US forum, the 'Defense Industry Initiative' – see box 12 overleaf. Additionally, the UK's Society of British Aerospace Companies and Defence Manufacturer's Association have produced a short handbook containing guidance for implementing the CIS.[22]

Other industry sectors have taken similar actions (Box 11).

Another type of defence industry cooperation is the sharing of good practices. For example, in the United States, following high-profile problems in ethical conduct in several large defence contractors, the Defense Industry Initiative on Business Ethics and Conduct (DII) was established in 1986 to create a common ethos of ethics and integrity across the defence sector in the USA (see box 12). The DII organises an annual best practices forum and provides substantial training and guidance in ethics and business conduct to its members. For more information, see **www.dii.org**.

BOX 11: **EXAMPLES OF SUCCESSFUL COLLECTIVE ACTION ACROSS INDUSTRIES**

OIL, GAS AND MINING

The Extractive Industries Transparency Initiative (EITI) is a multi-stakeholder coalition of civil society, governments, industry, investors and international organisations, which sets a global standard for companies and governments to disclose payments and receipts in the extractive industries. Established in 2002, the EITI arose from the realisation of the 'natural resource curse', i.e. the paradox that countries rich in natural resources also tended to have high levels of poverty, corruption and conflict, fuelled by competition for riches. Many of these problems are the result of poor governance. The EITI aims to strengthen governance in participating countries by improving transparency and accountability in extractive industries. Both governments and natural resource companies are actively engaged.

For more information, see ***www.eiti.org***

SANCTIONS ON COMPANIES

Ultimately, such efforts aimed at building confidence between the public and private sectors require recourse to sanction should anti-corruption laws and regulations be breached. Defence establishments owe it to companies who comply with ethical norms to take action against those who fail to uphold the same standards. Efforts by companies to gain advantage through corrupt means should be given a high priority in terms of prosecutions through the criminal justice system. The defence establishment can reinforce can reinforce incentives to refute corruption by instituting debarment procedures for companies which are found guilty of corrupt practices, whether at trial or by plea. Box 13 describes the use of debarment within the context of wider regulation of defence companies in the USA.

GOVERNMENTS

Those at the top of defence and security establishments have an important role in bringing both national and international contractors into the reform plan. This can include some or all of the following:

- meeting with contractors as a body and encouraging them to develop an industry initiative
- meeting regularly with industry bodies to discuss progress
- emphasising to international companies that they have obligations under the CIS and that the government expects strict adherence to these standards
- speaking frequently at industry and other events on the importance of high standards of behaviour by defence contractors
- Carrying out a detailed review of where governments need to crack down on their own practices so as to better enable industry reform.

BOX 12: DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

In the United States, following high-profile problems in ethical conduct in several large defence contractors, the Defense Industry Initiative on Business Ethics and Conduct (DII) was established in 1986 to create a common ethos of ethics and integrity across the defence sector. The DII supports the US federal legal framework by establishing six principles around which to organise companies and associations. The current principles are as follows:

1. Each Signatory shall have and adhere to a written code of business conduct. The code establishes the high ethical values expected for all within the signatory's organisation.
2. Each Signatory shall train all within the organisation in their personal responsibilities under the code.
3. Signatories shall encourage internal reporting of violations of the code, with the promise of no retaliation for such reporting.
4. Signatories have the obligation to self-govern by implementing controls to monitor compliance with federal procurement laws and by adopting procedures for voluntary disclosure of violations of federal procurement laws to appropriate authorities.
5. Each Signatory shall have responsibility to one another to share its best practices in implementing the DII principles; each Signatory shall participate in an annual Best Practices Forum.
6. Each signatory shall be accountable to the public.

For more information, see ***www.dii.org***

BOX 13: US AIR FORCE DEBARMENT PROCEDURE

The US Air Force has had much experience in dealing with defence contractors and has developed a structure whereby federal law can be used to punish and deter corruption, and to encourage compliance and ethical conduct.

US agencies have suspension and debarment officials, whose role is to debar or suspend contractors who contravene accepted rules of conduct. They update a public website of all debarred companies, which contracting officials are required to check prior to awarding new contracts. A decision to debar or suspend by an agency makes the person or organisation ineligible for new contracts by all agencies throughout the US federal government.

Companies and individuals become eligible for debarment if they engage in any crime that relates to business honesty, including fraud and corruption. The possibility of debarment is a substantial disincentive to participate in such activities. Debarment can also be employed should a party perform poorly on a contract, as well as for any other serious cause, at the discretion of the debarring official.

The US Air Force debarring official also oversees the US Government's investigation and prosecution of Air Force contractors suspected of committing procurement fraud. The legal basis for many of these actions is the False Claims Act (31 U.S.C. §3729-3733). This act provides incentives for people not affiliated with the government to file actions against federal contractors, by allowing them a share of the damages recovered. The US also requires the disclosure of misconduct by industry and imposes debarment as a sanction for failure to do so.

Incentives for strong ethical conduct by American firms are provided in the country's sentencing guidelines, which allow the strength of a company's compliance programme to be taken into account during sentencing for firms convicted of misconduct. Punishment for wrong-doing is further proportional to the extent the company has acted to prevent misconduct. The US Air Force also tends to favour contracting with companies which have good ethical reputations.[23]

Ethical Issues in Defense Systems Acquisition

Major General Robert Latiff, Ph.D. (U.S. Air Force, retired)
George Mason University*

[citation: Major General Robert Latiff, U.S. Air Force (retired): "Ethical Issues in Defense Systems Acquisitions," *Routledge Handbook of Military Ethics*, ed. George Lucas (Oxford: Routledge, 2015): 209-219

Generally speaking, when one talks about weapon systems and ethics, the conversation is about the weapons' use in combat and whether such use is morally justified and adheres to the laws of war. To be sure, history is replete with issues of inhumane weapons, some of which ultimately came to be banned or considered unacceptable for use by civilized nations. Chemical and biological weapons, nuclear weapons, and land mines are but a few examples. Debates about potential employment of certain weapons should obviously occur well before such weapons are even built.

What I wish to discuss in this chapter, however, are some of the less frequently discussed, but very important ethical issues encountered in the actual process of acquiring weapons, *after* the decision process about the moral propriety of their potential operational use has already been evaluated. The manufacture and sale of arms is an important component of national identities as well as national economies, and it is also the source of a great deal of morally-questionable behavior. Scandals, and the questionable ethics that underlie them, have erupted regularly in the weapons procurement business. I begin by reviewing some of these regrettable events, and then proceed to analyze the weapons procurement process to identify where things can go wrong.

I. The Economic Importance of the Arms Industry: The Lure of Money

It is an observation from history that war and violent conflict are seemingly constant elements of the human condition. And, while the technology and the weapons themselves change with time, the importance of armaments and arms industries remains. One has only to consider the importance of ships and shipbuilding in ancient conflicts like the Peloponnesian War, or the introduction of gunpowder weapons in fifteenth century Europe, or the rise of arms makers during the U.S. Civil War, or the dominance of arms makers like Krupp in Germany in WWI, or the emergence of powerful U.S. aircraft companies in World War II, or the rise of the nuclear weapons complex during the Cold War, or the continued growth and dominance of defense industries worldwide since the events of September 11, 2001. Aaron Plamondonin, notes "the improvements in the industrialization of weapons and equipment production have altered the way wars have been fought throughout history. Those nations that adopted better processes and were able to better equip their militaries often had the advantage on the battlefield. All nations were confronted with a new type of war, and *power began to be measured in how efficient a nation's defense industrial capability had become*."[1]

It goes without saying that combat operations are a tremendous drain on the human treasure of a nation. Weapon system acquisition, while it doesn't involve sending soldiers into combat, nonetheless represents a significant drain on the financial treasure as well. Defense spending accounts for large portions of many

national economies, whether it is expenditures for imports or income from exports. While not necessarily on a *per capita* basis, the U.S. remains, on an absolute basis, the largest single investor and customer for defense industries, and the largest exporter of armaments. With a Defense Budget of close to $650B, spending on actual equipment is annually about $100B, with another $60B on research and development. Weapons purchases constitute a large fraction of a very large DOD budget, and the decision to invest heavily in weapons should be taken only after sufficient debate. Unfortunately the debate often revolves, not around the propriety of such investments, but rather around politics and which party's politicians will benefit from the defense work proposed. A great deal of money is tied up in weapons acquisition and, where there is a lot of money, there are unfortunately many opportunities for poor ethical judgment.

The enormous amount of money involved in weapons development and production is important to the national industrial base, but is especially so to primarily defense companies whose existence depends on government contracts. Often, if a company is not adequately diversified and does not win major weapons contract competitions, they will exit the business. As defense budgets decline and the number of weapon projects shrinks, this problem worsens, and the impetus for ethical misbehavior grows.

II. Past Scandals

History reveals that where there has been a demand for weapons, there have been repeated cases of unethical and illegal behavior. These ethical abuses take

many forms, to include shoddy workmanship, influence peddling, bribery, contract fraud, and procurement impropriety. Scandals can be found dating back hundreds of years. During the American Civil War, for example, J.P. Morgan bought defective rifles and sold them to generals in the field for obscene profit. The rifles would shoot off the thumbs of the soldiers using them. After the Civil War, with the boom in technology and armaments, graft and corruption reached a fever pitch.[2] Marshall Baron Clinard, in his wide-ranging book on corporate corruption, states that:

> Throughout the civil war, the country was also plagued by the corruption of the arms suppliers; bullets were even filled with sawdust instead of gunpowder. These rip offs continued into the twentieth century. During WWI, profiteering, abuse of political power, arrogance, and fraud typified the defense industry. During WWII, Harry Truman suddenly found himself catapulted into the Presidency of the United States, in part because of his investigations into arms-maker fraud and excessive profiteering. Congressional hearings conducted by Senator William Proxmire (D-Wisconsin) during the Vietnam War revealed similar defense industry exploitation.[3]

Incidents of negligence or exploitation by defense contractors in the U.S. have occurred more or less continuously throughout the nation's history. Clinard has noted, "[b]etween 1983 and 1990, a quarter of the 100 largest Pentagon contractors were found guilty of procurement fraud. In the 1988 to 1990 period, there were 16 cases involving 14 of the largest weapons makers."[4] In a more recent example, the Defense Department Inspector General found that deaths reported in Iraq in showers installed by a military contractor were caused by "improper grounding or faulty equipment," leading to electrocution when it short-circuited. The report concluded, "multiple systems and organizations failed," leaving soldiers "exposed to unacceptable risk."[5]

Other spectacular cases have involved influence peddling. Melvyn R. Paisley, an Assistant Secretary of the Navy with major responsibility for procurement, brazenly

exploited Washington's infamous "revolving door." According to the government, in the first 15 months after he left the Pentagon in March 1987, Paisley collected more than $500,000 in consulting fees from companies he had earlier befriended. Even worse, while in office, he corrupted the bidding process on hundreds of millions of dollars of weapons systems in order to divert contracts to those who secretly bought his services. The scams that swirled around Paisley were brought to light -- and eventually to justice -- as part of "Operation Ill Wind," the biggest and most successful federal investigation ever of defense procurement fraud. "Ill Wind" led to the conviction of government officials, Washington consultants, corporate executives, and seven companies.[6] According to Wall Street Journal reporter Andy Pasztor, more than 90 companies and individuals were convicted of felonies, including eight of the military's fifteen largest suppliers, all of whom admitted to having violated the law.[7]

Most recently, a Singapore-based company was accused of an audacious bribery scheme to defraud the U.S. Department of Defense into overpaying at least $20 million for supplies and services. Allegedly, Navy officers ordered ships steered toward ports where the company had an office. The firm then submitted bills that were padded or that included services never rendered, according to the indictments. The personnel involved allegedly engaged in a conspiracy to commit bribery. As part of the conspiracy, a senior Navy officer allegedly sent the contractor information that the Navy had classified as "Confidential," including schedules reflecting the movements of Navy ships months in advance. This officer had also operated as an advocate within the Navy for the company's interests, urging decisions about port visits and contractor usage that were designed to benefit the company. In return, the company provided the officer with paid

travel, luxury hotel stays and prostitution services.[8]

The U.S. Army has also experienced its share of contractor fraud. According to federal officials, one company obtained contracts with the Army Corps of Engineers to provide technology-related work and services. Starting in 2007, several company individuals began directing orders for technology work to a sub-contractor. The chief technology officer for the subcontractor then submitted fraudulently inflated quotes for work; the prime contractor then passed along those bills to the Army Corps. The contracting officers and company officials referred to the inflated work as "overhead," which was then paid out to the individuals originally ordering the work. In total, the unidentified company fraudulently inflated its invoices by about $20 million. For their help in the scam, the contracting officers received millions of dollars in kickbacks, flat screen televisions, luxury cars for themselves and their relatives, as well as high-end watches and liquor.[9]

The U.S. Air Force, too, has suffered from major procurement scandals. In the early 2000s, in an attempt by the Air Force to acquire new in-flight refueling tanker aircraft, senior Air Force and Boeing officials were convicted of procurement integrity violations and sentenced to prison for allegedly sharing procurement and competition-sensitive information.[10] At the same time, Boeing had been barred from government satellite launch activities because of procurement integrity violations stemming from the theft of rocket technical data from Lockheed Martin, their main competitor.

All of the above represent brazen acts that were both illegal and unethical, fueled largely by desire for personal gain. They are examples of the dangers involved when large sums of money are at stake involving contracts for weapons or services related to

weapons. These are highly visible deviations from ethical behavior. Let us now turn to the process of weapon acquisition itself, and see where along the way the process can go wrong and facilitate or produce the behavior described above.

III. Where can it go wrong?

In the weapons acquisition business, we recognize that there are three basic processes, each of which must operate properly for a well-designed and well-executed system of acquisition. They are:

1) the requirements process (embodied in the Joint Chiefs of Staff, Joint Capabilities Integration Development System) in which the senior warfighter leadership convinces itself a weapon is needed;

2) the financial process embodied in the DOD Planning, Programming, Budgeting, and Execution System (PPBES); and

3) the program management process embodied in DOD Regulation 5000.1.

These processes operate simultaneously and interact in multiple and complex ways, but each also has its own vulnerabilities. In the requirements area, we will discuss some potential issues as they relate to the very early phase of concept development in which the most basic decisions about the system are made. In the financial area, where budgets are developed but not yet enacted, we will discuss such potential ethical issues as realism in cost-estimating and lack of skepticism in reviewing and accepting contractor bids.

In the program management area, there are numerous points involving technology, testing, contracts, and financial rigor, at which ethical decision making by a program manager may be crucial. Weapon system acquisition professionals generally

think about the development and production of a weapon in terms of a so-called acquisition life cycle. Current thinking divides the life cycle into five phases, each separated by a decision milestone. First, of course, is the refining of the basic concept: what is it we are trying to accomplish, what problem are we attempting to solve, or need are we trying to address – and how do we propose to meet this need through the design and development of a proposed new system? The second phase involves technological development: what new technologies must we develop and deploy to meet the identified need? Thereupon follows the third phase of "System Development & Demonstration," in which engineers and defense contractors design, build, and extensively test prototypes of the new system and demonstrate their capacities to address the identified need. Assuming successful design and testing of the prototype, the next (fourth) phase of the acquisitions cycle is to gear up for full-scale production and initial deployment of the new system to the client military services. And, assuming the production phase proceeds as planned, the cycle ends with the fifth and final phase, in which the new system is put to broad use, maintained, repaired, modified as needed, and otherwise supported in its normal military use. It is important to recognize that there is a detailed ongoing assessment process in each of the phases, determining the degree of progress, cost-effectiveness, and overall satisfaction with the process, which can (in principle) be revised or terminated at the crucial "decision milestone" separating each distinct phase of the acquisitions cycle. Finally, while it is not the goal of this chapter to further explain the details or nuances of the acquisition business in its entirety, it is worthwhile to understand what goes on in the different phases to understand where ethical challenges may arise.

III.1 Moral Hazards in Concept Development and Refinement

Very early in the life of a weapon system, the developers (systems commands and contractors) begin working closely with users (soldiers, sailors, airmen, or marines) in an attempt to determine what the war fighter needs to be successful in his mission. Decisions made during this phase determine the basic type and functionality of a system and have a very big influence on its ultimate cost and schedule. While on the surface concept development sounds innocuous enough, there are, in fact, many opportunities in the formative life of a weapon system for ethical challenges and questionable behavior.

A question that needs to be asked early in, and even before, the concept development phase is: why are we considering the system in the first place? In most cases, the answers are clear and the systems are justified. Nonetheless, we must ask. Can the mission not be accomplished without the system, or is mission performance of our current system or systems in the face of new threats merely degraded? Would a change in operational concepts or tactics, techniques, and procedures preclude the need to buy an entire new system? Is the threat real, or is it only estimated and, if real, is it a case of increased adversary capability along with stated intent, or only increased adversary capability?

Since a company's existence may depend on winning or re-winning a contract, the contractor may actually try to convince the user they need a new system. One only has to attend one of the many military-themed conferences or symposia to find legions of contractors exhibiting their systems and proposed systems to understand the relationship between the military and the defense industry in the military decision process. And we

not only need to be concerned about the military, but Congress as well. Congressional influence, and the influence of corporations on Congress, is well known.[11] To continue to employ people in a particular State or Congressional District, a contractor needs to stay in business. To stay in business, contractors need to make a profit. To make a profit they have to sell things, and defense contractors sell weapons. So we might be led to wonder: are the weapons we buy a result of contractors pushing them, or warfighters demanding them or, more likely, some of both? Are the contractors exaggerating the threat? Are the government program managers doing likewise?

At the present moment, for example, military planners in the U.S. are attempting to assess prospects for cyber warfare and cyber weapons. Thomas Rid, writing in *Foreign Policy* on the topic, contends that cyber war is "still more hype than hazard."[12] In many respects, rhetoric about cyber catastrophe resembles threat inflation we saw before the Iraq War. Deliberately overstating (or understating) the threat—even for the well-intentioned reasons of advocacy—can raise questions of ethics and professionalism. As Brito and Watkins suggest,[13] the run-up to the war with Iraq in 2003 makes clear what can happen when a threat is misconstrued. In short, candor and tempered rhetoric are called for. They also point out that Washington teems with people who have a vested interest in conflating and inflating threats to our security.

A good example of a program in which the need was questionable, but the Service demanded a new system, is the new Air Force tanker aircraft. In the late 1990s, the market was declining for commercial airliners, and in the early 2000s, Boeing had lost the competition for the next generation fighter. The commercial airlines were in distress

due to the attack on 9/11/2001, and the Air Force was in the midst of buying and funding the C-17 transport plane, the F-35 fighter and the F-22 fighter. The Air Force had never indicated in any requirements process that they needed a new tanker, but then they tried to make the case that the current tanker was insufficient -- and that a sole source contract to Boeing was the only alternative. Numerous studies, to include those from the RAND Corporation and the Defense Science Board, however, indicated otherwise. The Air Force's appeal stalled until 2008, when Congress finally approved a competitive acquisition. This case was fraught with attempts to circumvent appropriations law, violations of procurement integrity laws, and improper competitive contract design and administration. Ultimately, both government and contractor executives served prison sentences as a result.

In addition to all of these corporate, political, and institutional issues, we find moral hazards on the level of personal and professional interests of those involved in acquisitions. Becoming an experienced and successful first-rate program manager is a difficult and career-long process. Promotion opportunities to senior ranks are far more limited than they are in the combat sectors of the military. A government program manager may be deeply invested in a particular program and view the success of that program as important to his or her promotion. Deliberate or not, this might influence the government manager's belief that a program is desirable or needed, and thus cloud what might otherwise be good judgment. While this is not the same as blatantly "unethical" behavior, it demands, at the very least, mature ethical judgment.

In sum, the ethical caveats at the concept development stage of acquisitions are these. Before we commit to hugely expensive new systems, we should be certain that

there is a real threat and that the motivations of both warfighters and their supporting industry are understood. There is a real possibility in this phase that insufficient skepticism by the government and excessive salesmanship by industry may lead to the procurement of unnecessary systems. Warfighter senior leaders should be sensitive to this classic "guns and butter" question: before we commit treasure to weapons, we should be absolutely sure of their need, lest other important priorities go unfunded. This is the perennial ethical dilemma at the core of defense acquisitions.

III.2 Moral Hazards in Technology Development

Once a decision has been made that a new weapons or defense system is needed and a determination is made of what types of system and technology are called for, that technology is to be matured to the point that a system prototype can actually be built and demonstrated. It is in the assessment of technology maturity that both government and contractor program managers must maintain objectivity and not allow extraneous pressures to drive poor judgment. Very often, contractors and their government counterparts will try to push a program into the next system development phase before the technology is ready. Sometimes this is based on a legitimate, but poor, assessment of technology readiness, but is often driven by schedule (and budget) pressure.

Entering the next phase of weapons procurement before the requisite technology has been adequately developed is known as "concurrence." Concurrence is almost always a bad and expensive decision. Why, then, do program managers frequently engage in it? Perhaps they truly believe the technology's success is just around the corner, perhaps the contractor assures them technology success is just around the corner,

perhaps it is a desire not to delay the schedule the program manager originally agreed to, as that could be taken as a sign of failure. Improperly motivated decisions at this point could be construed as unethical.

An excellent example of a program attempting to exceed the limits of technology – and failing at great cost -- is the Advanced Medium Range Air-to-Air Missile (AMRAAM). This was a case in which there was a well-documented need based on improvements in enemy air-to-air missile technology. However, the service (Air Force) and its contractors chose to implement a technology known to be immature (in this case, advance integrated circuits) too early into a production system. This program was also marked by excessive optimism on the part of industry and government program managers in regard to schedule, plus highly unrealistic contractor budget estimates – in the face of independent estimates to the contrary. Was all of this merely technological *hubris*, or was it motivated by other crass, and perhaps unethical, instincts?

Similar problems of concurrency occurred in both the F22 and F35 fighters, for which technologies such as advanced flight software and unique propulsion systems were designed into production systems, and production contracts were signed before demonstrating sufficient technological maturity – with resulting dramatic cost overruns. The Spaced Based Infrared (SBIRS) satellite system is another good example of the service prematurely committing to a production system: in this case, true advanced infrared detector technology maturity was wrongly assessed. More importantly, in this case the program managers demonstrated excessive optimism by allowing somewhat unchecked growth to requirements for the system, which could not be met by the technology.

These very expensive mistakes can occur legitimately, simply for reasons of misunderstanding the complexity and uncertainty of the required technology. It is just as, or even more likely, however, that the frequent occurrence of mistakes like this should be attributed to *hubris,* or else to an unwillingness to consider reality in the face of budgetary, and perhaps leadership pressures. In either case, the examples above resulted in staggering costs to the taxpayers and lengthy delays in delivery of the systems to the warfighters. While not the flagrant ethical scandals discussed earlier, the avoidable outcomes in these cases render them scandalous in their own right.

III.3 Moral Hazards in System Development and Demonstration

This is the phase of a new system's development during which, after the required technology development has been completed, major acquisition contracts are signed and the contractors are busily completing design and testing of their systems. It is at this phase, where a program is actually designated as a program, and where, as a result, the largest sums of money begin to flow.

If there is a competition, government managers must be extra scrupulous in designing the terms of the competition, and exceptionally diligent in watching for attempts by contractors to influence the outcome. It is here that lobbyists and contractor representatives have often resorted to bribery and other patently illegal and unethical behavior. During an arms-contract bidding competition, alternatively, contractors often provide bids -- hoping to win -- which are exceedingly optimistic and assume perfect

success. Perfect success, however, is never a realistic assumption, especially if there are lingering questions of technical maturity from the previous phase.

Government program managers need to treat optimistic bids with healthy skepticism. Unfortunately, even when presented with credible cost estimates by seasoned government estimators, government program managers too often opt to believe the contractor. While the managers are doing nothing overtly "wrong", this is perhaps an ethical error of omission. Once awarded, a contractor must successfully complete this phase and the successful bidder must convince the government that they indeed have a good system before a production decision is approved.

At the end of this phase the all-important test phase begins. First, developmental testing is conducted to insure the contractor has met contract requirements, and then operational testing is done to insure that a system, even if it meets contract requirements, is suitable for use in the field. This is an extremely important time in the life of a system, and contractor payment is on the line if the system fails to meet contract requirements. A lot of money will have already been spent and government program managers are reluctant to admit if there has been a failure. There are several opportunities here for unethical behavior.

What often happens is that when a program begins running behind schedule or over budget, one of the first things to be cut is testing. While this is purely a management decision, it can have really bad (and, in isolated cases, disastrous or potentially fatal) consequences. It is only through a thorough program of testing that the government can know if a complex system really works under combat conditions, and whether it is really worth the cost. Undermining that certainty is at least stupid, if not unethical. There have

been cases where contractors have been caught (and prosecuted) for actually cheating on these tests. In one instance, a company was fined for falsifying test data on its cruise missiles and fighter jets. In another, a company paid in a civil settlement for false testing, in addition to paying for repairs to the system in question.[14]

After developmental testing is complete, the system is turned over to the war-fighting units for operational testing to determine if the system, regardless of whether it functioned according to contract specifications, can actually be used in combat conditions. Contractors and program managers have little or no involvement in this phase, but the pressure to pass Operational Test and Evaluation and move on to production is enormous.

III.4 Moral Hazards in Production and Deployment

By the time a program has reached a point where a production decision is required, there is no turning back if the user has a legitimate need for the system. Large sums have already been invested. Presumably, testing has been successful and the decision to proceed is sound. The contractor is then responsible for delivering the system at the cost agreed, often on a fixed price contract. It is a fairly standard practice for a contractor bid to minimize costs on the first items with an eye to making more of their profit in upgrades and engineering changes later on, particularly in programs which are expected to last a long time and where large numbers of systems will be built.

While this is a business decision and it is not inherently unethical, government and military program managers need to understand and perhaps more closely moderate this behavior. Obviously, if the company can cut or reduce costs in production, it is to

their profit advantage. But this creates the incentive for contractors to cut corners on quality, to use illegitimate and unapproved material and part substitution, to overcharge, to cross-charge to more expensive contracts, to engage in defective pricing, to excessively reduce the workforce, and so on. Pietragallo gives a concise description of the various ways in which a contractor may attempt to defraud the government in this phase.[15] The number of cases of contractor fraud in this phase of the life cycle is significant, and indeed, most major defense contractors have at one time or another been caught and prosecuted for engaging in fraudulent behavior at this crucial state. As an example of this, at a jet-engine plant, one contractor paid the government millions to settle five civil lawsuits alleging contractor fraud involving the alteration of daily labor vouchers to inflate its billings.[16]

III.5 Moral Hazards in Operations and Support

In this phase, the weapon system is now finally in the hands of the warfighter and is likely to be in service for many years. The unfortunate problem here is that after a new weapon is designed and fielded, the contractors and acquisition professionals want to move on to the next exciting new thing. This is as it should be, since expensive science and engineering talent is being retained to develop new technologies and design new systems. It is unfortunate, but true, that the business of logistics and maintenance does not pay as well as research, development, and acquisition. For weapons acquisition, contractors make relatively larger sums of money over relatively shorter periods of time. The operations phase and lower paying logistics and maintenance activities of a system may last several decades.

One way, however, in which contractors can and do make additional profit during the operations phase is through the sale of spare parts and the provision of upgrades to the fielded systems. These can be quite lucrative. The B52, for example, has been in service since the 1950s and remains a formidable system due to extensive upgrades. It is estimated that the F-35 fighter's total cost, once operations are included with development and production, will approach one trillion dollars. Ethical challenges in the operational phase occur in the area of insuring quality of spare and replacement parts and in assessing the need for expensive upgrades.

The corresponding temptations and pitfalls are not qualitatively different from those already discussed for earlier phases in the acquisitions lifecycle. However, the soundness, quality and safety of the final product placed in the hands of the soldier constitute the ultimate test of the ethics of the process. Since the health of the soldier (not to mention the success of the war effort) depend upon the quality and safety of the final product, ethical misconduct that affects operations and support seems most egregious, and should be dealt with most harshly. Indeed, during the American Civil War, Congress considered passing a law that would allow the death penalty in cases where a contractor was found guilty of committing a fraud against the government through which a soldier was bodily injured, as for instance in the sale of unsound provisions.[17] This may seem exceedingly harsh in the present-day imagination, but it is an understandable sentiment in wanting to protect our forces from unnecessary harm.

IV. Conclusion

The stakes in defense acquisitions are hard to overstate. Weapons are, and have always been, important both to the provision of military security, and to the economic health of many nations, including the U.S. Defense industries are a major factor in the economy of many nations, and can prove to be a major drain on their resources. Weapons are a type of product whose manufacture, however, does not directly result in improving the lives of the majority of a country's citizens. So it should be with great care that the decision to purchase weapons is made, and it should be with great care that the process of building and delivering a weapons system is accomplished.

Cases of illegal or unethical behavior directly involving the production and sale of arms are numerous. They have occurred throughout history, and infect not only the United States, but all countries where weapons are bought or sold, and where there are fortunes to be made as a result. Companies that make weapons, especially those companies for which weapons are the only product or are the main products, sometimes owe their very existence to the continued sale of arms and the resulting flow of funds. Where weapons are developed and sold, money – and lots of it - becomes a driving force behind unethical behavior. It was so in the past, and it continues to be so in the present. I have tried to show the nodes in the weapons acquisition process where there are opportunities for ethical misconduct. Some of these are quite subtle, including threat inflation in requirements development, and ill-informed or deliberately over-optimistic cost-estimating. Others are more obvious: impropriety in contracting, bribery and influence-peddling, contract fraud, the falsification of crucial test results, and so forth.

We can also conclude from this chapter that two distinct categories of ethical lapse lurk within the defense industry itself. First are acts of commission: the "scandals"

enumerated in Section III exemplify deliberate acts of such illegal or unethical behavior. A second category contains acts of omission. In much the same way that negligence, while not an act of commission, can nonetheless be considered criminal behavior, acts of omission in the weapon procurement business could be considered unethical. These may not involve any direct transgression, but they can be just as significant. There may be a lack of due diligence or an imperceptible slackening of supervision. Furthermore, I have described several junctures in the acquisition process where financial gain itself is not the driving issue, but the desire for success, reputation or promotion yields an ethical omission. These can be especially hard to identify, since their cause seems benign. There may be a fervent, vested, and enthusiastic hope for a project's success. There might just be a tiny bit more optimism than is warranted. But in the acquisitions process, and particularly for the project manager, these have ethical weight.

The weapons acquisition process is well-designed and clearly understood, albeit enormously, and perhaps necessarily, bureaucratic. There are many opportunities in this sometimes lengthy and often contentious process for ethical lapses, but also opportunities for good ethical judgment. From rational, well-supported decisions to buy weapons, to truthful assessments of technological maturity, to realism in cost-estimating, to adequate testing, proper construction and billing practices, all the way to continued support of the warfighter in the field, there are numerous points in the life of a weapon system where both contractor and government managers must be vigilant about ethics.

NOTES

[1] Aaron Plamondon, "Defense Industries," in *Oxford Bibliographies: Military History* (New York : Oxford University Press, 2012): ISBN: 9780199791279; Online Resource, University of Toronto Libraries, Published online February 2012: http://dx.doi.org/10.1093/obo/9780199791279-0036.

[2] Howard Zinn, "Rebels and Robber Barons," in *History Is A Weapon: A People's History of the United States* (New York: HarperCollins, 2003): ch. 11.

[3] Marshall Barron Clinard, *Corporate Corruption: The Abuse of Power*. (New York: Praeger Publishers, 1990): 69.

[4] Marshall Barron Clinard, "Sociologists and American Criminology," *Journal of Criminal Law and Criminology* 41, no. 5 (January-February 1951): 549-577. http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=3835&context=jclc.

[5] Scott Bronstein, "'Multiple' failures led to Iraq electrocution, Pentagon says" CNN.com, (27July 2009): http://www.cnn.com/2009/US/07/27/military.electrocutions/.

[6] Irwin Ross, *CNN Money* (11 January 1993): http://archive.fortune.com/magazines/fortune/fortune_archive/1993/01/11/77357/index.htm.

[7] Andy Pasztor, *When The Pentagon Was for Sale* (New York: Scribner, 1995).

[8] See "How US Navy Sex, Scams Scandal Reached Phuket," *Phuket Wan* (7 October 2013): http://phuketwan.com/tourism/navy-sex-scams-scandal-reached-phuket-details-report-18953/.

[9] See "Former U.S. Army Corps of Engineers Manager Sentenced to Six Years in Prison in Bribery and Kickback Scheme," United States Department of Justice (13 September 2012): http://www.justice.gov/usao/dc/news/2012/sep/12-323.html.

[10] See Renae Merle, "Long Fall for Pentagon Star," The Washington Post (14 November 2004): A4. http://www.washingtonpost.com/wp-dyn/articles/A48241-2004Nov13.html.

[11] Brandon Michael Carius, "Procuring Influence: An Analysis of the Political Dynamics of District Revenue From Defense Contracting." Master's Thesis (Fairfax, VA: George Mason University, 25 March 2009)

[12] Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs* (November/December 2013): 77-87.

[13] Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *National Security Journal* 3 (December, 2011): 39-84. Available at: http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins.pdf .

[14] As related in Mark Zepezauer and Arthur Naiman, *Take the Rich Off Welfare* (Tucson, AZ: Odonion Press, 1996).

[15] See "Defense Contractor Fraud," at the False Claims Act Resource Center Blog (2014): http://www.falseclaimsact.com/common-types-of-fraud/defense-contractor-fraud.

[16] As related in: "GE:Decades of Misdeeds and Wrongdoing," *The Multinational Monitor* 22, No. 7-8 (July-August 2001): 26. http://www.multinationalmonitor.org/mm2001/01july-august/julyaug01corp4.html.

[17] "Government Contracts: The Fraud of the Contractors," *New York Times* (6 February 1862).

REFERENCES

Brito,Jerry and Watkins, Tate. (2011) "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy." Harvard Law School: *National Security Journal* 3 (December): 39-84.

Clinard, Marshall Barron. (1951) "Sociologists and American Criminology," *Journal of Criminal Law and Criminology* 41 (5): 549-577.

Clinard, Marshall Barron. (1990) *Corporate Corruption: The Abuse of Power.* New York: Praeger Publishers.

Pasztor, Andy. (1995)*When The Pentagon Was for Sale.* New York: Scribner.

Rid, Thomas. (2013) "Cyberwar and Peace: Hacking Can Reduce Real-World Violence." *Foreign Affairs* (November/December): 77-87.

Zepezauer, Mark, and Naiman, Arthur. (1996) *Take the Rich Off Welfare*. Tucson, AZ: Odonion Press.

Zinn, Howard. (2003) *History Is A Weapon: A People's History of the United States.* New York: HarperCollins.

"The Sniper and the Psychopath: A Parable in Defense of the Weapons Industry"[1]

Duncan MacIntosh

Dalhousie University

I Introduction

I here seek to answer three questions. First, are the rules that regulate the weapons industry -- rules found in business ethics codes, engineering ethics codes, procurement ethics codes, laws of the land, and dicta of conscience -- properly seen as absolutely binding? Or do they vary in how binding they are from situation to situation? I argue for a limited form of the latter, for a preponderance of the former, for a principle that tells how to draw the line, for a theory of rational choice on which choosing by this principle is rational, and for teaching defense industry employees the truth of that theory. The theory says that a choice is rational if dictated by the policy by which it is best to be ruled taking into account the effects on others of one's being known to be disposed to follow it no matter what from the beginning of one's life forward. And here, one would be best to follow a meta-rule which says to follow the sub-rules governing the industry provided that by doing so, one does not commit or permit a larger harm to the values in play. It is the latter clause which affords exceptions to the standard codes, but it is the benefit from

[1] For helpful discussion, my thanks to the students in my Introduction to Philosophy class at Dalhousie University, to the students who attended a talk I gave on my work at St. Mary's University, both in Halifax, N.S., Canada; and to the students in two classes to which I gave guest lectures at Millwood High School in Middle Sackville, N.S. Canada. Thanks also to Sheldon Wein.

the effects on other persons of being disposed to follow the standard codes that makes the justified exceptions so rare.

Second, isn't the very idea of a defense industry problematic given that it aims to produce lethal weapons for profit, a morally suspicious motive? I argue that in fact it plays a morally valuable role precisely because of its prima facie problematic motive. It can help us make progress in situations where an all-pervading morality of altruism would leave us paralyzed, it will enable the production of tools for our defense when we need them, and it will leave the majority of us with morally clean hands when morally problematic things need to be done.

Finally, I ask whether the existence of the weapons such industries produce can be a good thing, given their terrible power. I answer yes: their existence in a culture is a bellwether of the goodness of the culture, since only cultures offering everyone dignity, economic security, and respect for their rights can attract the vast population and sustain the infrastructure needed to produce such weapons; their production and use is required as part of the "conversation" between cultures about what constitutes goodness in a culture as this is worked out in the progress of civilization, where, of course, weapons are valuable in the defense of cultures, including good cultures; the apparent excesses of the weapons industry are justified as signalling to global citizens that they exist in an assurance game where the co-operation of others in mutually beneficial total deals will be enforced; but as good cultures become the norm, the weapons virtuous to have become more subtle.

My argument proceeds in three steps. First, I point out that there are occasions where, for profit or national security, one may be tempted to deviate from the standard

norms governing the industry. But then I offer a principle to say when these things should and shouldn't be done, and I offer a theory of rational choice that justifies choosing by the principle, a theory it would be salutary to teach to those in the industry as a means of making it more successfully self-policing.

Second, I point out that the prima facie morally problematic motive driving the defense industry, namely, to profit from making weapons designed for killing, can in fact be a good thing under certain conditions, much as the selfishness that drives capitalism can be good. In particular, this defense industry motive solves certain moral problems for us. For example, it gives us the tools needed for our defense, but does so in a way that leaves the rest of us free to have more prima facie morally laudable motives.

Finally, I argue that the existence of the industry does much more than this. It drives the conversation between cultures that evolves them into an ever better civilization.

II The Defense Industry and the Rationality of Complying With Rules For Good Conduct; Delimiting Permitted Situational Variation in Compliance With Defense Industry Ethics

The defense industry is regulated by codes of engineering ethics enjoining the manufacture of quality products honestly represented, business ethics codes enjoining good business character, procurement ethics codes requiring that product purchases be driven by mission needs and the public good, legislation forbidding, for example, bribery; and at least some players in the industry are regulated, if informally, by what their consciences take morality to require of them. But since sometimes the national interest is at stake in the behavior of a given player, it might be thought that such players should

sometimes violate these standards, e.g., if this would procure the materials needed to build a weapon of decisive advantage against an enemy of the nation. Relatedly, while many in the domestic defense industry are disposed to behave with integrity, they must interact with cheaters domestic and foreign. Isn't it then permissible to cheat in turn to level the playing field?

I say yes for both sorts of scenario, but surprisingly rarely owing to the fact that both companies and the nation may benefit more from its being a known fact that industry players are indisposed to violate policies forbidding such behaviour. Here I apply ideas from David Gauthier, arguing that the courses of action players should take are those dictated by the policy it most advantages them to adopt under ideal choice conditions, not the courses most advantaging in a given moment.

Much of the substance of the above codes, laws and moral principles involves prohibitions against things like using bribery to secure a contract, or to obtain access to a raw material needed to make a product, or to influence the politics of a region in ways advantageous to the company in question, or advantageous to its sponsoring nation state. Other concerns have to do with keeping business promises, providing the best product possible for the client, and ensuring that the product is accurately represented.

Some people reason as if these requirements were absolutes; others think the question of what to do can be solved by people simply behaving with integrity in the ways their specific professions demand. E.g., perhaps we should just encourage individual engineers to do the right thing as understood in their profession.[2] Ditto for,

[2] See Michael Davis, "Ethical Issues in the Global Arms Industry: A Role for Engineers", this conference.

say, procurement officers.[3] The idea is that large moral issues will take care of themselves if all parties obey the codes of ethics of their respective technical fields. More generally, it might be thought that morally correct outcomes would come simply from the unswerving application of technocratic and bureaucratic expertise.

But both views seem doubtful given the plurality of moral values we have duties to serve, given that the magnitudes of our duties to any such value appear to vary from situation to situation, and given the limited purviews of each of the aforementioned norm sources. This becomes evident when we think about what at least some aspects of the defense industry are for, namely, defending the realm, a presumptively just goal (at least if the realm is a just realm, or a candidate for such, on which, more below); or for the ensuring of justice elsewhere by force. These seem like things than which there could be no more important goal. And this suggests that, if in a given situation that goal would be best achieved by a company's, say, bribing a potential purchaser, or government official, or raw materials supplier, then so be it. This would simply be inducing someone to do right.

Likewise, sometimes the foregoing goals might be best achieved precisely by violating codes of engineering ethics requiring the manufacture of good products accurately represented. For sometimes those goals will be best served by building an inferior product and lying about its quality. Maybe it would be better to build a weapon that will rust out after five years, for then it would be unlikely to be of use to any unjust

[3] Kevin Govern seems to think something similar of procurement ethics in his "Acting Astutely in Government Acquisition: Procurement Integrity, Corporate Ethics and Avoiding Fraud in Logistics", this conference.

enemy who might confiscate it in battle, or buy it on the black market, or to whom it might be sold when they are a good regime, but of whom it is feared they may transform into a bad one. Selling weapons that have a tendency to expire could have the effect of confining their usability to the situation for which they are ostensibly being purchased. Or maybe the weapons should be able to be turned off by their manufacturer at the behest of the state in which the manufacturer resides, or of some bigger political body responsible for supervising global conflicts, e.g., the UN. So the correct larger moral positions do not so straightforwardly emerge from such lower level expertises as constitute the normative part of good engineering, or, indeed, of any other profession. In fact, sometimes correct all-things-considered morality may require violation of an individual profession's ethical code.

Of course, we might amend, for example, engineering ethics codes to require that engineers demand the foregoing conditions on the sale of the weapons they design – the engineers could take themselves to be obliged to so design weapons as to be operable only by those we have reason to think are good guys, for instance. But this would be to intrude global political matters into engineering ethics codes, so that the codes were no longer just about engineering. That might not be a bad thing, but it wouldn't vindicate the idea that obeying codes for technical professions as such will always express all-things-considered moral wisdom.

There are real world examples of the sometime appropriateness of violating engineering ethics codes from the software and computer hardware engineering professions. Think of the NSA's efforts to make electronics hardware and software non-secure so as to be able to monitor terrorist use of it. I'm not sure how this played out,

whether by the NSA asking, e.g., hard-drive manufacturers to emplace code allowing the drives to be accessed by others, or by the NSA hiring a private company to intrude the code stealthily, or by the NSA intruding the code stealthily themselves. But either way, we have those participant in the defense industry producing, arguably morally correctly, a bad product, or at least one that won't work as advertised. Obeying the supposedly absolute correct codes of conduct requiring producing a good product here might have been traitorous or morally evil, since it would be terrorism abetting.

Think too of the famous thought experiment due to Bernard Williams[4]: Suppose someone who has just earned his doctorate in chemistry can't find work, is in ill health, and can't support his family. But his former doctoral supervisor tells him he can get him a job. Unfortunately, the job is research aimed at making a weapon of mass destruction. The former student, George, objects on moral principle to working towards such a goal. But his supervisor points out that George isn't a very good chemist, and his involvement will set the project back years, so even as a pacifist he can accept the job in good conscience. This, again, would be a case where arguably someone would be doing right as an employee in the defense industry precisely by failing to live up to the various codes and standards presumed to govern it. And even if one was a good engineer, perhaps one should sometimes act to sabotage product developments, e.g., if the products are evil in purpose or likely consequence.

---

[4] In his "Utilitarianism and Integrity", excerpted from J.J.C. Smart and Bernard Williams, Utilitarianism: For and Against, 1973, Cambridge University Press in John Perry, Michael Bratman, and John Martin Fischer, Introduction to Philosophy: Classical and Contemporary Readings, (New York: Oxford University Press, 2007), pp. 519-527).

Or maybe sometimes one should leak to the other side trade secrets about weapons one's company or nation is developing (thus perhaps contravening a contract, this, again, in violation of a precept of good business ethics); for this might be hoped to produce a parity that will yield a standoff and so minimize the likelihood of the harmful use of the weapons. This is what motivated some people to divulge secrets to our enemies in the cold war. And sometimes such logic works directly to our advantage – think of defecting German physicists and Nazi scientists in WWII.

A related case of its being arguably appropriate to violate standard business ethics codes is that of the whistle-blower, someone who breaks commitments to her company and contravenes other supposed best practices because she thinks she has a higher duty to the public welfare. (Edward Snowden is the obvious example, although arguably he's not a whistle blower proper since he didn't stay to face the verdict of the judicial processes designed to adjudicate ostensibly whistle-blowing allegations.) True, whistle blowing might not be as good for my point, since arguably the laws enjoining and allowing whistle-blowing mandate the over-riding of other codes and laws, so that it's really an expression of defense industry rules -- at least taken all together -- not a violation of them. Still, it proves the point that sometimes right conduct consists in violating some rule, even if this is still at the behest of some other rule.

I've just argued that the correctness of the various codes defense companies operate under should be seen as situational, varying with such exigencies as may arise in the defense of the realm or in implementing justice more broadly; or that, even if they are always the right rules, sometimes it's better to break them -- however good the rules there

can be exceptions to them. But now let me make the opposing case that one should never violate these rules.

Taking an example from the above list, suppose this one time you'd get more money from an interaction in a business venture by bribing an official; or this one time your bribing him would be you inducing him to do the right thing. Why refrain?

There are many sorts of already well known general sorts of reason. For example, it could be that you so viewing a code as to have it that it's up to you whether you should obey it in a given context would make it more likely that you'll violate it in a context where it shouldn't be violated; or that it will make others lose confidence that you're likely to make correct choices in the future, this undermining your capacity to have self-advantaging or just effects in the future. Or maybe you so behaving will have indirect undermining effects on the likelihood of others behaving in ways advantageous or just. That is, the example of your behaviour may induce others into making bad choices, whether because these other persons are less morally discerning than you and so you should not set an example to them of autonomous, non-rule-governed decision making, or because your choosing to violate the rules will embolden persons less morally scrupled to do it more regularly than would be good.

Or maybe we have excellent reason to think that not even you can wisely make these calls; or that the greater wisdom would be to have these things be settled by rules once for all. For often, better outcomes result of people obeying rules of thumb about how best to act than of trying to figure out which action will have the best outcome in each case. This holds when there isn't time for research before acting; or when action is required in a time of panic when one would be better served by good habits of choice

than by trying to choose in some improvised way in a panicked state; and sometimes you may have chosen a rule at a moment of calm and wisdom, chosen it precisely to guide you in situations were calmness and wisdom were likely to be absent – you made a plan, and the entire point of plans is to provide clarity about what to do unless circumstances have provably changed. [5] Growing out of such reflections we even have act-utilitarian justifications for adopting rules against deciding how to behave by trying to ascertain the consequences of each action – act-utilitarian justifications against making choices the way an act-utilitarian normally would, namely, by calculating the utility of each action. Or think of contractarian justifications for adopting principles constraining one from making self-advantaging, or even prima facie everyone-advantaging, choices in the moment, justifications according to which you being able to be expected to be ruled by the constraint is likely to have better effects than you being free to do what you want in this individual situation. (I'll return to this last idea in a moment.)

Of course there may still be temptations. Perhaps the situation is this: domestically you must follow the rules because here we have the rule of law and these regulations on the defense industry advantage all local parties. Meanwhile, non-domestically, it's the Wild West. It may then seem that in non-domestic contexts you can and should do what advantages you even if it violates a rule prevailing domestically.

But even here the truth is that, if you behave that way non-domestically, you'll make it less likely that the region of what counts as domestic – the region regulated by mutually advantageous deals and so featuring reduced externalities – will expand. Yet such expansion would be to your and everyone else's disadvantage. Everyone is attracted

[5] See Michael Bratman's work on plans.

to the above codes of conduct provided they are as likely to rule the behaviours of others as of one's self. So by this argument you should exemplify the change you want to see in the world. At the very least, we have here an argument for you following the tit-for-tat strategy: be decent in your first interaction with someone, then copy what they do. If they are morally educable, they'll follow your good example. If they aren't and they then cheat you, cheat them back. Under conditions where there are more honest people than cheaters, as there typically are at the interface between home and abroad, this behaviour will reduce the number of cheaters even further (because they get out-competed by those who can trust each other in co-operative enterprises).

Meanwhile, it's widely agreed that the world as a whole is better off without corruption than with. Furthermore, studies show that companies do less well if they bribe. And yet individuals in companies might in the short-term be tempted. What could explain this? And what can stop them from thinking this way? George Ainslie has suggested that temporally near but inferior options can look better than temporally far but superior options by the obscuring proximity of the former, much as a short building seen close up can look taller than a tall building seen in the distance. So maybe we need to put the long run more fully in view.

But I suggest an additional strategy: we should teach as part of corporate culture that rationality and rational self-interest are not constituted of choosing the most advantageous action, but of choosing the action dictated by the most advantaging policy, which, of course, will forbid bribing. The idea is to recognize that individual company member rationality is really expressed by complying with the principles it benefits one's company to be known for following.

Bribery is known to be bad for the systems in which it occurs.[6] It's bad for companies as measured by their balance sheets, bad for individuals in companies as beneficiaries of success in companies, bad for countries as measured by the efficiency of their governments and as measured by the quality of the lives of its citizens. Why then does it exist? The standard answer is because an individual act of bribery can be to the immediate advantage of the immediate participants. And the standard responses to this are to set up a system of punishments, and to have company leaders model good character in hopes of this providing a compelling example to subordinates.

But I suggest both a further explanation of the temptation to bribe, and a further solution to the problem.

First, the advantage to an individual of a given act of bribery can explain its occurrence only if the advantageousness of an action is motivating of an individual, which it will tend to be only if the pursuit of advantage action by action is perceived by her as rational. And here philosophers have something to say. We know that the life of a given prospective participant in a bribe will go better if they are not disposed to participate. If they bribe, they will benefit from the act of bribing, but had they a character that would forbid participating in the act they'd benefit even more, since this would attract other opportunities for profit to them. And this raises the question whether it is more rational to perform individually advantaging actions, or to do the actions required by individually advantaging characters.

---

[6] See Philip M. Nichols, "The Business Case for Complying with Bribery Laws" American Business Law Journal Volume 49, Issue 2, Summer 2012, pp. 325–368.

The philosopher/decision theorist, David Gauthier has an answer[7]: the correct theory of rationality is the one most to your advantage to follow. The one most to your advantage to follow is the one that recommends you to have the character of a trustworthy person in business interactions, because this will attract to you more business opportunities, each one profitable to you. One might think that the character most advantageous to have will change over one's life. E.g., being known to be trustworthy might be to your advantage when making an exchange of promises of mutually beneficial behaviour with other persons, but disadvantageous when it comes time to fulfill your part of promise. If only you had a more scurrilous character at that moment, you could do even better, benefitting from the other person fulfilling her promise to you, while you get the additional benefit of breaking your promise to her. But of course, if you are known to be likely to think that way, no one will make sincere promises to you. Therefore, if you are to attract advantaging promises from others, it must be that the way you choose your character is once and for all, as if at the beginning of your life; for then you will not alter your character when it would be to your advantage to break a promise you would not have been in a position to break had you not first been the kind of person who would not break it, and so who could attract it. But since the right theory of rationality is the one that would afford you entry into the most advantageous arrangements in your life, and since the theory that you should choose the actions dictated by the characters you would find most advantageous to choose as if from the beginning of your life forever is the correct theory, and since the main such character trait in question would be that of a

[7] See David Gauthier, "Assure and Threaten", Ethics 104 (July 1994), pp. 690-721; and David Gauthier, "Twenty-Five On", Ethics Vol. 123 No. 4 (July 2013), pp. 601-624.

promise-keeper, it must be that what it is truly rational for you to do is to keep such promises.[8] The same rationale justifies not only promise-keeping, but also refraining from bribing, being honest, building good products, and all the rest of the things in the usual codes, laws, and dicta of conscience. For these are all characteristics essential to the magnetizing of other persons into profitable relations with you.

If only this theory of rationality were more widely taught and explained, we'd have less bribery. This therefore suggests inducing a level of philosophical reflection about the nature of rationality into corporate culture.

All right. I've given some examples of cases where it would seem good that the rules normally taken to regulate the defense industry be broken. I've also given arguments for why this shouldn't happen very much. But what rule should you use to decide which is which?

---

[8] This argument moves beyond even Gauthier's most recent work, I think, in the rationale it affords for adopting and keeping to a certain character. It represents my attempt to solve what I have called The Reversion Problem in Gauthier's own terms, using some ideas developed by Preston Greene (see his dissertation, "Rationality and Success"). The details of this needn't concern us here. But see my **Error! Main Document Only.**"Assuring, Threatening, a Fully Maximizing Theory of Practical Rationality, and the Practical Duties of Agents", Ethics, Vol 123, No. 4 July (2013), pp. 625-656. See also the debate between Gauthier and me in "Ethics Discussions at PEA Soup: David Gauthier's "Twenty-Five On," July 2013. (http://peasoup.typepad.com/peasoup/2013/07/ethics-discussions-at-pea-soup-david-gauthiers-twenty-five-on-with-precis-by-dimock-1.html)

The answer comes from the fact that the defense industry, like all industries, and indeed, like all economic activity, is animated by its participants aiming to make better lives for themselves. And like all economic activity, each participant has more advantage the bigger the system of which she is a part. For that means more trade, and so more profit, and so more advantage. But that means that one must always be aiming to expand the circle, to attract more and more people into arrangements regulated by a deal for mutual advantage. And people are attracted to people of good character, to businesses of good character, to countries of good character, and so on up to the largest possible units of social and economic interaction.

And this, finally, tells us the right principle, again, applying Gauthier's insight: Gauthier says a choice is rational if dictated by the character or policy by which it is best to be ruled considering the effects on others of one's being known to be disposed to follow it no matter what from the beginning of one's life. And here, one would be best to follow a meta-rule which says to follow the sub-rules governing the industry provided that by doing so, one does not commit or permit a larger harm to the values in play. It is the latter clause which affords exceptions to the standard codes, but it is the benefit one reaps from the effects on other persons of one's being disposed to follow the standard codes that makes the justified exceptions rare. In practice that means that you should obey the rules when obeying them expands the circle (for you, your company, your country, your civilization), break them to protect the expansion of the circle. So you get to cheat cheaters who cannot be attracted into the principles inside the circle and whose cheating obstructs the circle's expanding; and you get to bribe those who cannot be attracted into the principles of the circle and who would otherwise obstruct its expansion;

and likewise for each other sort of business vice. The matter is delicate, however; for if one deals too harshly with those who cannot be brought into the circle, others who might otherwise have been prepared to join may be repelled by the circle's preparedness to behave with inhumanity. This argues for a considerable gentleness to those intransigent to the attractions of the circle; you should make the circle such that, were you an intransigent outlier, you'd most want to be dealt with by that circle and not some other.[9]

III The Title Track Parable; An Argument for Exceptions to Compliance With Rules For Good Conduct

Next, I argue that sometimes morally best outcomes will be brought about only if some agents do not have normally morally approvable motives – their lack of such scruples and their readiness to be purely self-serving will liberate them to do things which happen to benefit all of us, but which leave most of us with morally clean hands. Along these lines it is therefore good that there exist private businesses in the defense industry driven by the profit motive, not moral goodness (rather than only public, governmental agencies bound by public morality). Here I apply in more extreme form some of the defenses offered of capitalism generally; and I speculate that this may explain the evolutionary persistence of occasional psychopathy and sociopathy (meant here non-pejoratively as referring to people disposed to self-serve, defy conventional morality, and test such things as legal boundaries).

[9] For more on this, see my "Re-drawing the Boundaries of Sovereignty: Permissible and Obligatory Interventions in the Affairs of Sovereign Nations", ms., Dalhousie University, 2013.

On the face of it, the defense industry is, well, indefensible. For prima facie it has the amoral aim of producing for profit devices meant to kill people. But I shall argue that an amoral entity such as this is sometimes needed to resolve moral dilemmas that cannot be properly resolved by ordinary morality, and yet whose proper resolution is essential to producing morally approvable outcomes. Later I will consider whether this means such an entity is functioning in defiance of morality, or whether it is something a proper understanding of morality shows in fact to be functioning morally.

Consider this case: a platoon has been pinned down by a sniper. One platoon member has been wounded by the sniper. Other members are agonized by his cry for help. Every few minutes one of them dashes over to try to rescue the wounded man. But each time, the would-be rescuer is killed by the sniper. The platoon has a safe exit route but cannot bring itself to retreat because this would mean leaving behind their wounded man.

The motives of the platoon members in refusing to leave vary: for one man the motive is friendship, for another, empathy, for another, a promise, for another, a sense of military duty, for another, a commitment to a moral principle, e.g., The Golden Rule; for yet another, a religious dictate, for another still, a view about dignity, for another, a respect for rights, for another, a view about what is virtuous conduct in a man, for another, enlightened self-interest and the worry that him letting down the wounded member would result in others letting him down later. Each, then, has as a motive for not leaving, one or another of the things that have been thought by one theorist or another of morality to be the basis of all morality, the ground of all duty.

One of the platoon's members is a psychopath. And since psychopaths cannot be moved by the sorts of considerations that move moral people as such, he is therefore unmoved by friendship, for this friend has outlived his usefulness. Empathy is foreign to him, because it is in his nature to be able to care intrinsically only for himself. And promises? They are made only for convenience to induce self-advantageous action from another and lose force once compliance would have no benefit. Military duty? That's something to which you pay lip-service to rise in the ranks, but all duty except duty to self is a myth. Moral principles? Just rules one follows only if there is situational advantage to doing so. For how could following any rule for its own sake be a benefit to the self? Religious dictates? Rights? They don't exist, or they do but there is no reason not to violate them for personal advantage. Virtue? What is virtue talk but the attempt by one man to impose a groundless limitation on the behaviour of another? Fear of later consequences? No; for psychopaths don't believe bad consequences will inevitably be imposed on them for bad action; in fact, they are compelled to test boundaries. So our man believes he has a good chance of evading all bad consequences for selfish action; indeed, he is compelled to try to prove this. And if he is caught for doing a "bad" thing, he thinks, whether caught by man or by God, he will figure out a way to escape the punishment when the time comes.

No, our psychopath quickly assesses the situation: he can't get home without a team to help him. The team won't let him leave as long as they are bound to stay, for then he'd be a mutineer. And the team won't leave as long as the wounded man is alive. Meanwhile the longer they stay the fewer of them there will be, because they keep sacrificing themselves in attempts to rescue the wounded man. So the longer they stay

the fewer of them there will be to help ensure our psychopath gets home if they ever decide to leave.

On the other hand, if our psychopath were to kill the wounded man, while the rest of the platoon would be outraged, they'd secretly be grateful that there was no longer a basis for a duty to stay; and they'd all retreat, grumblingly taking the psychopath along -- possibly for punishment later, but that is a bridge to be crossed when the time comes.

So without a pang of conscience our psychopath rises up quickly and shoots the wounded man dead. "Problem solved," he says, "let's move out".

What is the lesson? A number of possibilities:

First, maybe the psychopath in fact took the morally correct path – it was better that the rest of the platoon survive. But did he take it for morally correct reasons? Arguably not: his only motive was self-preservation. And did he cause the outcome in a morally correct way? Arguably not. He was not consultative, for example. And he didn't ask the victim's permission. (He knew consultation would only yield the status quo. And why take the risk of the wounded man's pleading for help yet again?)

Couldn't the platoon have come to the decision to do what the psychopath did, but by morally approvable deliberation? Arguably not. After all, each member would have the same reasons to vote not to kill the wounded soldier and retreat as each had to try to mount a rescue.

Couldn't all the members have reasoned together to come up with the conclusion that it would be all-things-considered objectively and impersonally morally better that they survive than that they all die trying to save the wounded man? And then couldn't they figure out a morally right way to bring that about? They could all act together like a

kind of firing squad to kill the man, putting him out of his misery in a way that shares out the responsibility, and freeing them to leave. Or maybe they would draw straws – short straw takes the shot. Either way, couldn't they have made the shooting righteous by asking permission of the wounded man?

All of these things might be possible. But as Bernard Williams points out in his discussion of the relationship between Utilitarianism and integrity[10], people who think duty requires only that they bring about the greatest good or happiness for the greatest number – Utilitarians – fail to be able to explain why, where bringing about the greatest good requires sacrificing someone, it is appropriate to feel morally bad about what one has done. Each member of the platoon would have to feel some blame and regret about abandoning their man. And each might well have felt, and be expected to feel, that in this case the Utilitarian calculation is self-serving in a way that is morally unseemly.

But if the psychopath solves their problem for them, they have no reason to feel pangs of moral blame, nothing to morally regret about themselves. Indeed, since the psychopath is immune to these sorts of bad feelings, the net result is better even by Utilitarian measures – the wounded man is put out of his misery quickly, the rest of the men survive, so their happiness is added into the equation; and the psychopath, since he does not suffer any pain of conscience about the killing, does not with such suffering detract from the pleasure added to the equation; and, of course, he adds in his own happiness at surviving. This outcome is then best by Utilitarian measures, even if non-psychopaths could have decided to kill the man. Of course there is another measure by which this outcome is not the morally best. For surely the psychopath ought to have felt

[10] See Williams (1973), reprinted in Perry, Bratman and Fischer (2007).

some remorse. It would be indecent not to feel in some way bad after having to do something like what he did. So the outcome is morally deficient for its failure to contain guilt. On the other hand, arguably the psychopath has an excuse for not feeling remorse, namely, that, because of his psychological condition, he cannot feel remorse. And an outcome cannot be morally faulted for failing to include an action or attitude that an excusing condition has made impossible.

Well, suppose the shooter hadn't been a psychopath, but instead what we shall call an 'altrupath', someone exclusively motivated by altruistic considerations. Couldn't he have reasoned that the correct action would be the one bringing about the greatest good for the greatest number, vis., killing the wounded man? And couldn't he then have taken the shot, and done so for morally right reasons? Well, perhaps such a person could make himself take the shot. But in doing so he would have to violate other things we think important in a moral agent, namely, each of the considerations that hypothetically motivate the other men to stay and attempt rescue – duty, promises, a sense of the other man's rights, friendship, empathy, love of his fellow soldier, and so on. Indeed, in this way, our altrupath is like the psychopath: he discounts important moral considerations in driving towards a good outcome. For reasons of generalized altruism arguably he fails any number of other duties.

Another possibility: our psychopath did something wrong. But in so doing, he made it possible for others to do right – to try to fulfill their duties of friendship, to follow their empathy, and so on. Indeed, maybe this was a better way for there to be the morally approvable outcome of the platoon being saved, namely, for them to be saved by the psychopath, and for each other member of the platoon to have the additional morally

good status of trying to be a friend, fulfill a promise, and so on. This is a better way to the outcome than, for example, by each of them having had to vote to violate their various other moral duties.

We now have a number of possibilities: that our psychopath did something purely wrong, or wrong but redeemed by the consequence of the platoon's survival, or wrong but redeemed by that consequence and by providing the occasion for yet additional morally right things from other agents (their good intentions and good efforts towards rescuing the wounded), as well as providing for the saving of them from having to do bad things (e.g., compromise their principles, or their commitments, or their natures).

To these possibilities, we might add that the psychopath did something understandable and forgivable. Or might we? What would be the basis of our forgiveness? That we could imagine ourselves doing something similar in similar circumstances? But we can't imagine it. That's what distinguishes psychopaths from us. They aren't merely selfish. They are exclusively selfish. Would it be that we forgive him because he couldn't have done otherwise given his nature? But for that sort of consideration, forgiveness is not appropriate at all.

At any rate, suppose we like the option that he did something wrong but redeemed not only by the good consequence of saving the platoon, but also by the good result that each platoon member was able to be additionally morally good: could we have designed the situation to be thus, to feature a psychopath? Could it have been morally required and permissible to put him in the mix?

But who could have made the decision to put him in the mix? Arguably not any of the directly involved persons who had reason of duty, empathy, friendship, and so on to

attempt a rescue. For their adding a psychopath would be the same as them pulling the trigger they morally can't bring themselves to pull. And not any other person who might have anticipated having any of those duties. One might think that the commander who put the troop together would have a duty to make sure that the outcome would represent a correct Utilitarian calculation about what should happen, so he should be sure to include a psychopath. On the other hand, surely the commander too would have difficulty making this decision. For by adding in a psychopath he would in effect be conditionally pulling a trigger that would actually kill a man should the platoon face the foregoing scenario. But perhaps the commander is in precisely the sort of situation that calls for him to make such choices. He's not supposed to be too close to his troop, precisely so that he can make the more impersonal decisions required to preserve his troop strength, and, speaking in more humane terms, to do right by the greatest number of people. Yet if the commander included a psychopath, and later learned that a situation arose in which the psychopath did what he was put there to do, the commander would have some degree of understandable regret and self-blame, even if it was the ultimately right call. Or maybe the commander could have arranged for the psychopath to be in the platoon, but be guilt free if the psychopath ever has to act. For the commander is morally called upon to make such decisions, and the right decision is to deploy a man who can do what the commander could not make himself do. Maybe I couldn't make myself kill someone who wanted to steal from my safe the medicine my daughter needs to survive. But perhaps I could put a spring gun in the safe. And if it winds up defending my daughter's medicine, that's not something that would have to be on my conscience. On the other hand, surely if something is the right thing to arrange be done, then it must be the right thing to do. And

if it can't be done without guilt, then it can't be arranged for without guilt either. It is known that one can find it rationally and morally obligatory to arrange for the doing of something one can't find it rationally and morally obligatory actually to do.[11] But it appears that putting that kind of distance between what gets done and one's self doesn't suffice to separate one from liability for guilt for what gets done. At any rate, we might think that a better outcome still would be one where the commander doesn't have to make these sorts of decisions. Better that there just happen to be a psychopath in the mix. For then the commander too is saved from pang of moral conscience.

Even better, perhaps, would be this: the commander has and acts on a duty to eliminate all psychopaths from the equation, but discovers that, luckily enough, he has failed in this. Now the commander is even better, morally, and so the outcome is better still. To take another tack, arguably we all have a duty to try to eliminate the psychopath from the equation. And yet we might be grateful to discover that we had failed. (To return to our commander, in constituting and sending out the platoon, perhaps he has a duty to insert a psychopath. But should he find himself a member of someone else's platoon, arguably he has a duty to root out the psychopath and neutralize him.)

Note that the psychopath can only do his job if he himself is empty of moral motivation. For if he is moved by empathy, friendship, and so on, he won't engage in the incidentally platoon-saving behaviour. So we need to be grateful for him having non-moral, immoral, or a-moral motivation.

---

[11] See Gregory Kavka, "Some Paradoxes of Deterrence", The Journal of Philosophy, Vol. 75, No. 6 (Jun., 1978), pp. 285-302.

Now, some, of course, will say that Utilitarian ethics would applaud what the psychopath would do, and, indeed, might even criticize those soldiers who would not do it. For their so-called moral scruples in effect result in many needless and morally unjustified deaths. And yet many criticize Utilitarianism for its using of the end to justify the means. Utilitarian arguments, it may be said, are in effect precisely attempts to justify immorality, perhaps to claim that sometimes immorality is necessary, even morally necessary. A paradox.

Either way, it appears to be better if the psychopath does what he does while at the same time the others don't do the kind of thing he does, and perhaps even have a nature precluding them from doing this, or follow a moral code precluding them doing this. It would seem good to have some people resisting Utilitarian calculi, while having others impose such calculations. The former persons in effect desperately treasure a given human life, while the latter persons proportion the value of each life to the total numbers of lives at risk; and the combination results in us having the net good of lives both saved and desperately individually mattering. We achieve this by moral division of labour, with some people doing the job of being Utilitarians, others, Kantians, Virtue Ethicists, Sentimentalists, and so on. In recognizing that this is a good thing, we discover that morality may recommend conflicting things to different people. (The Utilitarian and the others may be advised by the one true morality to fight over the gun that may be used or not used to kill the wounded man.)

I've said the presence of psychopaths can be a good thing. I want now to give some simpler, briefer examples. Suppose you and I are in a slowly burning room with only one exit. There is lots of time for us to escape, but the exit is only big enough for

one of us to leave at a time. Suppose we are both moral, altruistic people. Then likely each of us will say, “you first”. Then, trying to be helpful, we’ll both say, “OK, I’ll go first”. Then, back to “you first”. Then maybe I reach into my pocket and say “let’s flip a coin.” Unfortunately you do the same thing at the same time. Then, trying to be helpful, I say, “let’s use your coin.” But of course you are simultaneously saying the same thing to me. No, this could in principle go on forever. But suppose one of us is an ordinarily morally decent person, the other, a psychopath. Then the psychopath’s first impulse will be to leave first, and the decent person’s first impulse will be to offer the other person first exit. “Me first” says the psychopath; “I was just going to suggest that”, says the decent person.

Of course, sometimes it is useful to have an altruist around. Imagine the burning room contains two psychopaths. “Me first”, each says, and no one gets out. Then each tries to break the tie by mimicking altruism: “You first.” And now we have a repeat of the preceding problem. But suppose we replace one of the psychopaths with a morally decent person. Then she would say, “you first”, and the psychopath could say “thanks.” Problem solved.

It appears then that, despite the prima facie rightness of making moral evaluations of persons by the objectives given to them by their dispositions and characters – evaluations by whether they are selfish or generous, for example -- this does not correlate with whether their presence in a situation will be useful to the morally laudable solving of moral problems. Each character can have its place. Note that the burning room problem is not guaranteed to be solvable even by two altrupaths – they’d stumble all over each other

trying to figure out whose coin to use. But the problem would certainly be solvable by the presence of a psychopath with an altruist.

Now back to whether there is a morally clean way for a psychopath to be designed into a system, given his usefulness in solving moral problems. There seems to be no way for this to happen. For if someone, say the platoon commander, arranges for this, then if the psychopath ever has to act, the commander is morally tainted, should feel some remorse about what the psychopath has done, and so on. On the other hand, if the commander does his best to prevent the presence of a psychopath, and if this results in his whole platoon being wiped out, the commander is obviously in for another sort of remorse. Even if he gets lucky, inserts the psychopath, and the psychopath doesn't have to be used, or if he doesn't insert the psychopath, and there proves to be no occasion for his use anyway, the general is in line for a kind of moral condemnation, in this case, for either failing to make sure the platoon was equipped for a possible eventuality, or failing to make sure it wasn't infected with someone so cold-blooded.

What is the solution? Well, remember the special moral properties of the psychopath: he will feel no guilt, and he can't help do what he does. Then clearly the person whom it is morally best to have making the decision about whether he should be present or absent in a situation is the psychopath himself! He will feel no guilt either way, and he cannot be faulted either way because he has no choice about what he does given his nature.

My argument for there being able to be a good deployment of psychopaths presupposes that it is we who decide what situations the psychopath will be in, so we can make sure his nature will result in him doing things that have morally salutary results.

But what if the psychopath manages to be in the position of being the social engineer who constructs the scenarios, using us for his purposes? Surely then he is not so morally useful.[12]

It is true that if we don't get to define the parameters in which psychopaths operate and instead they define the parameters, then there are moral risks. But what I've just suggested is that, in fact, that might at least sometimes be a good thing. A psychopath's taking over can be the morally best way to solve a moral problem.

What finally to say then about psychopaths? Should we vilify them, or welcome their alternative perspectives and values? Where behaving as a psychopath would cause a morally worse situation, as where there is a consensus on what ought to be done by all moral values but the psychopath's impulses put him at odds with this, then the psychopath is unwelcome and must be policed. But where there is no such consensus, and where, paradoxically, a morally cleaner result will be afforded by someone not bound to conventional morality, incapable of guilt, driven exclusively by his own interest, and compelled to test boundaries, then the psychopath is most welcome.

Remember that I use the term "psychopath" without judgment or prejudice. I take it merely for a term of art to describe a certain psychological type. I neither condemn nor valorize that type going in. Moreover, a good deal of the moral valuableness in some contexts that I'm attributing to psychopaths could be offered by degrees of ordinary selfishness. Not all of it, however. This is because, for any merely selfish person, as the suffering of another person rises, and as the cost of helping them falls, there is an intersection point where the selfish person would help. Merely selfish people are in

[12] My thanks to Scott Edgar for this concern.

principle reachable by considerations of the suffering of others. Psychopaths by definition are not. They are not on the spectrum of selfishness and generosity. They stand in a different relation to those ideas. My purpose here is to see what may be said in defense of such a type. Arguably good managers don't see people as good or bad, just differently useful for different situations; and as a philosopher, in trying to provide a context in which psychopathy is morally acceptable, I am operating as a kind of "manager" of the over-all moral scheme in which we live, proposing (or recognizing) a morally laudable use for a certain kind of person. This may make me a psychopath. For I am proposing to insert psychopaths into the moral mix, the very thing I've been arguing cannot be done in a morally clean way. There is a reason academics are the first to go in oppressive states! At any rate, I suspect there is a morally good purpose for psychopaths in some situations. Indeed, according to evolutionary theory, nothing survives evolutionary testing unless it's good for something. Well, apparently at least one person in a hundred is a psychopath. And finding out why they haven't been eliminated from the gene pool would therefore be the same as finding out what they are good for, which is the same as finding out how they are good for us.

All right, but what exactly does all this have to do with the weapons industry? Weapons are things most cultures at one time or another have a need for. And as I will argue, weapons are both evidence of, and means towards, goodness in cultures. But the motives that drive weapons production are prima facie not moral. The aim to make a profit building devices for killing people is prima facie morally problematic. And yet there is a Utilitarian call for such weapons. So it is morally good that they get made. But it they are to get made, we need manufacturers who in effect have non-moral (neither

right nor wrong), immoral (wrong), or amoral motives (motives had without regard to their rightness or wrongness). Someone has to have these motives in the division of moral labour. Metaphorically speaking, someone has to have psychopathic motives. And because some people have them, others of us get to have nice motives most of the time – we get to have the officially valorized humane motives. We get to be nice, until it's time to be not nice. And then, when we need weapons for self-defense or some other, hopefully good cause, the weapons manufacturer has products ready to sell. Moreover, weapons producers in effect select themselves into the business by the profit motive, a motive that is neither here nor there morally speaking; and in self-selecting into the business, they spare others the moral stain of having decided to put them into the mix.

Problem solved. Let's move out.

Now, it might be argued that we do not need to represent, and would be mistaken in representing, the typical player in the defense industry as being psychopathic, or as having psychopathic motives. Well, I agree that the first claim is too strong. Most people in the business are just ordinary people who are wonderful to their spouses, children, parents and friends, are good community citizens, and so on. They just happen to have unusual jobs. They aren't psychopaths. On the other hand, a part of their psychology is a little unusual: it allows them to build devices for killing people.

It might also be objected that we can see defense industry players as being perfectly ordinarily moral rather than psychopathic in their motivations if only we see them as people who wouldn't design and build weapons except for a good cause – the cause of killing only people who deserve to be killed, for example.

But this objection misunderstands my point. I'm saying that the weapons industry can only solve certain of our moral problems if it is prepared to produce not just weapons for those deemed to be on the good side of conflict. Rather, the problems I imagine the weapons industry to solve require a preparedness to sell weapons to anybody, good or bad. We need Lords of War. And if a given person in the weapons industry isn't that kind of person, he isn't contributing to the solution of the problems I have in mind. (Of course that might be fine. That person might be doing other things, perhaps morally useful things.)

I turn now to explaining this special role for the weapons industry.

IV Right Makes Might

I now suggest that the existence of the weapons the defense industry produces can be a good thing, even given, and indeed, because of, their terrible power; and a good thing not just because they can be used in self-defence or for some other prima facie good cause. I claim that their mere existence in a culture is a bellwether of the goodness of the culture, since it tends to be true that only to the degree that a culture offers everyone dignity, economic security, and respect for their rights can that culture attract the vast population and sustain the infrastructure needed to produce such weapons.

It is the measure of the goodness of a culture just how good its weapons are -- the better the weapons, the better the culture. Thus it is no coincidence that the most well-weaponed and powerful country on earth – the U.S. -- is also the country that mostly has the morally right end of the stick, and that most defends individual liberties. Probably too it is no coincidence that it is also a gun culture. For what is true in the large in this case is also true in the manner of fractals right down to the small.

But the better the cultures there are, what counts as virtue in a weapon changes. When there are good as well as very bad cultures, both ideologically evangelical, or at least one rapacious, cultures therefore constituted as engaged in mass conflict, weapons of mass destruction are virtuous. But when most cultures are good, and the only conflict is with misguided outlier cultures, or outliers within good cultures, it is weapons of precision and minimal or highly controlled lethality that are virtuous. Indeed, the subtilization of the world's weapons is a bellwether of the moral evolution of its cultures. This has come so far that now soft skills needed to win hearts and minds are the best tools of warfare – they've been weaponized.[13] And this is the transformation of war into something else – the display of the virtues of a given culture to attract others to participate in it.

Given all of this it is right that military matters have come more to pervade university culture, just as law pervades all culture. It is obviously important material for academic study. And it is good to have this studied in a university context since it is there that it will be most independently studied, and there that the military impulse will be best negotiated with the sorts of liberal, left and pacifist thinking that tends to be found in universities. This will result in its tempering by the social sciences and the humanities, the soft arts; and its study is ultimately the sort of thing that the social sciences and humanities are for. They are supposed to be the deep and reflective conscience of a liberal culture. And it is especially important that this be studied in America, since

[13] See David Miller and Tom Mills, "Counterinsurgency and terror expertise: the integration of social scientists into the war effort", Cambridge Review of International Affairs, Volume 23, Number 2, June 2010, pp. 203-219.

America really is the leader of the free world. And increasingly, warfare as it is researched and taught at American universities is more statecraft than anything else.

One might think that, for obvious reasons, the defense industry is necessarily immoral or amoral. But some weapons are so fantastically knowledge-dependent, expensive, and labour intensive that they can only come to exist in highly socially stable nations with broad liberties, social safety nets, and so on. Only the morally best societies can afford the best weapons; morally best social arrangements tend to attract, and attract for morally good reasons, more people than other societies, and they tend insofar as they accrete other individuals through violent means to do this more justly than other societies – e.g., by fulfilling duties of rescue to those in unstable states, or in states whose regimes persecute them, then withdrawing all but the forces needed to supervise democratic reform. So the existence of superior defense industries in a society can come about only by virtue of the moral goodness of that society, their existence is evidence of the goodness of that society, and their existence tends to cause the morally good increased pervadingness of that society; for it provides the means for the society to defend itself, to fulfil duties of rescue, and to encourage the formation of other, like-minded states. The defense industry also employs vast numbers of people and makes huge contributions to the economy and to people's wealth. What with one thing and another, then, and again contrary to conventional thinking, Might Makes Right.

Counter-examples will be offered: Germany, Russia, China. But Germany lost, Russia lost and is losing still, and China only progressed by increasingly approximating the presumptively good societies of the West. And as more and more of these moral victories are achieved, the natures of the fruits of the defense industry are changing too,

to a more moral product. Thus we move from weapons of mass destruction with which to fight wars, to weapons of micro-destruction to be used in police actions as we clean up intractable pockets of moral infection. Indeed, we are now at the point where the bigger the weapon you think you need to solve the problem, the bigger the mistake you are probably making in whether you are seeing the problem in the right way, and taking the right step.

What of the public/private distinction? First, one might think that federally produced weaponry should be governed by whatever would best advance the national defense. But should there then even be a private defense industry? Sure, for arguably not all issues of defense are national: individuals and sub-national entities have need of defense too. Well, should a defense company in one nation be able to sell to other entities? Arguably yes, on the ground that on average and over the long haul, whomever can best afford the best weapons is most likely the most just deployer of the weapons.

And in any case, a weapons industry that is not necessarily dictated by government will have a profit motive and therefore be capable of the quasi-moral role I discussed above, something perhaps not possible if it is an organ of government, with all the limitations that implies.

One might think that the best explanation for the predominance of the weapons industry in the U.S. is that, first, the weapons industry has in effect created a merely perceived need for its own weapons with false advertising, or has bought the interest of legislators in its products; or that, because its weapons were available to the U.S. in the past, the U.S. engaged in risky and violent adventurism in its foreign policies and now

finds itself with many enemies for defense against whom it now needs these weapons. Either way, the predominance of the industry is, arguably, specious.

I favour another explanation: the U.S. is just the pre-eminent player in a larger social role, that of ensuring the stability of the global Assurance Game. Studies have shown that most people will do the right thing – not steal, not lie, work hard for others, and so on -- provided they think everyone else is being like this too. What many people won't do is be the only person doing the right thing – they won't play the sucker. Thus most people in a given country obey its laws not from fear of being caught and punished if they don't, but because they are disposed to do so provided they don't think that others are taking advantage of them by cheating. Thus in these persons' minds, the role of the police is not so much to regulate them; it is to regulate others. And the same holds true, I suggest, of the relations between nations. Most nations will do their part in proper relations between nations provided they think all other nations are doing this too. And this would be advanced if there were an international force that would police violations of things like international agreements. Each nation would then feel like this force is not so much to regulate them, as it is to regulate deviating outliers.

Now, there is no giant supra-national enforcing agency. There is the UN, of course, and various international regulative bodies. But they have no muscle. Or rather, their muscle is provided by countries like the U.S.

Nations need of a sense that people and peoples won't get away with very bad behaviour. It is a good thing that there be large countries with large symbols of power to keep other countries in line, not necessarily from fear, but from the sense that someone

will punish free-riders and marauders, this freeing the rest of us to do right things, confident that we won't be played for suckers.

Enter the massive weapons industries of the West, in particular, of the United States. The United States is a bit like Iron Man, or Superman, someone enormously powerful and, fortunately, benevolent, someone whose presence therefore makes others feel secure against offending outliers. It is of interest that there are very few people who really want to see the U.S. undergo a decline in its status as the world's only superpower. The U.S. is a kind of Leviathan by default.[14] Indeed, the size of its power is widely seen as proof of its righteousness, and of its being suited to play this role.

I call it a kind of Leviathan, rather than a Leviathan unqualified, because it has influence and power not simply by the threat or exertion of force, but by being the best power in the market – it offers people what they want, so they aren't just agreeing to

[14] "Leviathan" is Thomas Hobbes' name for the state, conceived as an all-powerful force for the regulation of human affairs. He saw two possible ways people to come to be ruled by such a thing. The first way was by "institution": people who otherwise find themselves at war with each other agree to give up their power to another entity, one made more powerful by each person ceding her power to it, in hope that this entity will bring about more peace and order than is found in the war of all against all. The second way one could come to be ruled by a Leviathan is by an extant Leviathan threatening you with death unless you concede your power to it. This is coming to be ruled by a Leviathan by "acquisition". In the first way, people institute a Leviathan from fear of each other; in the second way, people get acquired by a Leviathan by means of conquest.

accept some strongman rather than none, nor even accepting the strongest strongman; they are accepting the best strongman, the one they'd create if they had the power.

Another way in which the U.S. is only a pseudo-Leviathan is that it is not itself invincible. But its moral compass is very appealing, and the head-start that its might provides in advancing a just cause attracts and emboldens others to fight arm-in-arm with it as required. It is a Leviathan "kernel", a nucleus around which other forces will gather to create a Leviathan ad hoc on an as and when required basis.

The foregoing argument may even provide an excuse for the existence of expensive weapons boondoggles. For their existence proves that there is a large and powerful authority constantly trying to perfect the weapons of authority, something which gives us all confidence that we are in a well-regulated assurance game. These giant weapons, most probably never to be used, are like the Pyramids of Ancient Egypt, symbols of a consensus about who should be the great power.[15] And the fact that so many people work on the production of these symbols tends further to be part of what gives them this power: they are the symbol of the security of the Assurance Game, they provide employment to many, the employment they provide is in the service of something prima facie good and powerful, they fuel an economy, and so on.

[15] Josh Ritter has a song about an archeologist who unearths a mummified Egyptian Pharaoh. It is a story of a mummy's curse. The curse is that whoever awakes the mummy gives her life force to him. "Why pyramids?" she asks as she lies dying, mummifying. "Think of them as an immense invitation," he replies. Then he kisses her and hopes that she'll forget that question.

Why does someone have to have the most weapons? Because someone has to stand out as salient for the according of highest authority. And this means someone has to have the greatest symbols of such authority, the most "bling", even if, in some sense, this means having a superfluity of bling. Lots of countries have nuclear weapons. But the U.S. has the greatest superabundance of them, the capacity to destroy the world the most times over. Will it ever use them? Of course not. That's not why they exist. They exist to induce alliance, and to induce it not by fear, but by instilling confidence of righteousness and of victory.

Couldn't something else in a nation play this role? Perhaps. NASA may have done this for a while. And you can't kill people with pyramids. Maybe one day the salient kernel will be a giant health system. On the other hand, there has to be the sense that there is an undiluted source of justice and the power to enforce it.

So strong is the correlation between the increasing justice of a society and the increasing success of its defense industries that one might even wonder which is the tail and which the dog.

V Bringing the Three Strands Together

I have suggested that the most successful weapons tend to be deployed by the most just societies. This may go some way to easing the conscience of defense industry players. For on average, the only people who can afford to buy the best weapons are likely to be those morally just of heart and just in their intentions for these weapons. Now, it may seem that if one is selling weapons to one or both sides of your basic small potatoes civil war, it is not clear who has the right view about what should be the outcome. But this is really an argument to go ahead and sell your product; for the question who is in the right

is in the process of being decided, and the winner will tend in the limit of inquiry to converge on the group that ought to win. One should simply sell to the highest bidder. (In fact, one should sell to all bidders. This is partly why one needs a certain amount of "psychopathology" in the defense industry: it has to be willing to do this, else culture cannot progress.) In general, on average and over the long run, the highest bidder will be the most just bidder, because the wealthiest societies will tend to be the most just. Selling small arms to the highest bidder is defensible for the same reason as that the best weapons are had by the best culture. They'll tend to go to the highest bidder, who will be the best culture.

But of course, even if it were true that having good weapons is a bellwether or indicator that a culture is good, surely that doesn't constitute a justification for the existence of such weapons? E.g., surely if a culture was now good, but didn't have good weapons, it shouldn't go out and make some.

I reply that as it happens, the only way for a good culture to appear, to come about, is by dueling it out with other candidate cultures – it is precisely by the process of warring that one finds out which cultures are good. Over a suitably long period, might makes right. Right is therefore discovered by the contesting of mights; and the inevitable by-product is amazing weapons. The weapons phase is a necessary phase in the evolution of cultures, and one therefore morally justified. For while one might think that in the ideal culture there would be no need of weapons, people are still learning to live in large cultures, and still learning how to raise children well in them; and until the lessons are learned there will be conflict between cultures, and between people within cultures raised problematically and without the meeting of their basic needs. And weapons are necessary

to resolve this. It might be thought that a better culture would be one that settles things by peaceful means, and that the existence of the weapons industry sabotages this by making available the tools to settle things by violent means. Unfortunately, the fact that conflict is best dealt with non-violently is itself a piece of cultural wisdom that had to be discovered the hard way, and that, ironically, still needs weapons to defend itself from those culturally unable to appreciate it.

Now, Jens Ohlin has recently used David Gauthier's ideas to provide argument to the effect that people and nations can find it rational to form and fulfill agreements to co-operate in Prisoners Dilemma type situations even without need of enforcement mechanisms for compliance.[16] And I used similar arguments above in a proposal about how to improve compliance with good codes of conduct in the weapons industry. Surely then I must think that it is false that conflict is inevitable, false that weapons are ever strictly needed, false even that we need a Leviathan, pseudo- or otherwise.

But the foregoing sorts of argument only establish that enforcement will not be needed among agents who can detect each others' natures and so who can restrict the offering of mutually beneficial deals that require mutual vulnerability to those who will be disinclined to exploit the vulnerability. This is no guarantee against the existence of irrational agents who will try to be predatory on the former sorts of agent. For these outlying agents you need force. The world of co-operators could create such a force for the neutralization of these irrational free-riders. This would be for the co-operators to create a kind of Leviathan by institution. But instead what it has done is allow such a

[16] See Jens Ohlin, The Assault on International Law (New York: Oxford University Press, 2015).

force to accrete. That force is America. And it is both the Leviathan and armourer of the world.

Acting Astutely in Government Acquisition:
Procurement Integrity, Corporate Ethics and Avoiding Fraud in Logistics
by Kevin Govern

Abstract:

To maintain global repute for integrity, both military and civilian leaders need to keenly understand the operating environment in which they are and want to be located: they recognize legal obligations, cultural expectations and ethical dilemmas; they avoid conflict when possible; they balance the interests of various stakeholders; and finally they develop strategies for legally, morally, and ethically influencing friendly and adversarial individuals and entities.

This "executive summary" of a forthcoming paper will highlight not only domestic and international legal obligations but also guiding ethical and moral principles critical to procurement and acquisition integrity. Most common ethics and procurement integrity issues can be avoided by avoiding circumstances of public officials using their office for private gain, treating all members of the public with fairness and impartiality, and preserving the notion of public service as a public trust. Much more subtly, all involved in government procurement and acquisition must employ what business executives define as "cultural astuteness;" "[t]he ability to get out of your . . . comfort zone and navigate smoothly through the cultural nuances of your specific area of responsibility."[1]

This paper will help define the ways in which procurement officials cooperatively "move …goals forward in a way that is not seen as self-serving . . . through a combination of direct communication, influence, and asking other people to be [their] advocate or champion,"[2] in ways that comport not just with legal and ethical requirements but promote efficiency, effectiveness, and economy.

Procurement and Acquisition Integrity:

To establish a common vocabulary, the term *procurement* involves the acquisition of goods, services or works from an outside external source. When speaking of and acting consistent with *integrity,* there should be a firm adherence to a code or standard of values. Together, *procurement integrity* encompasses a range of legislation, regulations, directives, actions, and attitudes for preserving the integrity of procurement and assuring the fair treatment of bidders, offerors, contractors, and others with a legal and / or operational stake in the outcome.

Commonly accepted cornerstones of procurement integrity are to: refrain from using public office for public gain; treat all members of the public with fairness and impartiality, and; act consistent with the notion that public service is a public trust

Some Common Ethics and Procurement Integrity Issues include but are not limited to:

- Conflicts of Interest
- Financial Conflicts

[1] Connie Glaser, *Doing a good job isn't enough – 'cultural astuteness' is needed to succeed*, BUS. FIRST – LOUISVILLE (July 20, 2007) < http://www.bizjournals.com/albany/stories/2007/10/22/smallb2.html>.
[2] Id.

- Impartiality Issues
- Gifts (from / to contractors and from/to US and Foreign Government Officials)
- Procurement and Other Nonpublic Information
- Restrictions on Employment Discussions
- Seeking (post-government and concurrent outside-) Employment (with a bidder or offeror, after government)
- Accepting Compensation from a Contractor
- Post-Employment Restrictions
- Fundraising
- Letters of Recommendation

Acquisition Logistics and Fraud, Waste and Abuse (FWA):

Acquisition logistics is a multi-functional technical management discipline associated with the design, development, test, production, fielding, sustainment, and improvement modifications of cost effective systems that achieve the user's peacetime and wartime readiness requirements. In this field of technical management, fraud is a type of illegal act involving the obtaining of something of value through willful misrepresentation; a judicial or other adjudicative system beyond an auditor's professional responsibility.

Waste involves the taxpayers not receiving reasonable value for money in connection with any government funded activities due to an inappropriate act or omission by players with control over or access to government resources (e.g., executive, judicial or legislative branch employees, grantees or other recipients). Waste goes beyond fraud and abuse and most waste does not involve a violation of law; it relates primarily to mismanagement, inappropriate actions and inadequate oversight.

Abuse is the sort of behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. Whether one-off instances by those who are otherwise good stewards of resources and leaders of people, or by "toxic" leaders whose *modus operandi* is such consistent practice, abusive behavior includes, but is not limited to, misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate. It is notable that abuse does not necessarily involve fraud, violation of laws, regulations, or provisions of a contract or grant agreement, but inevitably is inconsistent with the morale and welfare of teams and work groups, and may well erode corporate "good will" or organizational reputation.

Preventing and remedying FWA saves valuable resources by identifying illegal, inefficient and wasteful practices. This also makes funds available for other, better uses than detection, investigation, correction, and remediation. The key to prevention, detection and reporting of FWA is recognizing early indicators; that is, conditions that allow management controls to be exploited. These early indicators often show up as minor administrative or managerial irregularities but are initial warning indicators key to prevention.

General Legal Considerations: Procurement Integrity Act (PIA) and FAR 3.104 (Procurement Integrity) with the special DoD, Service and Command Regulatory Supplements

The Federal Acquisition Regulation (FAR) is a system that codifies and publishes the "uniform polices and procedures for acquisition by all executive agencies." The FAR system consists of the primary document of the FAR, "and agency acquisition regulations that implement or supplement the FAR," such as the Army Federal Acquisition Regulation (AFAR), the Defense Federal Acquisition Regulation (DFAR) and the Special Operations Federal Acquisition Regulation Supplement (SOFARS). Consistent across the board of these legal considerations, there exists with few exceptions or exclusions:

- A ban on disclosing procurement information ("contractor bid or proposal information" and "source selection information");
- A ban on obtaining procurement information;
- A requirement for procurement officers to report employment contacts by or with a competing contractor; and
- A 1-year ban for certain personnel on accepting compensation from the contractor.

Special Legal Considerations Abroad - Foreign Corrupt Practices Act (FCPA)

Anti-bribery provisions of the FCPA prohibit any U.S. Company or person in the U.S. from "corruptly" giving "anything of value" directly or indirectly to Government Officials for the purpose of obtaining or retaining business or securing an improper advantage; in short, no bribery. The FCPA contains accounting provision that prohibit secret accounts, and requires keeping books, records and accounts in reasonable detail that accurately and fairly reflect the transactions and dispositions of the company.

The "cardinal rule" of an FCPA–compliant accounting program is documentation of expenditures. At a minimum, such programs should document every marketing expense, facilitating payment; the effect is also to discourage cash payments. FCPA-compliant programs also maintain an internal accounting system assuring that transactions are executed and assets are disposed of only in accordance with management's authorization; recorded to meet generally accepted accounting procedures (GAAP), and include periodic audits of existing assets

Department of Defense Standards:

To protect the trust the Nation bestows upon Government employees, it is necessary that Government employees uphold the highest ethical standards. Department of Defense (DoD) employees abide by the standards of ethical principles (Principles of Ethical Conduct) and set a personal example for fellow employees in performing official duties within the highest ethical standards. Government employees fulfill the public's trust when following the ethical standards.

The Ethics in Government Act of 1978, October 26, 1978, as amended, the Office of Government Ethics implementing regulations, and the DoD Joint Ethics Regulation DoD 5500.7-R (JER) are sources of the standards of ethical conduct and ethics guidance, including direction in the areas of financial and employment disclosures and post-employment rules among other matters.

For uniformed service members, Congress has promulgated Exemplary Conduct Statute prescriptions and proscriptions, with a heritage that dates back to the Colonial Era rules established by John Paul Jones for the nascent Navy; as an exemplar, the Exemplary Conduct Statute for the U.S. Army, at 10 U.S.C. 3583, and notable for private industry partners who work with uniformed service members, the statute reads as follows:

> All commanding officers and others in authority in the Army are required—
> (1) to show in themselves a good example of virtue, honor, patriotism, and subordination;
> (2) to be vigilant in inspecting the conduct of all persons who are placed under their command;
> (3) to guard against and suppress all dissolute and immoral practices, and to correct, according to the laws and regulations of the Army, all persons who are guilty of them; and
> (4) to take all necessary and proper measures, under the laws, regulations, and customs of the Army, to promote and safeguard the morale, the physical well-being, and the general welfare of the officers and enlisted persons under their command or charge.

Business Ethics Standards – the Essence of Any Business With DoD and Any Client / Customer

Every business entity should have a “Corporate Vision” that is consistent with its clients'/customers’ needs and “vision,” or at least not at cross-odds with it.

Case in point, and by way of comparison, Lockheed Martin's Vision is as follows:

> Lockheed Martin is the leading global security and aerospace company, solving our customers’ most difficult problems through our employees’ innovation, performance and unmatched integrity.

The DoD Chief Information Officer’s (CIO’s) Vision is:

> DoD and partners securely access information and services they need at the time, place and on approved devices of their choosing.

Similarly corporate values must be lived and not just stated. Lockheed-Martin exhorts its employee team members to:

Do What's Right: Committed to the highest standards of ethical conduct in all that they do. Believe that honesty and integrity engender trust, which is the cornerstone of our business. Abide by the laws of the United States and other countries in which they do business, strive to be good citizens and take responsibility for their actions.

Respect Others: Recognize that their success as an enterprise depends on the talent, skills and expertise of their people and ability to function as a tightly integrated team. Appreciate diversity and believe that respect - for colleagues, customers, partners, and all those with whom they interact - is an essential element of all positive and productive business relationships.

- ✓ *Perform With Excellence:* Understand the importance of missions and the trust customers place in them. With this in mind, strive to excel in every aspect of our business and approach every challenge with a determination to succeed.
- ✓ Compliance with the Anti-Corruption Laws (a very specific "Do What's Right)
  - Conduct every international business transaction with integrity.
  - See, e.g., Lockheed-Martin's policy on compliance with Anti-Corruption Laws.
- ✓ Corporate Public-Private Partnership Ethos
  - For instance, suppliers are an integral part of Mission Success; value their support. Partnership is a critical factor to business and customers. Expect all employees to set the standard" for ethical business conduct, and, in turn, we build relationships with suppliers who commit to integrity and share values. Want suppliers to understand, foster, and mirror the ethical conduct they expect from their employees in all business challenges and transactions.
  - Expect contractors and suppliers to conduct themselves in a manner consistent with the principles of a Code of Ethics and Business Conduct.
  - In addition, as may be required by the Federal Acquisition Regulation (FAR), strongly encourage the supply chain to have proactive and meaningful ethics programs established within their organizations.
  - Commitment not only to having a sound and robust Ethics & Business Conduct program within our organization, but committed to helping ensure that one exists throughout the supply chain as well.

Differing Cultural Overlays, Ethical Conduct, And Anti-Corruption:

Whether a uniformed service member, defense department civilian, or civilian contractor, those involved with government procurement have more challenges and responsibilities than meeting or exceeding published, domestic legal standards. The onus is on leaders of every level involved in procurement, whether in the US Government or corporate executives and other civilians to understand local customs. By doing so, they are better equipped to head off potential conflicts before they become conflicts.

This is part and parcel of what many would call "cultural astuteness." Business executive Karen Benjack Glatzer defines "cultural astuteness" as "[t]he ability to get out of your . . . comfort zone and navigate smoothly through the cultural nuances of your

specific area of responsibility." Organizational consultant Kevin Hummel asserts a critical component of "cultural astuteness" as being able to "move your goals forward in a way that is not seen as self-serving . . . through a combination of direct communication, influence, and asking other people to be your advocate or champion."

When values collide, it is important to understand the consequences of drawing the line and standing on principle. In the tradition of "seek first to understand, then to be understood," those involved in government procurement, in advancing and enhancing integrity, should ask themselves at every step of the process:

- Is there a "meeting of the minds" on requirements, the terms of reference, technical specifications or statement of work (depending on the procurement category), including an estimate of the budget, and, most importantly, the procurement lead-time?
- Is what is being called for – or being offered – legally required?
- Is what is being called for – or being offered – ethically prudent?
- Is what is being called for – or being offered – operationally sound?
- Is what is being called for – or being offered – enhancing the organizational image and reputation?

Adapted in part from:

References:

1. Ethics in Government Act of 1978 (5 U.S.C. App. § 101 et. seq.).
2. Foreign Corrupt Practices Act of 1977 (15 U.S.C. §§ 78dd-1, et seq.)
3. Procurement Integrity Act of 1988 as amended (formerly 41 U.S.C. §423, 51 U.S.C. §§ 2101-2107, implemented at FAR 3.104-4).
4. Executive Order 12674, "Principles of Ethical Conduct for Government Officers and Employees," April 12, 1989, as amended.
5. Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635 (Office of Government Ethics Rules).
6. DOD 5500.07-R, JOINT ETHICS REGULATION (JER), 30 Aug 93. Change7, effective 17 November 2011.
7. Federal Acquisition Regulation (FAR), includes amendments thru FAC 2005-69 effective September 3, 2013.
8. 10 USC § 3583 - REQUIREMENT OF EXEMPLARY CONDUCT
9. Ethical Dilemmas Across Cultures, Ceo Middle East, September 2007, 54 et seq.
10. Connie Glaser, *Doing a good job isn't enough – 'cultural astuteness' is needed to succeed*, BUS. FIRST – LOUISVILLE (July 20, 2007).
11. Stephen Covey, *Seven Habits of Highly Effective Peop*le (1989).

Seattle Journal for Social Justice

Volume 4 | Issue 1 Article 41

November 2005

Corporations and the Public Purpose: Restoring the Balance

Charlie Cray

Lee Drutman

FEDERAL CHARTERING AND NATIONAL SECURITY

It is hard to imagine an industrial sector better suited for federal chartering than the nation's defense and security contracting firms. The existence of these firms is predicated upon federal policy goals with the largest receiving major income streams through federal contracts. For example, Lockheed Martin, the Pentagon's number one primary contractor, received $21.9 billion in 2003 from the Pentagon out of its total sales of $32 billion.[169] Yet, even national defense corporations are chartered under state law and they enjoy the same weaknesses of state control that benefit other private corporations.

As private firms, the defense contractors are able to engage in lobbying, make campaign contributions to key members of Congress, and engage in other forms of influence-peddling in order to influence defense policy planning and weapons systems expenditures. Examples of private contractors defining the government's defense policy are rampant and systemic. In the recent case of Halliburton in Iraq, for example, Bunnatine Greenhouse, the senior contracting specialist with the Army Corps of Engineers blew the whistle on Halliburton's involvement in the contracting process.[170] "I can unequivocally state that the abuse related to contracts awarded to KBR represents the most blatant and improper contract abuse I

have witnessed during the [twenty year] course of my professional career [in government contracting]," said Greenhouse.[171]

The problem extends far beyond Halliburton. The growth of private military firms and corporate intelligence contractors in the past decade has created additional profitmaking pressures on national security policymaking processes.[172] Interlocking relationships exist between the largest defense contractors and the Pentagon—including corporate representation on key defense planning boards, and the regular passage of Pentagon and industry personnel through the proverbial "revolving door"—i.e., to the private sector companies that they formerly oversaw.[173] The result is a steady stream of abusive contracting practices and a potentially dangerous distortion of American national security objectives. As a *New York Times* reporter describes the situation, "Lockheed has become more than just the biggest corporate cog in what Dwight D. Eisenhower called the military-industrial complex. It is increasingly putting its stamp on the nation's military policies, too."[174]

Another result of defense contractors' influence over Congress and defense policy boards is a long-term commitment to the development of high-tech weapons systems that only specific contractors are able to produce.[175] These weapons systems arguably have little to do with preventing acts of terrorism—one of the nation's current greatest security concerns.

Two decades after President Eisenhower alerted the nation to the perils of maintaining a permanent "military-industrial complex,"[176] John Kenneth Galbraith suggested that it was time to recognize that big defense companies like General Dynamics and Lockheed, which do all but a fraction of their business with the government, are really public firms and should be nationalized.[177] "By no known definition of private enterprise can these specialized firms or subsidiaries be classified as private corporations," Galbraith wrote.[178] He noted that much of the fixed capital of these firms is owned by the government and that as a highly-concentrated

industry, the defense firms were effectively protected from competition.[179] In 1968, 10 percent of defense contracts were subject to competitive bidding and 60 percent went by negotiations to contractors which were the only source of supply.[180] There was no market between the firm and the government. Instead, members of two public bureaucracies worked out agreements for supplying weapons and other war technologies.[181]

"The process of converting the defense firms from *de facto* to *de jure* public enterprises would not be especially complicated," Galbraith suggested, outlining a transition plan for doing so: If a company or subsidiary exceeded a certain size and degree of specialization in the weapons business, its common stock would be valued at market rates well antedating the takeover, and the stock and the debt would be assumed by the Treasury in exchange for Government bonds. Stockholders would thus be protected from any loss resulting from the conversion of these firms. [182]

Galbraith proposed that the new nonprofit companies directors would could be designated by the Government.[183]

The greatest enthusiasm for Galbraith's proposal came from individuals associated with these defense firms who had witnessed fantastic waste and misuse of the nation's resources. Many liberal members of Congress, who received campaign contributions from the defense sector, opposed the idea.[184]

Converting the companies to publicly-controlled, nonprofit status would introduce a key change: it would reduce the entities' impetus for aggressive lobbying and campaign contributions. Chartering the defense contractors at the federal level would in effect allow Congress to ban such activities outright, thereby controlling an industry that is now a driving force rather than a servant of foreign policy objectives. As public firms, they would certainly continue to participate in the policy fora designed to determine the nation's national security and defense technology needs, but the profit-driven impetus to control the process in order to best serve corporate shareholders would be eliminated. Thus, by turning defense and security

firms into full public corporations, we would replace the criteria by which their performance is judged from quarterly earnings targets to criteria that is more consistent with the national interest.

LEGAL AND ETHICAL PRECEPTS GOVERNING EMERGING MILITARY TECHNOLOGIES: RESEARCH AND USE

George R. Lucas, Jr.*

From the emergence and increasing use of unmanned or remotely piloted vehicles to the advent of cyber war and conflict, the development of new and exotic military technologies has provoked fierce and divisive public debate regarding the ethical challenges posed by such technologies.[1] I have increasingly come to believe that the language of morality and ethics has served us poorly in this context and presently serves to further confuse us, rather than to clarify or enlighten us, on how best to cope with the continuing development and deployment of seemingly exotic new military technologies.

There are numerous reasons that justify this concern. Segments of the public involved in these discussions harbor distinctive and incompatible—and sometimes conceptually confused and unclear—notions of what "ethics" entail. From individual and culturally determined intuitions regarding morally right conduct, through the achievement of beneficial outcomes, all the way to equating ethics to mere legal compliance, this discord results in frequent and virtually hopeless equivocation. Moreover, many scientists and engineers (not to mention military personnel) tend to view the wider public's concern with ethics as misplaced and regard proponents of ethics as little more than technologically and scientifically illiterate, fear-mongering, nay-saying Luddites who simply wish to impede the progress of science and technology.

Why insist on invoking fear and mistrust and posing allegedly moral objections to the development and use of unmanned systems, instead of defining clear engineering design specifications and operational outcomes that incorporate the main ethical concerns? Why not require engineers and the military to design, build, and operate to these standards if they are able, and otherwise to desist until they succeed? Why engage in a science-fiction debate over the future prospects for artificial-machine intelligence that would incorporate analogues of human moral cognition when what is required is far more feasible and less exotic: machines that function reliably, safely, and fully in conformance with applicable international

 Professor of Philosophy & Public Policy, Global Public Policy Academic Group, Naval Postgraduate School; Distinguished Chair in Ethics, Stockdale Center, U.S. Naval Academy. A similar version of this Article is being published by the *Amsterdam Law Forum*.

[1] *See, e.g.*, ARMIN KRISHNAN, KILLER ROBOTS: LEGALITY AND ETHICALITY OF AUTONOMOUS WEAPONS 117–44 (2009); P.W. SINGER, WIRED FOR WAR 382–412 (2009); George R. Lucas, Jr., *Postmodern War*, 9 J. MIL. ETHICS 289, 289–98 (2010); George R. Lucas, Jr., *"This Is Not Your Father's War"—Confronting the Moral Challenges of "Unconventional" War*, 3 J. NAT'L SEC. L. & POL'Y 329 (2009).

laws—such as the law of armed conflict (LOAC)—when operating in wartime?[2] And why insist that the advent of cyber conflict is a "game changer" that ushers in a new mode of unrestricted warfare in which all the known laws and moral principles of armed conflict are rendered obsolete,[3] when what is required by this development is merely the application of appropriate analogical reasoning to determine how the known constraints extrapolate to these novel conditions?[4]

In this Essay, I propose the initial outlines of a framework for identifying and fostering productive debate over the acceptable ethical boundaries regarding novel technologies. First, I survey the state of discourse surrounding the ethics of autonomous weapon systems and cyber warfare. Next, I discuss how attempting to codify the emerging consensus on ethical boundaries for a given technology can focus the conversation on unsettled areas more effectively than vague moral discourse. Finally, I offer a set of precepts for the development and operation of autonomous systems and invite discussion on their accuracy and degree of comprehensiveness. I suggest how this methodology, and many of these precepts, applies to the regulation and governance of other military technologies as well.

I. ETHICAL DEBATE OVER NOVEL TECHNOLOGIES

Three recent and prominent threads of discussion serve to illustrate the ethical debate over the use and development of novel technologies: first, the Arkin-Sharkey debate over the proposed benefits and liabilities of "machine morality" as part of the larger, seemingly relentless drive toward developing ever-greater degrees of autonomy in lethally armed unmanned systems;[5] second, the efforts on the part of members of the International Committee on Robot Arms Control (ICRAC)—led by Peter Asaro, Robert Sparrow, and Noel Sharkey—to outlaw the future development of autonomous lethally armed unmanned systems under international law;[6] and third, the identification of areas of emerging consensus or agreement among the contending stakeholders regarding the role of ethics in cyber warfare. This third debate centers on the development of cyber weapons and tactics, both those aimed indiscriminately at civilian personnel and "objects" such as vital civil infrastructure, and highly discriminate cyber weapons like Stuxnet

---

[2] *See* George R. Lucas, Jr., *Engineering, Ethics, & Industry: The Moral Challenges of Lethal Autonomy*, *in* KILLING BY REMOTE CONTROL: THE ETHICS OF AN UNMANNED MILITARY 211, 217–21 (Bradley Jay Strawser ed., 2013).

[3] *See* Randall Dipert, *The Ethics of Cyber Warfare*, 9 J. MIL. ETHICS 384, 394–95 (2010).

[4] *See* George R. Lucas, Jr., Jus in Silico*: Moral Restrictions on the Use of Cyberwarfare*, *in* THE ROUTLEDGE HANDBOOK OF ETHICS AND WAR: JUST WAR THEORY IN THE TWENTY-FIRST CENTURY 367, 368–71 (Fritz Allhoff et al. eds., 2013).

[5] *See* Ronald C. Arkin, *The Case for Ethical Autonomy in Unmanned Systems*, 9 J. MIL. ETHICS 332, 332–34 (2010); Noel Sharkey, *Saying 'No!' to Lethal Autonomous Targeting*, 9 J. MIL. ETHICS 369, 376–81 (2010).

[6] *See Who We Are*, INT'L COMMITTEE FOR ROBOT ARMS CONTROL, http://icrac.net/who/ (last visited Oct. 13, 2013).

and Flame that may be used in a preemptive or preventive fashion against perceived threats that have resulted in no actual harm, as yet, inflicted by the recipient of the cyber attack.[7]

These three examples do not exhaust all of the features of the wider debate over emerging military technologies, by any means. The increasing array of so-called nonlethal weapons, for example, involves questions about the use of such weapons on noncombatants and the potential of such weapons to expand the rules of engagement for use of force, rather than lessening the destruction or loss of life as compared to the current regime.[8] Prospects for military uses of nanotechnology raise specters of weapons and systems that might cause widespread and catastrophic collateral or environmental destruction.[9] And efforts to use biological, neurological, and pharmaceutical techniques to enhance the capabilities of human combatants themselves raise a host of ethical questions. Such questions range from topics like informed consent for the use of these techniques, to the likely long-term health prospects for enhanced individuals following their military service, to the potentially undesirable social conflicts and transformations (i.e., "civilian blowback") that such techniques might inadvertently bring about.[10] For the present, however, I will stick to the three illustrations above because they collectively encompass a great deal of the public debate over military technology, and the lessons learned in response have a wider applicability to these other areas and topics as well.

First, the prospects for machine models of moral cognition constitute a fascinating, but as yet futuristic and highly speculative enterprise. The goal of

---

[7] *See* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 188–209 (2012) (providing a retrospective account of the "Olympic Games" project to deploy the Stuxnet worm against Iranian nuclear facilities); George R. Lucas, Jr., *Permissible Preventive Cyber Warfare*, *in* THE ETHICS OF INFORMATION WARFARE (Luciano Floridi & Mariarosaria Taddeo eds., forthcoming 2013) (giving a preliminary summary of the discovery and strategic implications of the Stuxnet worm against the backdrop of three prior conflicts in Estonia, Syria, and Georgia in 2007 and 2008).

[8] *See, e.g.*, Paula Kaurin, *With Fear and Trembling: An Ethical Framework for Nonlethal Weapons*, 9 J. MIL. ETHICS 100, 100–02 (2010).

[9] *See, e.g.*, James J. Hughes, *Global Technology Regulation and Potentially Apocalyptic Technological Threats*, *in* NANOETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF NANOTECHNOLOGY 201, 201–04 (Fritz Allhoff et al. eds., 2007) (discussing the environmental threat of "grey goo" or unrestrained self-replicating nanotechnologies); Ray Kurzweil, *On the National Agenda: U.S. Congressional Testimony on the Societal Implications of Nanotechnology*, *in* NANOETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF NANOTECHNOLOGY, *supra*, at 40, 44–47 (providing examples of true nanotechnology such as the military's development of "smart dust," which consists of millions of nanodevices dropped on enemy territory to provide detailed surveillance).

[10] See PATRICK LIN ET AL., ENHANCED WARFIGHTERS: RISK, ETHICS AND POLICY 11–27, 66–76 (2013), *available at* http://ethics.calpoly.edu/Greenwall_report.pdf (providing an account of enhancement technologies and their prospective military uses and potential abuses).

developing working computational models of reasoning, including moral reasoning, is hardly impossible, but the effort required will be formidable.[11] "Morality" and moral deliberation remain firmly in the domain of human experience for the foreseeable future. In any event, discussions of ethics and morality pertaining to unmanned systems at present are largely irrelevant. We neither want nor need our unmanned systems to be ethical, let alone more ethical or more humane than human agents. We merely need them to be safe and reliable, to fulfill their programmable purposes without error or accident, and to have that programming designed to conform to relevant international law (such as the LOAC) and specific rules of engagement (ROEs). With regard to legal compliance, machines should be able to pass what is defined below as the modified "Arkin test": autonomous unmanned systems must be demonstrably capable of meeting or exceeding behavioral benchmarks set by human agents performing similar tasks under similar circumstances.[12]

Second, proposals at this juncture to outlaw research, development, design, and manufacturing of autonomous weapons systems seem at once premature, ill timed, and ill informed—classic examples of poor governance. Such proposals do not reflect the concerns of the majority of stakeholders who would be affected; they misstate, and would attempt to overregulate relevant behaviors.[13] Ultimately,

---

[11] The degree of futuristic speculation involved in such efforts is indicated in the Arkin-Sharkey debate. *See* Arkin, *supra* note 5; Sharkey, *supra* note 5; *see also* RONALD ARKIN, GOVERNING LETHAL BEHAVIOR IN AUTONOMOUS ROBOTS 93–113 (2009) (giving a proponent's account of the formidable challenges entailed in such efforts); Ronald Craig Arkin et al., *Moral Decision Making in Autonomous Systems: Enforcement, Moral Emotions, Dignity, Trust, and Deception*, 100 PROC. IEEE 571, 572–86 (2012) (providing an account of the progress on such efforts to date).

[12] This criterion—that robots comply as, or more, effectively with applicable constraints of LOAC on their use of force and doing of harm than human combatants under similar circumstances—constitutes what I have termed the "Arkin Test" for robot "morality" (although that is likewise somewhat misleading, as the criterion pertains straightforwardly to compliance with international law, not with the exhibiting of moral judgment). In this sense, the test for "morality" (i.e., for the limited ability to comply with legal restrictions on the use of force) is similar to the "Turing Test" for machine intelligence: we have satisfied the demand when machine behavior is indistinguishable from (let alone better than) human behavior in any given context. *See* George. R. Lucas, Jr., *Industrial Challenges of Military Robotics*, 10 J. MIL. ETHICS 274, 281 (2011); *see also* Robert Sparrow, *Building a Better Warbot: Ethical Issues in the Design of Unmanned Systems for Military Applications*, 15 SCI. & ENGINEERING ETHICS 169, 177–78 (2009) (explaining the need to design systems capable of complying with LOAC).

[13] In addition to proposals to outlaw armed or autonomous military robotic systems by ICRAC itself, a recent report from Human Rights Watch makes similar recommendations. *See* HUMAN RIGHTS WATCH, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS 5 (2012), *available at* http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0.pdf. While unquestionably well intentioned, the report is often poorly or incompletely informed regarding technical details and highly misleading in many of its observations. Furthermore, its proposal for States to collaborate in banning the further development and use of such technologies would not only prove unenforceable but likely would impede

such regulatory statutes would prove unacceptable to, and unenforceable against, many of the relevant parties (especially among nations or organizations with little current regard for international law), and would thus serve merely to undermine respect for the rule of law in international relations. Machines themselves (lacking the requisite features of folk psychology, such as beliefs, intentions, and desires) by definition cannot themselves commit war crimes, nor could a machine be held accountable for its actions. Instead, a regulatory and criminal regime, respecting relative legal jurisdictions, already exists to hold accountable individuals and organizations that might engage in reckless or criminally negligent behavior in the design, manufacture, and ultimate use of unmanned systems of any sort.[14]

Lastly, in contrast to robotics, which has spawned tremendous ethical debate but little in the way of jurisprudence, discussions of the cyber domain have been carried out almost entirely within the jurisdiction of international law,[15] with very sparse comment from ethicists until quite recently.[16] Some have found the threat of a grave "cyber Armageddon"—of the sort predicted by Clarke and Brenner[17]—somewhat exaggerated. These commentators have even denied that the genuine equivalent of armed conflict has or could likely occur within this domain: no one has yet been killed, nor have objects been harmed or destroyed, in a cyber conflict.[18] What has transpired instead is an increase in "low-intensity" conflict, such as crime, espionage, and sabotage, which blurs the line between such conflict and war and results in cumulative harm greater or more concrete than damage

---

other kinds of developments in robotics (such as the use of autonomous systems during natural disasters and humanitarian crises) that the authors themselves would not mean to prohibit. It is in such senses that these sorts of proposals represent poor governance.

[14] Gary E. Marchant et al., *International Governance of Autonomous Military Robots*, 12 COLUM. SCI. & TECH. L. REV. 272, 300–05 (2011).

[15] *See* MICHAEL SCHMIDT ET AL., THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 15–41 (2012), *available at* https://www.ccdcoe.org/249.html; *see also* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 98–100 (2010) (summarizing the applicability of the existing laws of war to cyber warfare); Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARVARD INT'L L.J. ONLINE 13, 15–18 (2012), http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (discussing the applicability of international law to cyberspace). Cyber conflict and international law is also a topic of a special issue of the U.S. Naval War College's journal, *International Law Studies*. *See* Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger, *Preface* to 87 INT'L L. STUD. xxiii, xxiv–xxvi (2011).

[16] Randall Dipert authored the first article by an ethicist to address cyber warfare. Dipert, *supra* note 3, at 394–95. Computer scientist Neil C. Rowe had earlier raised moral concerns about cyber weapons and strategy. *See id.* at 394.

[17] JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 137–47 (2011); RICHARD A. CLARK & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 64–68 (2010).

[18] Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 10–15 (2011).

caused by conventional war.[19] However, several recent conflicts, at least one of which (Stuxnet) did cross the boundary defining an act of war, [20] have suggested the emergence of increasingly shared norms by which such conflict can be assessed, and perhaps constrained.

II. CODIFICATION OF EMERGENT NORMS

The final comment above illustrates an approach to understanding and governing the future development and use of exotic military technologies first suggested by Professor Gary Marchant et al.—namely, that rather than a rush toward proposing unenforceable treaties or ineffectual bright-line statutes of black-letter international law, what is required is a form of governance known as soft law.[21] Professor Marchant and his co-authors invited those engaged in the development and use of such technologies, in the course of their activities, to reflect upon and observe what appear to them to be the boundaries of acceptable and unacceptable conduct and to codify these boundaries by consensus and agreement as the principles of best practice in their fields.

In many of the areas outlined above, emergent norms regarding ethics, legal jurisdiction and compliance, and perhaps most importantly, appropriate degrees of consent and accountability for all the stakeholders—that together constitute the hallmarks of good governance—have already been largely established. What is urgently needed at this juncture is a clear summary of the results of the discussions and debates (such as those surveyed above) that would, in turn, codify what we seem to have proposed or agreed upon in these matters, as distinguished from what requires still further deliberation and attention.

In the case of the debate over autonomous systems, for example, I would summarize the past several years of contentious debate in the following precepts, which define good or best practices and address the limits of acceptable versus unacceptable practices. I have already undertaken this task in the realm of cyber conflict[22] due to the reactions to several internationally acknowledged examples of

---

[19] John Arquilla, *Cyber War is Already Upon Us*, FOREIGN POL'Y, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us (last visited Mar. 5, 2013); Thomas Rid, *Think Again: Cyberwar*, FOREIGN POL'Y, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar (last visited Mar. 5, 2013).

[20] *See* SANGER, *supra* note 7, at 188–209; Lucas, *supra* note 7.

[21] Marchant et al., *supra* note 14, at 306–14.

[22] *See* Lucas, *supra* note 4 at 367–75. There I summarize from extant literature that the use of a cyber weapon against an adversary is justified whenever there is a compelling reason for doing so, when every reasonable effort toward resolution has been expended with little likelihood of success, and when further delay will only make matters even worse. *See id.* at 372–73. Resort to cyber conflict is only justified, moreover, when the weapon is directed purely at military targets, the attack would inflict no more damage or loss of life than is reasonably proportionate to the threat posed, and finally, every effort is made to avoid or minimize harm to noncombatant lives or property. *Id.* In other respects, as noted below, these precepts of cyber conflict are similar to, or can be straightforwardly derived

cyber conflict that have recently occurred, from Estonia in 2007 to Stuxnet/Operation Olympic Flame in 2010.[23] The point of these exercises is not to presume or preempt proper legislative authority, but instead to focus future discussions upon whether such precepts are correctly stated (and if not, to modify them accordingly), the extent to which they are in fact widely held, and finally, to identify areas of omission that must still be addressed. This seems to me a far more constructive enterprise at this point than further futile hand-wringing over the ambiguities of moral discourse.

III. PRECEPTS FOR USE OF AUTONOMOUS SYSTEMS

Law and moral discourse, famously, always lag behind technological innovations—especially, if not exclusively, in warfare—and the innovations' transformative impact on the cultures in which they arise. That does not mean that law and morality are irrelevant and must be cast aside; neither does it require that ethics always be portrayed as an impediment or obstacle to technological development. Rather it demands, as such developments always have, that human agents employ appropriate ingenuity in the framing of suitable metaphors, the drawing of the most appropriate analogies, and reasoning by extrapolation from the known to the unknown in the continuing quest to order and organize the perplexing opportunities and risks that innovation and change otherwise invariably pose. In that spirit, I offer these precepts as the emerging consensus on the use of autonomous weapons systems.

Precept #1: The Principle of Mission Legality

A military mission that has been deemed legally permissible and morally justifiable on all other relevant grounds does not lose this status solely on the basis of a modification or change in the technological means used to carry it out (i.e., by removing the pilot from the cockpit of the airframe or replacing the pilot with demonstrably reliable software). However, this does not hold true if the technology in question represents or employs weapons or methods that are already specifically proscribed under existing international weapons conventions, is in violation of the prohibitions in international humanitarian law against means or methods that inflict superfluous injury or unnecessary suffering, or is otherwise judged to constitute means *mala in se* (i.e., evil in themselves).[24]

---

from, several of the precepts regarding the development and use of unmanned systems discussed in this Article.

[23] *See supra* note 7.

[24] Wendell Wallach of Yale University, a well-respected ethicist, has recently proposed that lethal autonomous systems, at least, should—like rape and biological weapons—be classified among the means and methods of warfare that are *mala in se*. *See* Wendall Wallach, *Terminating the Terminator: What to Do About Autonomous Weapons*, SCI. PROGRESS (Jan. 29, 2013), http://scienceprogress.org/2013/01/terminating-the-termina tor-what-to-do-about-autonomous-weapons. This position would render the argument

Precept #2: The Principle of Unnecessary Risk[25]

Within the context of an otherwise lawful and morally justified international armed conflict or domestic security operation, we owe the war-fighters or domestic security agents every possible minimization of risk we can provide them in the course of carrying out their otherwise legally permissible and morally justifiable missions.

Precept #3: The Principle of the Moral Asymmetry of Adversaries[26]

By contrast, no such obligation is owed to opponents or adversaries during such missions in their pursuit of presumably illegal and morally unjustifiable activities. That is, there is no requirement of fairness or technological equality in carrying out justified international armed conflict or lawful domestic security operations. NATO/ISAF forces no longer owe combat parity or fairness to Taliban and al-Qaeda operatives than domestic immigration and border security forces owe such parity to armed agents of drug cartels. Both sets of adversaries are engaged in virtually identical behavior: violation of domestic legal statutes and defiance of duly elected legal authorities, indiscriminate targeting of civilians and destruction of property, kidnapping, torture, execution, mutilation of prisoners, and so on.

Precept #4: The Principle of Greatest Proportional Compliance

Furthermore, in the pursuit of a legally permissible and morally justifiable military or security mission, agents are obligated to use the means or methods

---

regarding mission legality with respect to the use of such technology moot. It is not at all clear, however, that the reasons adduced for this classification are compelling in the case of unmanned systems generally. Not only does the analogy between autonomous systems and the examples of means *mala in se* given above not appear obvious, but Wallach's argument also rests on the largely discredited objection that machines cannot be held accountable for their actions.

[25] Bradley Jay Strawser, *Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles*, 9 J. MIL. ETHICS 342, 343–49 (2010).

[26] Note that this is not an explicit rejection of the doctrine of the "Moral Equality of Combatants," an essential element in what Michael Walzer defines as "the War Convention." *See* MICHAL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 34–37, 44–46 (1977). Rather, it is a repudiation of a misplaced notion of fairness in combat, according to which it would be unfair for one side in a conflict to possess or use weapons or military technologies that afforded them undue advantage. This is sometimes cited in public as an objection to the use of drones in warfare. It seems to equate war with a sporting competition, after the fashion of medieval jousting, and upon examination, is not only patently ridiculous, but contradicted in most actual armed conflicts of the past where maneuvering for technological superiority was a key element in success. In any case, no such argument is made concerning legitimate domestic security operations, as noted above, and does not obtain either within the realm of wars of law enforcement or humanitarian intervention.

available that promise the closest compliance with the international LOAC and applicable ROEs, such as noncombatant distinction (i.e., discrimination) and the economy of force (i.e., proportionality).

Precept #5: The Modified "Arkin Test"[27]

In keeping with Precept 4, an artifact (such as an autonomous unmanned system) satisfies the requirements of international law and morality pertaining to armed conflict or law enforcement and may therefore be lawfully used alongside or substituted for human agents whenever the artifact can be shown to comply with the relevant laws and ROEs as (or even more) reliably and consistently as human agents under similar circumstances. Moreover, from application of Precepts 2 and 4 above, the use of such an artifact is not merely legally permissible but *morally required* whenever its performance promises both reduced risk to human agents and enhanced compliance with LOAC and ROEs.

Precept #6: The Principle of Nondelegation of Authority and Accountability[28]

The decision to attack an enemy (whether combatants or other targets) with lethal force may not be delegated solely to an unmanned system in the absence of human oversight, nor may eventual accountability for carrying out such an attack be abrogated by human operators in the "kill chain."

Precept #7: The Principle of Due Care

All research and development, design, and manufacturing of artifacts such as lethally armed or autonomous unmanned systems that are ultimately intended for use alongside, or in place of, human agents engaged in legally permissible and morally justifiable armed conflict or domestic security operations must rigorously comply with Precepts 1–5 above. All R&D, design, and manufacturing of unmanned systems undertaken with full knowledge of, and in good faith compliance with, the above precepts (with such good faith at minimum to encompass rigorous testing to ensure safe and reliable operation under the terms of these precepts) shall be understood as legally permissible and morally justifiable.

Precept #8: The Principle of Product Liability

Mistakes, errors, or malfunctions that nonetheless might reasonably and randomly be expected to occur, despite the full and good faith exercise of due care as defined in Precept 6 above, shall be accountable under applicable international or domestic product liability law. Such accountability shall include full and fair

[27] *See* Arkin, *supra* note 5, at 332–34.

[28] This principle is indebted to the work of philosopher Robert Asaro of the New School in New York City, cofounder of ICRAC.

financial and other compensation or restitution for wrongful injury, death, or destruction of property.

Precept #9: The Principle of Criminal Negligence

By contrast, R&D, design, or manufacturing of systems undertaken through culpable ignorance or in deliberate or willful disregard of these precepts (including failure to perform or attempts to falsify the results, tests regarding safety, reliability of operation, or compliance with applicable law and ROEs, especially in the aftermath of malfunctions as noted above) shall be subject to designation as war crimes under international law, or as reckless endangerment or criminally negligent behavior under the terms of applicable international or domestic law. Individual parties to such negligence shall be punished to the full extent of the law, to include trial and conviction in the International Criminal Court for the willful commission of war crimes or civil and criminal prosecution within the appropriate domestic jurisdiction for reckless endangerment or criminal negligence. In domestic jurisdictions providing for capital punishment upon conviction for the occurrence of such mishaps within that jurisdiction, such punishment shall be deemed an appropriate form of accountability under the precepts above.

Precept #10: Benchmarking

Testing for safety and reliability of operation under the relevant precepts above shall require advance determination of relevant quantitative benchmarks for human performance under the conditions of anticipated use and shall require any artifact produced or manufactured to meet or exceed these benchmarks.

Precept #11: Orientation and Legal Compliance

All individuals and organizations (including military services, industries, and research laboratories) engaged in R&D, design, manufacturing, acquisition, or use of unmanned systems for military purposes shall be required to attend an orientation and legal compliance seminar of not less than eight hours on these precepts, and upon its conclusion, to receive, sign, and duly file with appropriate authorities a copy of these precepts as a precondition of their continued work. Failure to comply shall render such individuals liable under the principle of criminal liability (Precept 9) above for any phase of their work, including but not limited to, accidents or malfunctions resulting in injury, death, or destruction of property.

Government and military agencies involved in contracting for the design and acquisition of such systems shall likewise require and sponsor this orientation seminar and facilitate the deposit of the required signed precept form by any contractors or contracting organizations receiving federal financial support for their activities. Federal acquisitions and procurement officials shall also receive this training and shall be obligated to include the relevant safety/reliability

benchmarks of human performance along with other technical design specifications established in RFPs or federal contracts.[29]

IV. CONCLUSION

My intent in offering these precepts is to suggest areas of consensus and agreement discerned among contending stakeholders and positions in this debate, and to suggest the norms emerging from this debate that might serve to guide (if not strictly govern) the behavior of states, militaries, and those involved in the development, testing, and manufacture of present and future unmanned systems. I likewise believe that discussion of the meaning, application, and refinement of these precepts as soft-law guidelines for proper use of unmanned systems would be substantially more efficacious than further moral hand-wringing over their potential risks, let alone rushing to legislation that would have both unenforceable and unintended harmful consequences.

Some of the foregoing precepts are specific to military robotics (e.g., Precepts 5 & 6, pertaining to the Arkin test and prohibition on delegation of authority to unmanned systems, respectively). This general approach, based upon mutual consensus regarding emerging norms and many, if not most, of the precepts elicited above, however, would prove useful by analogy as well in other areas of technological development, such as nonlethal weapons, cyber warfare, projects for "warrior enhancement," and other military or domestic security technologies.

In the case of cyber conflict, for example, Precept 1 pertaining to mission legality would likewise suggest that, in any situation in which a use of force was otherwise deemed justifiable, that justification would extend to the use of cyber weapons and tactics as well as to conventional weapons and tactics. Moreover, by the Principle of Greatest Proportional Compliance (Precept 4 above), in an instance in which the use of force was otherwise justifiable, given a choice of cyber versus conventional weaponry, the use of the more discriminate and less destructive weapon (presumably the cyber weapon) would not merely be permitted, but obligatory. This principle also dictates the use of less-lethal (or nonlethal) weaponry, when the effects otherwise achieved are equivalent.

In sum, I believe there is far more consensus among adversarial parties arguing about ethics and law in such matters than we have heretofore been able to discern. That emerging consensus, in turn, points toward a more productive regime of governance and regulation to ensure against the risk of unintended harm and consequences than do rival attempts at legal regulation or moral condemnation.

[29] A similar set of procedures (i.e., Precepts 10 and 11) is recommended for analogous programs involving cyber weapons and tactics, nonlethal weapons, and human enhancement projects (the last already to include compliance with relevant federal requirements regarding research on human subjects).

Ethical Issues in the Global Arms Industry: A Role for Engineers

Ethical Dilemmas in the Global Defense Industry Conference
University of Pennsylvania Law School
Philadelphia, April 16, 2015

This paper has four parts. The first two seek to clarify the subject of this conference, ethical issues in the global arms industry. The third sketches the role engineers have in much of the global arms industry. The last part considers one way that engineers might help with resolving some of the industry's ethical issues. While the first part of this paper should contain few surprises, the last three will, I hope, contain more.

1. Dilemmas and Defense

Let me begin with two differences between the official title of this conference and the title of my paper. First, I have substituted "issues" for "dilemmas". Second, I have substituted "arms" for "defense". The purpose of these changes is to avoid unnecessary disputes rather than to change the subject of the conference. Let me explain.

A "dilemma" is a situation in which a difficult choice has to be made between two (or more) equally undesirable alternatives.[1] If the alternatives were not *equally* undesirable, the choice would be easy: choose the more desirable alternative. There would be no dilemma (though the choice might, like most good choices, have its cost). My impression is that the main ethical issues, questions, problems, or quandaries posed by the global arms industry are not dilemmas (in this sense) but complex situations in which most of the choices on offer are hard to assess and many of the best choices have yet to be devised. Indeed, many of the issues, questions, problems, or quandaries are so ill-defined that we cannot say what a good choice would look like. We are dealing with a subject requiring the work philosophers typically do. We must understand the issues before we can have anything so tidy as a dilemma. Hence, my substitution of "issue" for "dilemma". I might have used "problem", "question", "quandary", or some other catch-all instead of "issue".

My substitution of “arms” for “defense” has a different rationale. I regard “defense” in such terms as “Defense Department”, “defense forces”, and “defensive weapons”, as a misleading euphemism. The “Defense Department” is the department of the American government that oversees war-making, offensive as well as defensive. In most countries that call their military “Defense Forces”, the military still consists of an army, air force, navy, and so on, all of which can, and sometimes do, engage in offensive warfare. Much the same is true of weapons. Few, if any, are purely defensive. Even a shield, that epitome of defense, can be used offensively, for example, to strike an opponent too focused on one’s sword arm. Rather than try to sort out whether a particular piece of equipment, say, an anti-aircraft missile or landmine, is an offensive or defensive weapon (or both), I have substituted “arms” for “defense”.

By “arms industry”, I mean all those organizations, whether commercial or not, that design, build, sell, or service weapons or related equipment for military use, provide military research, training, or advice, or otherwise aid the military. The military is that technological system—a combination of people and things—the purpose of which is to kill on a large scale. Though the military is typically an arm of government, it can also be an arm of non-governmental agencies, such as a business corporation (“private army”) or religious organization (the Knights Templar or the warrior monks of ancient Japan).

“Arms industry” (as used here) does not include the design, construction, sale, or servicing of weapons for non-military use, whether use by police, hobbyists, or civilians intent on self-defense or mayhem, even if the non-military weapon is indistinguishable from its military counterpart and manufactured in the same factory. So, while the manufacturer of ordinary bandages or backpackers’ dinners is not, as such, part of the arms industry, the manufacturer of field dressings or combat rations is. Products of the arms industry include aircraft, artillery, ammunition, electronic systems, light weapons, operations support, software, research, and uniforms.

While much of the arms industry is “domestic”, that is, serves the “home country”, a significant part is “international” or “global”, that is, serves the military of other countries, rebellions outside the home country, or other foreign military forces. Our subject is the *global* arms industry, that is, that part of the arms industry that is not domestic.[2]

The distinction between the global arms industry and domestic is, of course, artificial in at least two respects. First, much of the domestic arms industry seeks foreign customers if they

have a product they can sell abroad (and permission of their home government to sell it abroad). Foreign sales can reduce the unit cost of a product, help tie foreign customers to the home country, and otherwise serve domestic interests. Much of the global arms industry is, in this respect, also part of the domestic arms industry.

Second, much of what even a strictly domestic arms industry produces depends on raw materials, research, or subsystems produced outside the home country. Even a domestic arms industry must rely on international trade to provide much of what the military of the home country needs, everything from iron or rubber to computer chips or Kevlar. Much of the domestic arms industry is global in this respect—and has been for at least a century.

The distinction between the global arms industry and the domestic is nonetheless worth making. The patriotism that may justify producing arms for one's own country cannot justify producing arms for others, especially those not allied with the home country. The ethical issues of the global arms industry seem to differ in systematic ways from those of the domestic arms industry.

We must now turn to the ethical issues of the global arms industry.

2. Ethical issues

"Ethics" has at least three uses potentially relevant here. First, it can be a synonym for ordinary morality, those standards of conduct that apply to all moral agents simply because they are moral agents—"Don't kill", "Keep your promises", "Help the needy", and so on. Second, "ethics" can refer to those morally binding standards that apply to members of a group simply because they are members of that group. Legal ethics applies to lawyers and no one else; business ethics to people in business and no one else; and so on. Third, "ethics" can refer to a field of philosophy, that is, the attempt to understand morality (including its special standards) as part of a reasonable undertaking. Other names for "ethics" in this third sense include "moral theory" and "ethical theory". I shall hereafter reserve "ethics" for the special-standards sense, using "morality" for the first sense and "moral theory" for the third.

Given this terminology, some "ethical issues" identified in the call for our conference seem in part moral (whether or not they are also ethical, that is, whether or not they concern an

existing special standard or might lead to the adoption of such a standard). For example, the threat drones pose to people's privacy is a moral issue.[3] Every moral agent, even the agents of the global arms industry, should, all else equal, avoid contributing to the invasion of people's privacy. Other issues, such as what to do about "government officials [who] expect some form of quid pro quo for their cooperation", though ethical issues for most of the global arms industry, are no longer difficult issues. Most of the global arms industry have long since adopted a special standard resolving them. So, for example, the National Defense Industrial Association's "Statement of Defense Industry Ethics" says that:

> When contemplating any international sale to a governmental or quasi-governmental buyer, it is imperative that effective measures be undertaken to ensure full compliance, not only with the letter, but also the spirit of the Foreign Corrupt Practices Act, as amended, and the FCPA's bar against improper payments to foreign officials.[4]

Of course, we can debate whether such special standards are wise, morally required, merely morally permitted, or even morally wrong. But that debate is likely to do little more that return us to ground that business ethics (the philosophical study) has worked over pretty well during the last forty years.[5] I therefore propose to limit this paper to moral issues that the global arms industry faces while ordinary businesses do not (or , at least, do not face in the same way), issues not much discussed in business ethics.[6] I have identified six. No doubt there are others.

1. Weapons versus non-weapons. Much of what the global arms industry sells are weapons (artefacts designed to kill, wound, disable, or destroy) but much is not. For example, much of what the global arms industry sells consists of clothing, field kitchens, tents, and so on, artefacts harmless in themselves even in military service. And some of what the global arms industry sells is neither clearly a weapon nor clearly not a weapon, for example, body armor, observation drones, communications equipment, circuit boards, reflective paint, software, and other non-lethal elements of a "weapons system". How morally significant, then, is the distinction between weapons and non-weapons? Should the global arms industry consider the sale of non-weapons less morally objectionable than the sale of weapons or non-lethal elements of a weapons system? After all, every artefact embedded in the technological system we call "the military" is there to help the military do its job, which is (in part at least) to kill other human beings on a large scale, a morally dubious undertaking, especially if the regime directing the

military is itself morally dubious. (A morally dubious undertaking can, of course, turn out, all things considered, to be morally justified, but the burden of proof must fall on those claiming justification.)

2. Morally dubious regimes. Some customers of the global arms industry respect human rights but most, to varying degrees, do not. Of those that do not, some may simply deny their people certain basic rights, such as self-government or decent medical care, but many actively harm those under their control by, for example, imprisoning, torturing, or killing them for political, religious, or other beliefs, for forming various kinds of peaceful voluntary associations, or for speaking a certain language, dressing in a certain way, or the like. How abusive must a regime be before the global arms industry should refuse to sell it weapons. How abusive before the global arms industry should have no dealings with it at all? How important is the argument that if "we" do not sell to them, others will?

3. Cultural differences. By "culture", I mean a distinctive way of doing something, including the beliefs and evaluations that accompany the doing. So, for example, eating with knife, fork, and spoon is a gastronomic culture (a distinctive way to eat) while eating as such is not (since everyone eats). There are military cultures. For example, some militaries "live off the land" on which they fight, while others routinely bring all their supplies with them. Some routinely take prisoners; some do not. Some militaries force young men to serve while others take only volunteers. Some allow "children" (adolescents under 18) to be soldiers; some do not. How important should such cultural differences be to the global arms industry when deciding whether to take on a certain customer? Should international standards preempt non-complying military cultures?

4. Lawful artefacts having illegal uses. Most weapons have illegal uses as well as legal ones. For example, the same rifle that is legally used to kill a soldier in combat can be used illegally to kill enemy soldiers who have surrendered. Something similar is true of many non-weapons. For example, the same small electric generator that can lawfully be used to power field radar can be used illegally to deliver electric shocks to a prisoner's genitals. How important should the likelihood of illegal use of military equipment be to the decision to sell the equipment to a certain customer? Should military equipment be designed, as much as possible, to prevent illegal use?

5. Weapons likely to fall into the wrong hands. Much of what the arms industry sells can be stolen, resold, transferred to another by capture, or otherwise "diverted". How much responsibility should the global arms industry take for preventing its products falling into the wrong hands? For example, should the global arms industry refuse to sell to unstable regimes (a regime likely to lose control of its military soon) or regimes (such as the current regime in Iraq) with a record of losing many of its weapons to its non-state enemies? Should the products of the global arms industry be designed to make diversion of its products more difficult or less attractive (for example, by making rifles requiring unusual bullets or hard to replace parts)?

6. Relatively indiscriminate weapons. Some weapons are relatively indiscriminate, even when used by a sophisticated military. For example, landmines can as easily be set off by a civilian as by a soldier and even the US military can fail to retrieve all its mines when it departs. Landmines may go on killing and maiming civilians for decades after the end of the war justifying their use. Something similar is true of conventional bombs. Lost "duds" can explode long after the end of hostilities, killing anyone who happens to be nearby. While some weapons are relatively indiscriminate even in sophisticated hands, some are indiscriminate only in unsophisticated hands. For example, without good record keeping, a military may lose track of the age of artillery shells. Past-date shells may explode when they should not, say, when being transported on a rough road or even when being loaded into a naval gun. How much care should the global arms industry take to make weapons as discriminating as practical in the circumstances in which they are likely to be used?

The classic indiscriminate weapons are, of course, nuclear bombs, biological devices, and deadly gases, weapons that, I believe, are not currently part of the official global arms trade. I shall therefore ignore them here.[7]

3. Engineers in the global arms industry

Engineers have had a significant role in the arms industry since at least the 1700s. Their role has only increased as the products of the arms industry have become more sophisticated. Today one in ten US engineers works in military-related industry, including about 39,000 electrical engineers (just under 14% of all US electrical engineers) and about 6,000 aerospace engineers (just under 19% of all aerospace engineers).[8] Engineers design weapons and other

equipment the military needs, test them, sell them, and oversee their manufacture, maintenance, and even disposal. Indeed, it is hard to imagine today's arms industry without engineers, not only "bench engineers" but technical managers up to, and often including, senior management.[9] So, for example, of Lockheed Martin's eight vice presidents, three are engineers.[10] There is no reason to think that engineers do not have a similar part with respect to most products of the global arms industry or, at least, most of its most distinctive products.

Suppose, for example, that a certain large African country contacts a US manufacturer of modern jet fighters in order to buy twenty for its air force. The sale is likely to be a long process, lasting months or even years. At an early stage, the US manufacturer would have to send out engineers to assess the African country's airbases, maintenance practices, pilot training, local suppliers, and so on. A jet fighter requires a complex technological system to operate. The would-be customer may be surprised to learn that its runways are too short, that its fuel storage is inadequate, that its maintenance staff will have to be larger, better trained, and provided with more sophisticated tools, and so on. While some of this information is typically public, some is not, being proprietary or classified. Much of it will, in any case, be in a form engineers are used to and others are not. The African country will need its own engineers to talk to those of the US manufacturer.

The African country need not agree to all the requirements that the US manufacturer seeks to impose as part of the sale. It may suggest changes in the design of the jet fighters so that, for example, they can use fuel that the African country is already using for other aircraft. Indeed, after a full assessment, the parties may agree on a less sophisticated fighter. In any case, the final specifications for the fighter, including training, support, munitions, replacement parts, and so on, should be the result (in part) of extensive negotiations between the engineers of the US manufacturer and those of the African country.[11] Though the terms of such a sale are, in principle, entirely under the control of the US manufacturer's senior management and the African country's senior government officials, in practice many of the decisions, perhaps most, will be made by engineers, some quite junior, no one else having the information, time, and skills to appreciate their import.

The involvement of engineers typically does not end with the writing of specifications or even with the signing of the sales contract. Engineers will oversee the manufacture of the planes, not only making sure that every part satisfies the specifications and the whole is constructed

properly but also changing the specifications if, say, there is difficulty getting a specified part or a better part has become available. Given that there will typically be several years between the initial writing of specifications and the delivery of the last jet fighter, there may be many changes in the specifications, most quietly made by agreement among engineers. Some of these changes will, of course, be “no brainers”, but a substantial number may involve painful balancing of cost, reliability, timeliness, and so on. So, for example, a new part may be cheaper and, based on experience, as good as the old. But, since the part is new, experience with it must be short. The part may fail long before it should. Who knows? The engineers will have to rely on experience with parts analogous in one way or another to forecast the probable failure date of the new part—and decide accordingly. There may be a good deal of discussion between the manufacturer’s engineers and those of the African country.

The relationship between the engineers of the US manufacturer and those of the African country should not end when the last fighter is delivered. The US engineers should keep the African engineers informed of problems identified in similar aircraft elsewhere in the world and the solutions devised. The African engineers in turn should advise the US engineers of any problems they identify in the jets they purchased, anything from unusual wear on engine blades to difficulty getting ground crews to comply with required maintenance procedures. The purpose of this exchange of technical information between the manufacturer’s engineers and those of the African country is not simply to maintain the fighters; it is in part to improve them where possible, not only the fighters that the African country has purchased but other fighters in that family, both those yet to be built and those already in use elsewhere in the world. In principle, this exchange of information should continue until the last fighter delivered has ceased to exist. That is normal engineering.

While much of this exchange of information will go on long-distance, some of it may require “site visits”, for example, to see the troublesome dust clouds possibly contributing to unusual engine wear or the conditions under which maintenance must actually be performed.

The relationship between a manufacturer’s engineers and those of a customer can be both intimate and enduring. There is often a tension between the legal department’s “arm’s length” conception of how information should be shared and the engineers’ conception (something more like a long hug than a handshake). For example, engineers of a manufacturer can seldom do a good job of designing a sophisticated piece of equipment without knowing how it will be used,

under what conditions, and for how long. Similarly, a customer purchasing such equipment cannot be as helpful in its design as it could be unless it knows the details of manufacture, including some trade secrets and (in the case of a fighter jet) even some highly classified information.

4. How engineers might help resolve some ethical issues

Most engineers working in the global arms industry are civilians. Most who are not have nonetheless been trained in the same way as civilian engineers, work in much the same way as civilian engineers, and have little trouble communicating with civilian engineers. Engineering is (in this respect at least) a single profession. It is also a global profession. Engineers in Brazil, China, Nigeria, or India are trained much as are engineers in Germany, Japan, or the US. Engineers also share certain standards, whether formalized in a code of ethics or not. They are committed not simply to maintaining technology but to improving it for the benefit of humanity. Their first loyalty is (or, at least, is supposed to be) not to their employer but to "the public health, safety, and welfare".[12]

Much of what engineers share are technical standards. Some of these are governmental, such as the standards of safety issued by the Environmental Protection Agency or the Nuclear Regulatory Commission. But many technical standards, perhaps most, are not the work of government. Of these, some are the work of professional associations, such as American Society of Mechanical Engineers (ASME) or the Institute of Electrical and Electronic Engineers (IEEE). Others are the work of trade associations or other private groups, the best known of which today is probably the International Standards Organization (ISO).

Whatever the source of engineering's technical standards, they will, in large part, be the work of engineers. They will be the work of engineers because only engineers have the knowledge necessary to write them. The standards are not deduced from physics, chemistry, or any other natural science; nor are they simply common sense (though generally consistent with common sense). They are instead a product of engineering experience. Some of that experience derives from laboratory experiments, much like the experiments of natural science. The chief difference between the experiments of natural science and those of engineering (insofar as there

is any) is that engineers typically experiment on human artefacts, not natural objects. However, much of the engineering experience on which the writing of standards depends will not be experimental but "field experience", that is, experience of artefacts in use where the control necessary for experiment is absent, for example, when the left wing of a fighter jet falls off at twenty-thousand feet during combat training. Engineers try to learn as much as possible from every such unhappy experience. Unlike surgeons in the old joke, engineers do not bury their mistakes. Instead, they record their mistakes, study them, and try to learn from them, typically embedding what they learn in new technical standards.

The recent history of the global arms industry offers enough examples of unhappy experiences with the products of engineering, such as the many children killed or maimed by landmines in peace time, for engineers to begin to develop international standards for the global arms industry similar to engineering's other international standards. There are even a few signs that now is a good time to begin developing such standards. I shall briefly describe three of those signs.

First, there is a US statute, the Arms Export Control Act, and the International Traffic in Arms Regulations (ITAR) issued under it. Since 1976, these have governed what military information and artefacts may be shared with "non-US persons". US persons (including organizations) can face heavy fines if they have, without authorization or the use of an exemption, provided non-US persons with access to ITAR-protected military articles, services, or technical data. Until the end of the Cold War, the focus of ITAR enforcement was preventing the Soviet Union from obtaining US military technology. Since 1990, the focus has increasingly become preventing weapons and weapons technology falling into the wrong hands, especially the hands of terrorists or rogue states.[13]

Second, in 2004, the National Defense Industry Association (NDIA), a US trade association, published a "Statement of Defense Industry Ethics", making several small revisions in 2009. Most of the larger US participants in the arms industry have adopted codes of ethics including provisions similar to those in the Statement. The Statement seems to reject making ethics relative to geographical cultures: the arms industry is to "[i]mplement effective ethics programs for company activities at home or abroad." The Statement is, however, almost silent about the health, safety, and welfare of people outside the US. The nearest the Statement comes to providing any guidance on that issue is the requirement that members of the arms industry

"[e]stablish corporate integrity as a business asset, rather than a requirement to satisfy regulators, by making ethics compliance integral to all aspects of corporate life and culture, including employee appraisals and promotions, to foster an environment where employees aspire to do the right thing." For engineers at least, doing "the right thing" seems to include taking into account, for example, the welfare of non-US children whom landmines might kill or injure. Such children are part of the "public" whose safety, health, and welfare engineers are supposed to hold "paramount".[14]

More important, the Statement does not treat ethical knowledge as proprietary. Instead, it urges members of the arms industry to "[c]ontribute to the common good of our industry and promote industry ethics whenever and wherever possible by sharing best practices in ethics and business conduct among NDIA members and including ethics training in NDIA sponsored events."[15]

Third, there is an initiative of the United Nations, the Arms Trade Treaty. Though it came into force on December 24, 2014, the first report detailing its implementation is not scheduled for publication until December 24, 2015.[16] So, we do not yet know how many of the states engaged in the global arms trade will sign the treaty, but it is a good guess that the most important, especially, China, Russia, and the US, will not—or, at least, will not sign it in the next few years. Still, the Treaty is an important step in regulating the global arms industry. It certainly provides a starting point for writing global standards for engineers.

The Treaty is 1) to "establish the highest possible common international standards for regulating or improving the regulation of the international trade in conventional arms" and 2) to "prevent and eradicate the illicit trade in conventional arms and prevent their diversion". The Treaty applies to all conventional arms within the following categories: battle tanks; armored combat vehicles; large-caliber artillery systems; combat aircraft; attack helicopters; warships; missiles and missile launchers; and small arms and light weapons.[17] The Treaty seems to cover non-lethal *parts* of weapon systems, such as radar or observation drones. It does not, it seems, cover non-lethal equipment, such as trucks, transport aircraft, body armor, or field kitchens.

How do these three documents provide a justification for the sources of engineering's standards, especially its international sources, to begin developing standards for the global arms industry that might help to resolve the ethical issues identified in Part 2 above? Let me give a

simple example: If there were an international standard prohibiting engineers from involvement with the sale of complete weapons or parts of weapons of any sort to a regime likely to misuse them, the standard would simply echo the Treaty. If, in addition, the engineering standards contained criteria for identifying weapons likely to be misused and the sort of regime likely to misuse them, engineers might then inform an employer considering sale of such weapons or parts of such weapons to such a regime that the sale not only violates international standards but is inconsistent with good engineering. Engineers can have no part in such a sale. Involvement would be unprofessional.

A source of engineering's standards, such as IEEE or ISO, would have a justification for issuing such a standard. Article 7 of the Arms Trade Treaty specifically requires a signatory State considering licensing an export to "assess the potential that the conventional arms or items [in question]" may be misused in various ways, for example, to "commit or facilitate a serious violation of international humanitarian law.... [or] human rights law." While the Treaty's authors probably thought of the decision to license as primarily governmental, there is nothing in that understanding to forbid a member of the global arms industry from deciding not to seek its government's permission or for engineers working in the global arms industry from appealing to their own ethical standards when asked to participate in such a transaction. Their employer is (according to the NDIA Statement) supposed to want engineers to "do the right thing" and standing by (morally justified) professional standards is doing just that.

Of course, engineers individually are not qualified to assess the likelihood that a particular regime will misuse a particular weapon, even though they are likely to know much about how the weapon can be misused. So, any standard developed for the use of engineers would have to include the sort of information an engineer would need to make such an assessment. That information might come in a quite simple form, for example, in the form of a checklist asking (among other things) how this or that human rights group rates the regime, what uses the regime has made of weapons in the recent past, and so on. An individual engineer could then inform the appropriate superior, "We need to check out the following to be sure that this sale meets international engineering standards."

This sort of individual response may not seem like much help with the ethical issues identified in Part 2. After all, the engineer's superior might simply ignore the international

standard and replace an engineer unwilling to participate in the sale with an engineer who is willing or with a willing non-engineer.

While it is true that a superior might do that, there is good reason to think that response is, all things considered, unlikely. Such a response can have substantial costs, especially when the manager most needs an engineer. There are at least three sources of that cost: First, engineers are not interchangeable. They are often quite specialized. The engineer first asked to participate in the sale is likely to be the most qualified. The replacement (assuming one can be found) is likely to be less qualified. Therefore, the substitution may increase the risk of bad decisions as the sale progresses. Second, the risk of bad decisions is even higher if the substitute for the engineer is a non-engineer. Engineers are generally brought into sales only when they are needed, only when they are likely to have knowledge or insight non-engineers lack. Third, overruling an engineer on a matter involving application of an engineering standard risks harm to the manager. If anything later goes wrong, the manager who overruled the engineer will be open to blame, even if he found another engineer or a "scientific expert" to replace the unwilling engineer. He was on notice that there might be a problem and he did not "do the right thing". If, on the other hand, he goes along with the engineer's recommendation, he can at least claim that he was acting on the best technical advice available.

These are all relatively short-term costs of one manager's respecting or not respecting the engineering standard in question. There is also at least one long-term cost worth considering if the organization makes a practice of overruling engineers on such issues. Widespread lack of respect for engineering standards may have a bad effect on the morale of the organization's engineers generally and so, on the ability of the organization to recruit and keep the most marketable engineers, not only the most marketable "bench engineers" but also the most marketable higher-ranking engineers (including senior management).

We have, of course, been assuming that the engineer's superior is unsympathetic to the appeal to engineering standards. That is a worst-case scenario. In practice, the superior is likely to be another engineer, one for whom engineering standards carry considerable weight, even if he is now acting as a manager rather than an engineer. And the organization in which these two engineers work is likely to have its own code of ethics, compliance procedures, and the like designed (as the NDIA Statement requires) to ensure, as much as possible, that organization employees, including engineers, "do the right thing." The ethical environment of the

organization is likely to be far friendlier to engineering standards than we have tacitly been assuming in dealing with this example.

This is, admittedly, a relatively simple example of a standard that might be adopted, one that does not look particularly technical. The standards actually adopted—for example, criteria for "safe landmines" requiring them to resist light touches, to disarm automatically after a certain period, and so on—are likely to look much more technical, making the overruling of the engineer look even more risky.

Acknowledgments

I presented the first version of this paper to the Philosophy Colloquium, Illinois Institute of Technology, March 6, 2015, to which I owe several improvements.

Notes

[1] This is the typical dictionary definition of "dilemma" (when the term is not simply wasted as a synonym for "hard choice"). However, until the last few decades, philosophers have had a much-more-precise definition of "dilemma", that is, as an inference having the following form: P v Q, P—> R, Q—>R, therefore R. I regret the eclipse of that technical sense.

[2] In defining "global" in this way, I may seem to be departing from the original call for this conference. The call (Finkelstein email, December 5, 2014) listed among relevant "dilemmas" two that seem to apply to the domestic arms industry at least as much as to the global arms industry (italics mine):

> Sometimes the industry can provide a necessary and ethically sound *national* security product only by using materials that are potentially legally problematic, such as "conflict minerals." Should the global defense industry be held to a higher standard than other industries given the sensitive and potentially controversial nature of its enterprise? Or perhaps a more relaxed standard, given the critical nature of its function and the overwhelming importance of a strong *national* defense….
>
> Finally, many of the dilemmas that arise at the intersection of ethical and legal standards pertain to new technologies, such as surveillance equipment and cutting edge defensive weapons systems. Often there are objections to such technologies on ethical grounds: do advanced surveillance technologies violate privacy norms, especially when they [the technologies] can be used on civilian populations? Should the industry be responsive to objections to technological development in *national* defense, such as the frequent concerns expressed that smart weapons are replacing human judgment on the battle field?

Concerns about "national defense" carry weight only when the nation in question is one's own—and, by the definition I proposed, the global arms industry is concerned (in part) with helping other nations make war; it is the domestic arms industry that is concerned with *the* national defense. I have therefore treated these two paragraphs as including "slips of the word processor" rather than as part of the conference definition.

[3] Finkelstein email, December 5, 2014: "Often there are objections to such technologies on ethical grounds: do advanced surveillance technologies violate privacy norms, especially when they can be used on civilian populations?"

[4] http://www.nationaldefensemagazine.org/archive/2011/March/Pages/StatementofDefenseIndustryEthics.aspx (accessed January 10, 2015). Lockheed Martin, a sponsor of this conference, has taken a similar position: "We have zero tolerance for corruption." Lockheed Martin, *Setting the Standard: Code of Ethics and Business Conduct*, p. 25, http://www.lockheedmartin.com/us/who-we-are/ethics/code-of-ethics.html (accessed December 28, 2014). That page includes enough explanation of what the standard means to make it clear that the quid pro quo in question is probably unethical.

[5] That is, since the Lockheed bribery scandal of the early 1970s. Interestingly, Lockheed is ancestor of Lockheed Martin. http://en.wikipedia.org/wiki/Lockheed_bribery_scandals (accessed January 5, 2015). For recent work on bribery in global business ethics, see, for example, Margo Cleveland, Christopher M. Favo, and Thomas J. Frecka, "Trends in the International Fight Against Bribery and Corruption", *Journal of Business Ethics* 90 (2009), Supplement: 199-244; or the initial discussion and references in Edmund F. Byrne, "Towards Enforceable Bans on Illicit Businesses: From Moral Relativism to Human Rights", *Journal of Business Ethics* (2014): 119–130.

[6] By "not much discussed in business ethics", I actually mean "virtually undiscussed". The following are the few discussions I have found: Gavin Maitland, "The Ethics of the International Arms Trade", *Business Ethics: A European Review* 7 (October 1998): 200-204; Edmund F. Byrne, "Assessing Arms Makers Corporate Social Responsibility", *Journal of Business Ethics* (2007) 74: 201–217; and Barton H. Halpern and Keith F. Snider, "Products That Kill and Corporate Social Responsibility: The Case of U.S. Defense Firms", *Armed Forces & Society* 38 (2012): 604-624.

[7] For more on these, see Jacque G. Richardson, "The bane of 'inhumane' weapons and overkill: An overview on increasingly lethal arms and the inadequacy of regulatory controls", *Science and Engineering Ethics* 10 (2004): 667-692.

[8] US Chamber of Commerce, *Defense Trade: Keeping America Secure and Competitive* (March 2007), p. 8, www.uschamber.com/sites/default/files/legacy/issues/defense/files/defensetrade.pdf (accessed December 30, 2014); Department of Defense, "Defense-Related Employment of Skilled Labor: An Introduction to LDEPPS" (March 2011), p. 4. www.economics.osd.mil/LDEPPS_Primer.pdf (accessed December 30, 2014).

[9] For a fuller discussion of the importance of engineers to the arms industry, see Aaron Fichtelberg, "Applying the Rules of Just War Theory to Engineers in the Arms Industry", *Science and Engineering Ethics* 12 (2006): 685-700.

[10] See biographies of: Patrick M. Dewar, Executive VP; Dale P. Bennett, VP for Mission Systems and Training; Richard F. Ambrose, VP for Space Systems, http://www.lockheedmartin.com/us/who-we-are/leadership.html (accessed December 30, 2014).

[11] The parenthetical "in part" recognizes the role that the US government would normally have in such a sale.

[12] For those who doubt this claim, see the first three chapters of my *Thinking like an Engineer: Essays in the Ethics of a Profession* (Oxford University Press: New York, 1998), as well as the more recent: "Is Engineering a Profession Everywhere?" *Philosophia* 37 (June 2009): 211-225; "Defining Engineering—From Chicago to Shantou", *Monist* 92 (July 2009): 325–339; "Does 'Public' mean an engineer's nation?" *2014 IEEE International Symposium on Ethics in Science, Technology, and Engineering* (Chicago, IL: 23-24 May 2014): 1-4. DOI: 10.1109/ ETHICS.2014.6893405; and "'Global Engineering Ethics': Re-inventing the Wheel?" *Engineering Ethics for a Globalized World*, edited by Colleen Murphy, et al. (Springer, forthcoming). Compare Fichtelberg (2006) which seems to miss the import of the engineer's obligation to the "public".

[13] http://en.wikipedia.org/wiki/International_Traffic_in_Arms_Regulations (accessed January 3, 2015).

[14] For a defense of this claim, see my "Thinking like an Engineer: The Place of a Code of Ethics in the Practice of a Profession", *Philosophy and Public Affairs* 20 (Spring 1991): 150-167.

[15] http://www.nationaldefensemagazine.org/archive/2011/March/Pages/StatementofDefenseIndustryEthics.aspx (accessed January 10, 2015)

[16] http://www.un.org/disarmament/ATT/ (accessed January 3, 2015).

[17] Art. 1 and Art. 2, The Arms Trade Treaty, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/67/234&Lang=E (accessed January 3, 2015)

DRAFT DRAFT DRAFT

SILO MENTALITIES, DOMINANT LOGICS AND THEIR ETHICAL CHALLENGES IN THE DEFENSE INDUSTRY

[and in all organizations]

Patricia H. Werhane

Professor Emerita, University of Virginia and DePaul University

INTRODUCTION

In this paper I shall analyze two ongoing ethical issues that pop up in many organizations: the phenomena of silo mentalities and the pervasiveness of organizational dominant logics. I shall focus on these phenomena only on the defense industry, but they occur in every type of organization. Silo mentality is a widely occurring phenomenon wherein a profession, particular division of a company or a company itself is so focused on their priorities or their expertise that they neglect or fail to perceive how those priorities affect or are affected by other professions, divisions in the company or other corporate members of their industry

The term dominant logic defines another kind of phenomenon. According to Prahalad and Bettis, who coined this term, a dominant logic refers to an organizational culture, a set of practices and habits that help frame the organizations goals and modes of operation. (Prahalad and Bettis, 1986) Dominant logics are vital for the coherent functioning of an organization as an organization. However sometimes a dominant logic can become so ingrained that it creates blind spots or hinders change.

These two phenomena, silo mentalities and dominant logics, which, to repeat, are ubiquitous in many organizations, can result in organizational failures. Using the well-documented Challenger and Columbia shuttle explosions as examples, I shall argue that silo mentalities at NASA and its dominant culture played, central roles in these disasters. These cases thus illustrate how these two phenomena, if unnoticed, can create untoward consequences in any organization. I shall conclude with some suggested remedies to this set of ongoing ethical issues.

A SOCIAL CONSTRUCTIVIST PERSPECTIVE

I shall begin reminding the reader of a commonly held presupposition. It is acknowledgement that our minds are not merely absorbing mirrors of experiential data. Rather, human beings deal with and interpret their experiences through cognitive frames, mind sets, or mental models,

following Senge (1992). These models represent intuitive and unconscious methods of sense-making (Weick, 1995). Our minds continually interact with others as well as with the data of our experiences (most if not all of which are shared), selectively filtering and framing that data though various social learning processes. In the process of focusing, framing, organizing, ordering, and discussing what we experience, we mentally bracket or simply omit data simply because we cannot observe or absorb all that we encounter through perception. Each mental model or set of models is finite. because no one has the capacity to take in all of the data of one's experiences; to the contrary, we selectively focus on some aspects and necessarily must ignore others. These cognitive framing exercises, then, can and often do ignore important data. (Werhane, 1999)

In philosophy of science it is now generally understood that scientific methodologies are themselves mental models through which scientists discover, predict, and hypothesize about what they then call reality. Social construction theory takes this idea one step farther with the claim that our shared mental models or schemes frame *all* of our experiences in the sense that they guide the ways in which we recognize and organize what we then call the world. From this claim it follows that the categories that we apply to reality are socially structured. (Gorman, 1992) Indeed, according to social constructionism, this is the only way in which human beings can understand *anything.* Notice this is not the claim that our minds construct reality or what we call experience or the data of experiences. Rather it is the contention that the incomplete and disparate ways in which we present and distill experiences are socially constructed, and thus finite. As a result, because we cannot take in nor frame all the data of our experiences, in sorting out we often leave out important data or ignore data that does not fit into our expectations or habits. This phenomenon, called "bounded awareness," is unavoidable and common, but it can create what Moberg, Bazerman and Tenbrunsel have called "blind spots," where we miss or ignore essential data. (Moberg, 2006; Bazerman and Tenbrunsel, 2011)

Often, too, we create habits that are reinforced either internally or externally through social interactions. In new situations these habits can reinforce choices and behavior that do not take into account bizarre or new situations as just that—new, and we often tend to interpret these situations through our habits. Thus "the most serious problem …is not that we frame experiences, it is not that these mental models are incomplete, sometimes biased, and surely parochial. The larger problem is that most of us either individually or in organizations do not realize that we *are* framing, disregarding data, ignoring counterevidence, or not taking into account other points of view." (Werhane, 2007, 404)

SILO MENTALITIES AND DOMINANT LOGICS

At least one dictionary defines silo mentality as "an attitude within an organization when the different sections or departments do not share information properly because they do not want to share success with others, with the result that the organization is not efficient." (Macmillan Dictionary, 2015)(Another depicts it as "a mind-set present in some companies when certain

departments or sectors do not wish to share information with others in the same company. This type of mentality will reduce the efficiency of the overall operation, reduce morale, and may contribute to the demise of a productive company culture." (Business dictionary, 2015) (www.businessdictionary.com/definition/silo-mentality.html)

In this context I am defining this term not as an attitude or deliberate mind set but as a phenomenon that can arise from various causes, the result of which the insufficient or lack of information sharing. This may or may not be because of worrying about success or failure. Rather silo mentalities can exist as outcomes of ingrown habits or a narrow interpretation of organizational roles. An engineer might see herself as a scientist, not as a decision-making while manager might not fully appreciate the importance of negative data when other counterevidence was positive. Or silo mentalities can arise in an organizational structure that does not encourage dissent or cross-communications. This phenomenon is also sometimes described as tunnel vision or tribalism. All of these phenomena can create a framing of expertise or organizational habits that focus on one area of expertise or model and ignore or do not take into account other areas that are pertinent to that organization and its decision-making.

In the defense industry where there is a great deal of collaborative work between companies to complete a finished product, focusing only within one's silo can have dangerous consequences. In both the Challenger and the Columbia explosions, in brief, and for different reasons we shall outline in the next sections, not all of NASA's subcontractors communicated properly with each other and with NASA as to the risks entailed in their contributions to the constructing and evaluating the structure of the shuttle in question. And within NASA itself, very simply put, it appears that many engineers and managers seemed each to have had different perceptions of the risks involved on those launches, and neither (and there were others) understood the mindsets (and thus the risk analyses) of the other.

Dominant logic refers to the most prominent or overriding "logic" or mind set by which an organization operates, its customs, culture, habits of decision-making and even organizational charts. But, as Prahalad and others have pointed out, a dominant logic can create blind spots constantly reinforced sets of habits that preclude creative thinking and adaptability to change in a changing economy. Worse, Prahalad and Bettis maintain, "…the more successful organizations have been, the more difficult unlearning becomes." (1986: 498) Firms' successes fortify their theories of action and makes revisions significantly more difficult (Argyris and Schön, 1978; Starbuck and Hedberg, 1977). "…[T]he longer a dominant logic has been in place, the more difficult it is likely to be to unlearn" (Bettis and Prahalad, 1995: 11).

According to both the Challenger and Columbia government reports, because of its many successful launches, the culture at NASA was rooted in a basic conviction that they were invincible, despite these 2 horrendous accidents. Moreover, at NASA, there was a well-documented logic of strict hierarchy. Engineers assumed that managers were in charge of decision-making. Raising issues or questioning a decision was not encouraged and genuine exchanges of ideas and suggestions were not part of the practice at NASA A third characteristic of this culture, and this was part of the invincibility mind set was the belief that if something worked, and worked repeatedly, it should not be tampered with. This conviction, the normalization of risks, which the *Columbia Report* called the "normalization of deviance" (196) or cognitive dissonance, precluded raising questions about early o-ring failures preceding the

Challenger explosion, and the repeated loss of tiles on almost every flight, including Challenger, preceding Columbia's disaster.

Let us consider these two classic examples: the well-documented Challenger and Columbia shuttle explosions in more detail as illustrating silo mentalities and unexamined dominant logics.

THE CHALLENGER DISASTER, 1986

The details of the 1986 Challenger space shuttle explosion are well-known. The causes of this explosion are complex, and those involved were intelligent, well-meaning, and cared deeply about the success of the shuttle program. And that highlights the problem in both examples: this was not a matter of evil that could easily be targeted and the culprits removed. There were no culprits.

As it is reported by the *Rogers Commission Report* there were a number of contributing elements, which together, caused the explosion. The most famous is the failure the shuttle's o-rings to properly seal due to the frigid conditions on the day of the launch. But as early as the 6th shuttle launch there had been o-ring problems, documented problems reported by engineers such as most famously, Roger Boisjoly. But his memos citing the possible risks to o-ring failure were by and large ignored and by the 25th launch o-ring weaknesses were considered "normal." On the evening before the Challenger launch, a group of engineers objected to the launch scheduled for the next day because of predicted bad weather making the rescue of the module problematic, and because the o-rings had never been tested at cold temperatures predicted for that day. The engineer mentality is ordinarily to worry about safety first. Their mind set usually based on the idea that if a mechanism cannot be proved to be safe, then one assumes it is not until there are more adequate positive indicators. But at the prelaunch meeting the manager of the project, Jerry Mason, now famously told the head engineer, Roger Lund to "take off your engineering hat and put on your management hat."(*Rogers Commission Report*, 1986) The management thinking was that if the engineers could not prove that the o-rings would not work well under cold conditions, one would assume the launch was safe, a mind set in contrast to engineering. The conflicts between a managerial and an engineering mind set where each is operating from his or her role-based silo are obvious, but worse, neither understood that these were mind sets, points of view that deserved to be challenged and were not. The engineers thought of themselves as scientists, which they are, but succumbed to managerial decisions that went against their best judgment, because they accepted that authority and the managerial roles as decision-makers even when those decisions were thought to be flawed. The engineers were in their scientific silos, managers in theirs, and neither imagined questioning those roles.

A second illustration of silo mentality is the various perceptions of risk. According to the physicist Richard Feynman, a member of the Rogers Commission team, estimates of the probably of failure varied considerably. On the launch pad ,and at NASA the perception of the

probably of an explosion was as little as 1 in 100,000 while engineers estimated the risk as high as 1 in 10. Yet again, each operated on his or her own calculations or the available data and did not think to consult others (Feynman, 1989)

One of the important contractors for the Challenger was Morton Thiokol and at that company in 1986 there was a policy that anyone within the organization could "blow the whistle" to the CEO at any time. But the engineers on this project did not step out of their assigned roles as scientists to do so. Whether that would have made a difference in the decision to launch remains unknown. But the fact that no one in the NASA organization thought to do so is disturbing.

Coupled with the silo mentalities at NASA was a dominant logic, a logic or ingrained belief that managerial decisions were not to be questioned and the siloed lack of communication and openness reinforced that. NASA had had so many successes and so few accidents, there is wide-spread belief both among managers and engineers that NASA was and could continue to be virtually error-free. That dominant logic at NASA creates an organizational silo that gets in the way of carefully considering the business of NASA (human space travel), the complexities of constructing space shuttles, the myriad of contractors (and thus possibilities of errors) involved, and thus the inherent risks of each shuttle launch, orbit, and landing. (*Rogers Commission Report*, 1986, *Columbia Report, 2003)*

THE COLUMBIA SHUTTLE EXPLOSION

The Challenger explosion was a terrible tragedy and an enormous loss to NASA and the space program. But there were lessons to be learned from that disaster. Unfortunately one could almost do a "search and replace" between the two subsequent reports of these disasters, because of the many parallels between the two explosions and the events that precipitated the explosions, reinforced by an unchanged dominant logic.

The cause of the Columbia explosion was a large piece of insulating from the Thermal Protection System protecting the shuttle, foam that dislodged from the shuttle just after launch. That insulating form struck the left wing of the craft and penetrated its protective seal, thus allowing hot air at the shuttle's reentry to penetrate the structure and break up the shuttle. (*Columbia Report,* 2003, 9) Insulating foam had dislodged from earlier Columbia missions, indeed according to the Report, "[f]oam loss occurred in over 80 percent of 79 missions which had imaged this loss." (53) Still, again according to the *Columbia Report* and despite some reporting to the contrary (e.g., see Langewiesche, 2003, p.) " previous foam losses were in a small area and of little concern. Nor was the foam material defective, having been tested numerous times and in various climatic conditions. Moreover, according to the Report, "Negligence on the part of NASA, Lockheed Martin, or United Space Alliance workers does not appear to have been a factor." (53) Rather, the dramatic foam loss on this flight was due to a number of factors some of which are still undetermined. However, the *Report* suggests that "a

combination of variable and pre-existing factors, such as insufficient testing and analysis [of the foam] in early design stages, resulted in a highly variable and complex foam material, defects induced by an imperfect and variable application, and the results of that imperfect process, as well as severe load, thermal pressure vibration, acoustic, and structural launch and ascent conditions. " (53-54)

But there are other factors contributing to this explosion, factors traced to the organization culture at NASA , factors that had also played significant roles in the previous Challenger explosion. Although NASA allegedly reformed its organizational culture after Challenger, remnants of that remained. In addition to budget constraints the hierarchical culture remained. According Langewiesche, dissenting opinions were discouraged throughout the organization, and as a result engineers saw themselves as merely engineers and managers as those in charge of decision-making. (24) Moreover, after it was discovered that foam debris had hit the left wing during launc,h the head Mission Management, Linda Ham, dismissed it as 'normal,' and refused admit that there might be unique problems with this flight, since foam loss had not created dangers on any of the previous flights. Thus she did not approve a request for more photos of the wing, and no one questioned her authority. (Donovan and Green, 69-76; *Columbia Report*, 2003, 147, 157)

That engineers went along with managerial decisions is not surprising. Numerous studies have documented that inescapable fact that most of us go along with authority or authority figures. (See MIlgram, 1974, Werhane, 2014) As children we learn to obey authority. This is reinforced in hierarchical organizations where decision making is also hierarchical and "from the top." Sometimes then, those in the middle or bottom of the organization imagine that because of their positions, manager decisions are correct or at least, not to be questioned. In other organizations such as the military, or in dictatorships, that assumption is rule-bound. Only in a flattened hierarchical culture where questioning is encouraged and disagreements are part of everyday communication can such habits be changed. NASA's successes have precluded considering such changes in their modes of operation. Moreover, as one of the independent investigators of the explosion Hall Gehman, is quoted as saying, [NASA]is an incestuous hierarchical system with invisible rankings and a very strict informal chain of command… [You hear, 'Well, I was afraid to speak up…If I had spoken up, it would have been at the cost of my job.' And if you're in the engineering department, you're a nobody." (Langewiesche, 2003,76)

Part of this may be due to "normalized deviance," habits that built up because previous launches of the Columbia had experienced foam tile losses and damage on every shuttle launch. to every shuttle. But there were no fatalities, it became assumed that this phenomenon was "normal" or "acceptable risk," without imagining what would happen if a foam tile went astray and penetrated the shuttle. (*Columbia Report* 121) (This is similar to the Challenger normalizing o-ring deterioration which occurred as early as the sixth flight of the Challenger shuttle.). Moreover, there was a widespread dominant logic at NASA that the shuttle was an operational vehicle, while in fact the whole shuttle program and these vehicles are experimental. This belief

led to flawed risk analysis of the inherent dangers of each launch and flight. (*Columbia Report*, 2003, 196)

Part of the neglect of this foam debris problem in this flight was due to the lingering mindset of invincibility. Despite the Challenger explosion, since 1986 there had been 87 successful shuttle flights over the 15 year period between that explosion and Columbia. (*Repor*t, 2003, 101) No wonder NASA developed extraordinary confidence in their invincibility in shuttle flights!

As the Chair of the Debris Assessment Team and himself an engineer, Rocha wrote in an email he shared with other engineers but did not send, "…this is the wrong (and bordering on irresponsible) answer from the SSP [Space Station Program] and Orbiter not to request additional imaging help from an outside source. …[S]evere enough damage ..combined with the heating and resulting damage to the underlying structure at the most critical locations…could present potentially grave hazards. The engineering team will admit it might not achieve definitive high confidence answers without additional images, but without …clarify[ing[the damage visually, we will guarantee it will not…" (Report, 157)

There are at least two interesting pieces of information from this unsent memo. First, it was not sent; was that a fear of questioning Ham's authority? According to Rocha, there was. (Report, 2003, 157) [1]Secondly , as in the case of the prelaunch discussion of the Challenger, there was a mindset disconnect between engineers and managers at NAS. As an engineer ,Rocha needed proof that the shuttle was not in danger, evidence that might have been seen through careful imaging of the shuttle's wing. That is a mindset that if you cannot prove a shuttle is safe, one assumes it is not until there is confirming evidence of safety. On the other hand, Ham, like the managers of the Challenger launch, assumed that because previous shuttles had not exploded despite foam debris, this one would not as well. Thus each was functioning within his or her silo of expertise or training, and each was unwilling or afraid to challenge their own mind sets and the thinking of others. Moreover, the hierarchical structure at NASA was not welcoming to dissent, and engineers imagined that their place was to do the science and not make or question decisions of managers. So while the stray foam was the physical cause of the explosion, the organizational culture at NASA precluded taking evidence and safety measures while the shuttle was in orbit that might have prevented that explosion.

The real tragedy is not remembering the organizational as well as physical causes of the previous explosion, a cultural amnesia that could reoccur again.

SOME POSSIBLE REMEDIES

The existence of silo mentalities and flawed dominant logics are evident in individuals, in organizations such as NASA, in corporations, and in our culture. They are outcomes of the ways

[1] "When asked why he did not send this e-mail, Rocha replied that he did not want to jump the chain of command. Having already raised the need to have the Orbiter imaged with Shack [a NASA manager], he would defer to management's judgment on obtaining imagery." *(Report,* 157).

in which individuals and organizations socially construct their experiences. And as one commentator noted, "[i]nstitutional logics, once they become dominant, affect the decisions of organizations…by focusing the attention of executives toward the set of issues and solutions that are consistent with the dominant logic and away from those issues and solutions that are not." (Thornton, 2004: 12-13). At NASA the hierarchical structure and lack of communication between engineers and managers reinforced silos of flawed decision-making. And the dominant logic, the pervasive mentality of NASA which the *Columbia Report* describes as "NASA appeared to be immersed in a culture of invincibility…" (199) precluded an ongoing consideration of the risks of this experimental vehicle. These organizational weaknesses are evidenced in both the Challenger and Columbia explosions, a pervasive mentality that was not seriously reexamined after the Challenger disaster.

How does one make changes to an organization to avoid some of these problems in the future? Adopting the model of the highly successful Navy Submarine and Reactor Safety Program, the *Columbia Report* proposes a series of recommendations for NASA. First and foremost, NASA must establish communication between all employees: engineers, managers, subcontractors and NASA administration that are open, nonjudgmental, encourage minority opinions, and without fear of hierarchical retaliation. These seem to be obvious suggestions but they are exactly what did not go on at NASA previously.

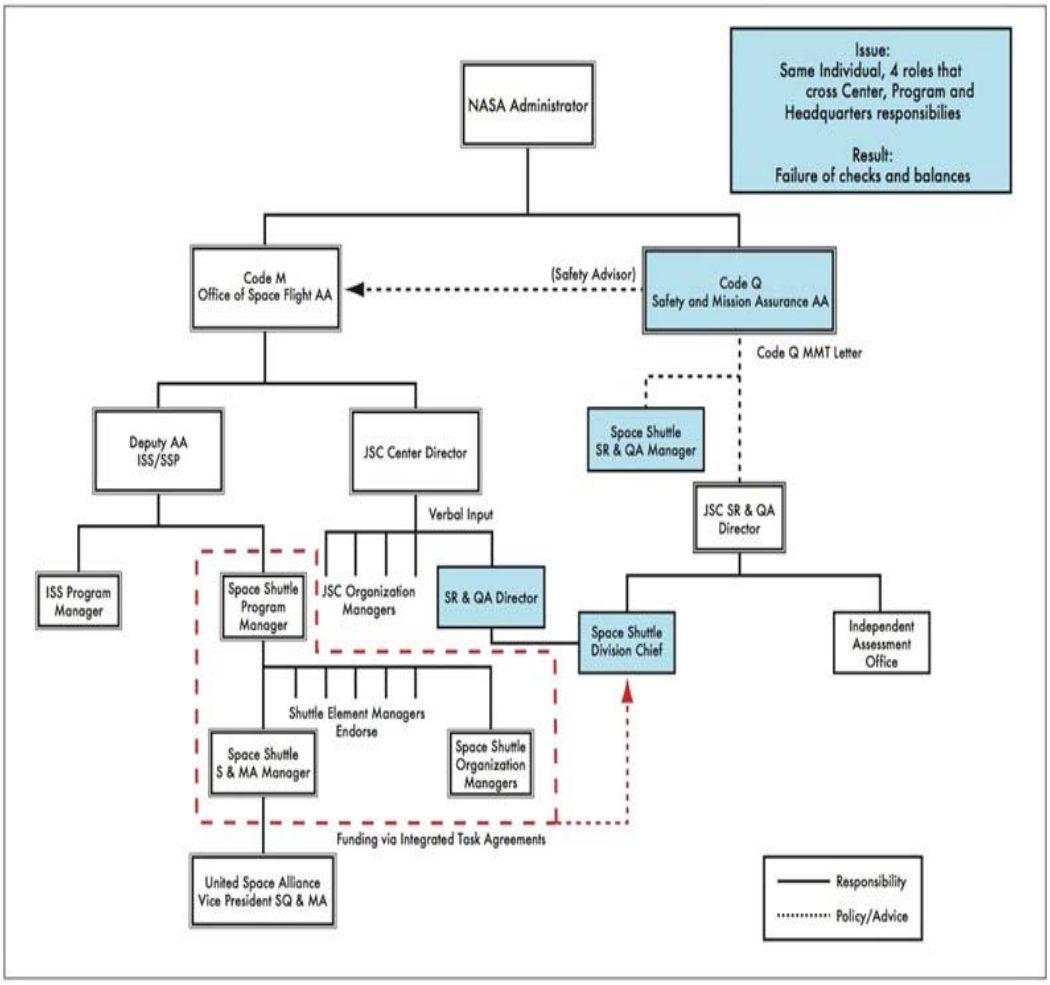
Secondly, training, which is obvious, but more importantly learning from the mistakes of Challenger and Columbia. I would suggest that this is best done through using the extensive Challenger and Columbia reports as case examples to illustrate what can go wrong despite the good intentions of all those involved. This sort of training should be carried out in a cross-disciplinary way, bringing in engineers , managers, subcontractors and NASA administrators together, not in separate training sessions. The latter would simply reinforce the pervading siloed culture. Using these disasters as learning experiences (rather than pointing fingers at particular managers) can also be effective in retaining knowledge at NASA . Somehow after 87 successful flights, the Challenger issues were forgotten and the continuing repeated occurrences of foam debris were dismissed as normal.

Third, part of this training should be in risk analysis including simulating worst-case scenarios that have not yet occurred. Such scenarios, the Navy discovered, reinforce the dangerous and experimental nature of their program, and reinvigorates risk analyses that are closer to that reality rather than merely the risks of every-day operational vehicles. Such analyses also strengthen the importance of safety as the primary consideration, a consideration that the Report found of secondary importance at NASA—"a broken safety culture…of blind spots." (*Columbia Report*, 184) created by the many successful launches and the managerial conviction that the past will always predict the future. (182-4)

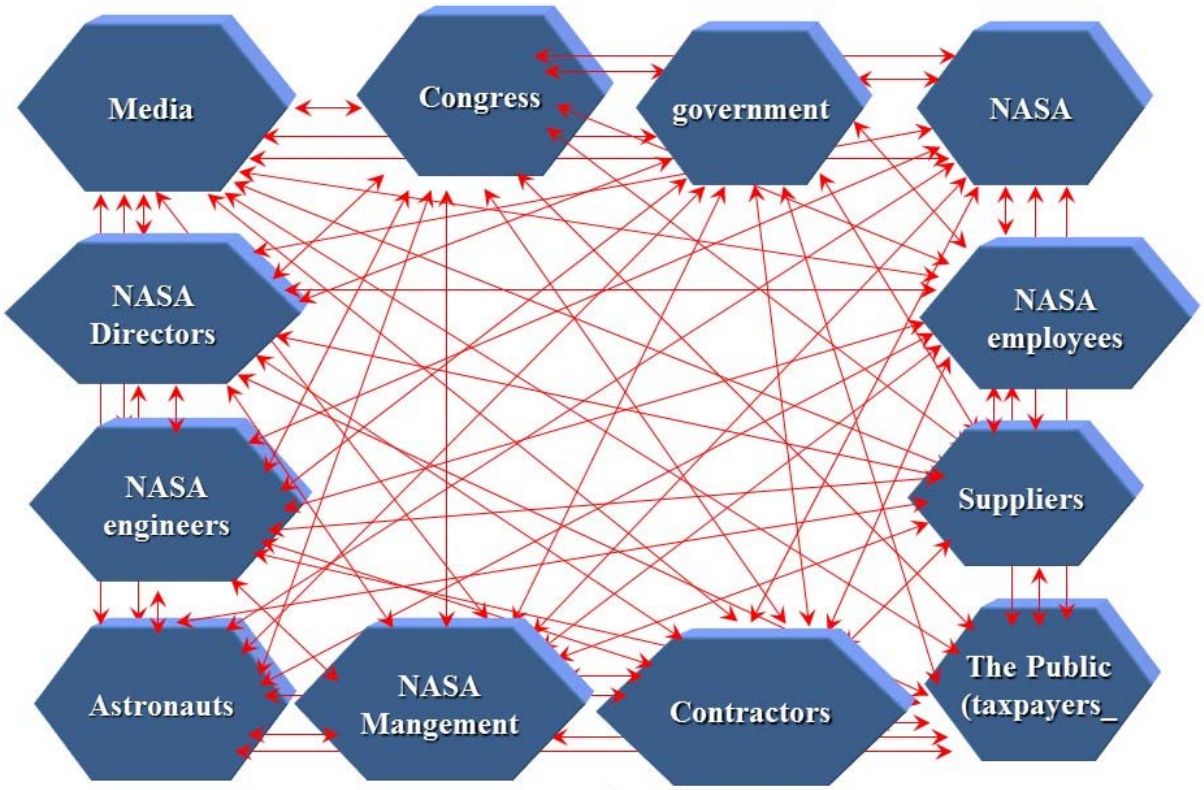
All of these are important recommendations not merely for NASA but for any organization. I would emphasize and elaborate upon two aspects. Returning to the assumption

with which I began this paper, despite that fact that all our experiences are socially constructed, because they are incomplete representations or reconstructions of the data of our experiences, one can step back from those constructions, reexamine a dominant mind set logic, and revise or change it. As human beings we do that all the time, and organizations do as well. To break out of a silo, to realize that one is in an organizational role that is merely that and overlaps with other functions of the organization, is important for employee development and to create instigators of change. To revise an organizational dominant logic individuals in that organization, usually its leaders, and the organization itself have to realize that these silos exist and that the dominant logic of the organization may be contributing to failure. Moreover, they have to experiment with new logics and be unafraid to change what seems to be "cemented" in place. Elsewhere I have call this the development of moral imagination coupled with courage to change. (Werhane, 1999) This is the most difficult thing to achieve in any organization. We are all creatures of habit and when operations seem to be going well, we loathe to change. NASA's successes are terrific and one would not want to interfere with the elements of that organization that has produced so many successful shuttle launches. However, every launch had problems, problems that were not addressed as life-threatening. Going back again and again to these successful but flawed launches and simulating worst-case scenarios could be very effective in changing NASA's culture. More importantly, a realization that there were many "near misses" in every flight that need not have happened, and that organizational mind sets contributed to those near misses (All documented in the two Reports) might help NASA to rethink itself.

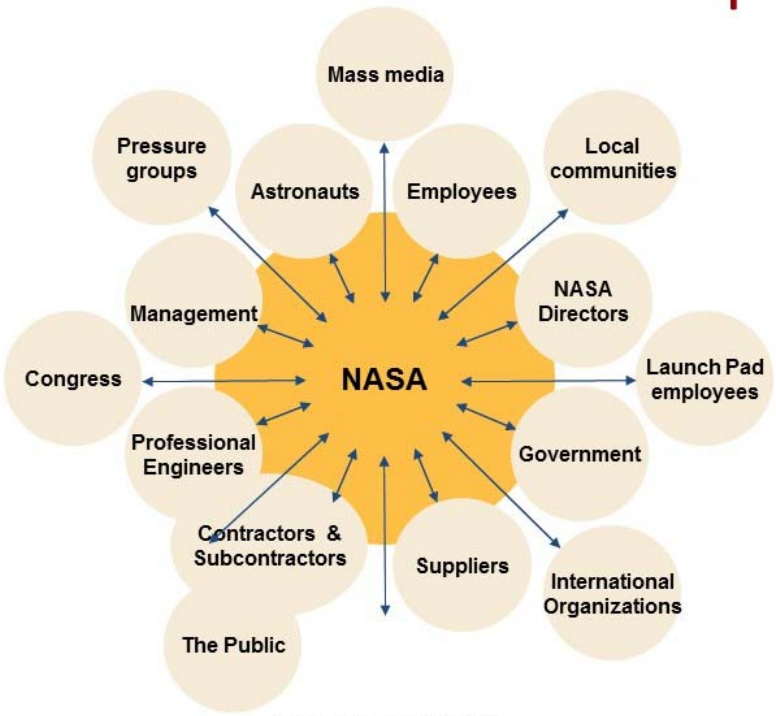
Finally, and this is only hinted at in the Report, probably because it seems obvious, the shuttle program is a massive systemic creation from a vast number of inputs from contractors, subcontractors, engineers, managers, suppliers, astronauts, government, etc. So what is required is a systems analysis of the program and of the design and launch of each shuttle. But it also requires rethinking the hierarchical structure or the organization. Figure 1 is one image of the organizational chart at NASA with arrows pointing to proposals for cross-sectional communication. But another way to encourage systems thinking is a graphic such as Figure 2 , undetailed but demonstrative of the complex interrelationships (and this is simplified) at NASA . Figure 3 places the shuttle program in the center to emphasize that that is what all of this is about. There are simple graphics but they have been effective in other organizations. For example, Novo Nordisk's graphic of their organization (see Figure 4) places people with diabetes in the center, to emphasize that they are in the business of ameliorating disease and that that, rather than the existence of the organization itself is of primary importance. These are simple graphics but in the age of visual rather than written thinking, they can be effective in revamping an organizational focus.



Columbia Accident Report, 2003, p. 185



A Stakeholder Map



Repositioned stakeholder maps

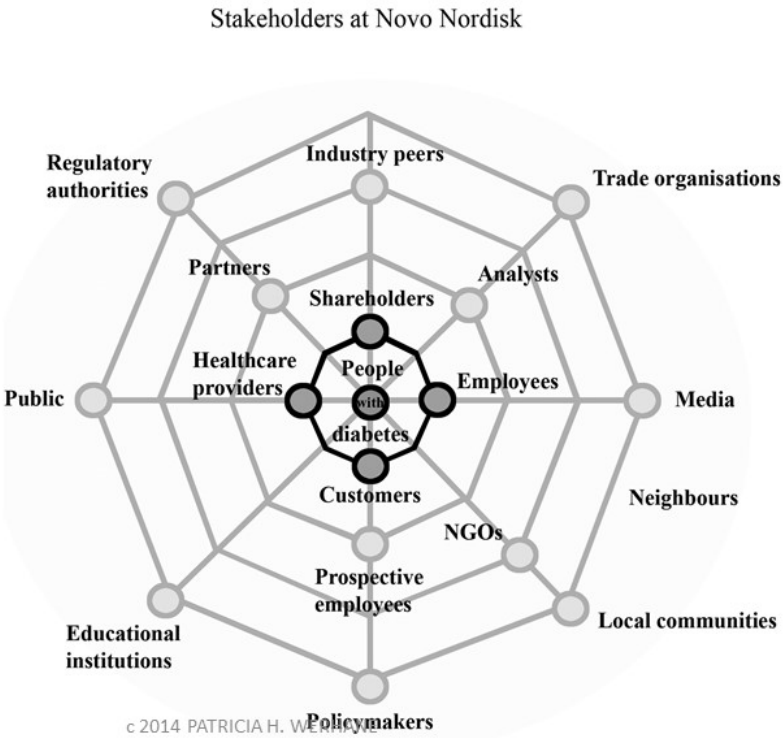


Figure 4

CONCLUSION

There are no simple solutions to discouraging silo mentalities or examining, evaluating, and revising ubiquitous dominant logics. Our schooling is, by and large, siloed. Managers don't learn much about engineering and engineers are not always good managers. Organizations can only function if there are some uniform practices in place. Yet each of these has its limitations, and being cognizant of those limitations and reexamining the mindsets that dominate an organization from time to time is essential to avoid disasters such as the two shuttle explosions. There is literature that argues that it takes a defining event (such as a shuttle explosion) to trigger these sorts of reexaminations. Isabella, Prahalad and Bettis observe that changing a dominant logic requires a precipitating crisis. "In general it appears…that changes in the ways organizations solve significant new problems (i.e. change dominant logics) are triggered by substantial problems or crises" (Isabella, 1992; Prahalad and Bettis, 1986: 498). Another researcher notes, "Organizational unlearning [a precursor to developing a new dominant logic] is typically problem-triggered….These triggers cause hesitancy and build up distrust in procedures and leaders. A turbulent period then frequently follows" (Hedberg, 1981: 19). But (a) that does not always work, particularly in an organization with a strong ingrained culture and habits such as NASA, which experienced a triggering event: the Challenger explosion. And (b) some organizations are able to evaluate ore reexamine their cultures and themselves without such an upheaval. In any case, the process of stepping back, which as conscientious or conscience-driven individuals we engage in all the time, and challenging operating procedures, ingrained habits, and decision processes is possible in organizations, all organizations, as well. This sort of thinking entails moral imagination and moral courage, it is risky since as we saw at NASA much of what they do is invaluable to the future of the space program and the various scientific experiments they engage in. Yet that set of exercises is vital to the future success of a very complex and worthwhile organization.

REFERENCES

Bazerman, M. and Tenbrunsel, A. 2011. *Blind Spots.* Princeton: Princeton University Press.

Business dictionary, 2015, www.businessdictionary.com/definition/silo-mentality.html. Accessed March 3, 2015.

Columbia Accident Investigation Board Report, (Columbia Report), Volume 1, 2003. Washington D.CL: National Aeronautics and Space Administration and the Government Printing Office.

Donovan, Aine, and Ronald M. Green. 2003. "CASE STUDY: Setup for Failure: The Columbia Disaster." *Teaching Ethics* 4.1: 69-76.

Feynman, Richard. 1989. *What Do You Care What Other People Think*. New York: W.W. Norton.

Gorman, Michael. 1992. *Simulating Science.* Bloomington IN: Indiana University Press.

Hedberg, B. 1981. "How Organizations Learn and Unlearn." In P.C. Nystrom and W.H. Starbuck (eds.), *Handbook of Organizational Design Vol 1, Adapting Organizations to their Environments*. Oxford: Oxford University Press. 3-27.

Isabella, L.A. 1992. "Managing the Challenge of Trigger Events: The Mindsets Governing Adaptation to Change." *Business Horizons.* September-October: 59-66.

Langewiesche, William. 2003. "Columbia's Last Flight." *Atlantic.* 292: 58-82.

Macmillan Dictionary. 2015. www.macmillandictionary.com/open-dictionary/entries/silo-mentality. Accessed March 5, 2015.

Milgram, Stanley. 1974. *Obedience to Authority.* New York: Harper and Row.

Moberg, Dennis. 2000. "Ethical Blind Spots in Organizations." *Organizational Studies* 27: 413-28.

Prahalad, C.K. 2004. "The Blinders of Dominant Logic." *Long Range Planning.* 37(2): 171-9.

Prahalad, C.K., and Bettis, R.A. 1986. "The dominant Logic: A New Linkage Between Diversity and Performance." *Strategic Management Journal.* 7: 485-501.

Report of the Presidential Commission on the Space Shuttle Challenger Accident, (*Rogers Commission Report"* Volume 1. 1986. Washington D.CL: National Aeronautics and Space Administration and the Government Printing Office.

Senge, Peter. 1990. *The Fifth Discipline*. New York: Doubleday.

Thornton, P.H. 2004. *Markets from Culture*. Stanford, CA: Stanford University Press.

Weick, K., Sutcliffe, K., and Obsfeld, D. 1995. *Sensemaking in Organizations.* Thousand Oaks CA: Sage Publications.

Werhane, Patricia H. 1999. *Moral Imagination and Management Decision-Making*. New York: Oxford University Press.

_____.2007. "A Place for Philosophers in Applied Ethics…" *Business Ethics Quarterly*. 16.401-8,

_____.Hartman, L. P. Archer, C., Englehardt, E. and Pritchard, M. 2014. *Obstacles to Ethical Decision-Making.* New York: Cambridge University Press.

Nanoethics (2012) 6:1–13
DOI 10.1007/s11569-012-0141-7

ORIGINAL PAPER

Anticipatory Ethics for Emerging Technologies

Philip A. E. Brey

Received: 25 October 2011 / Accepted: 14 March 2012 / Published online: 4 April 2012

Abstract In this essay, a new approach for the ethical study of emerging technology ethics will be presented, called *anticipatory technology ethics* (ATE). The ethics of emerging technology is the study of ethical issues at the R&D and introduction stage of technology development through anticipation of possible future devices, applications, and social consequences. I will argue that a major problem for its development is the problem of uncertainty, which can only be overcome through methodologically sound forecasting and futures studies. I will then consider three contemporary approaches to the ethics of emerging technologies that use forecasting: ethical technology assessment, the techno-ethical scenarios approach and the ETICA approach, and I considered their strengths and weaknesses. Based on this critical study, I then present my own approach: ATE. ATE is a conceptually and methodologically rich approach for the ethical analysis of emerging technologies that incorporates a large variety of ethical principles, issues, objects and levels of analysis, and research aims. It is ready to be applied to contemporary and future emerging technologies.

Keywords Anticipatory technology ethics · Emerging technologies · Uncertainty · Futures studies · Forecasting · Technology assessment

P. A. E. Brey (✉)
Department of Philosophy, School of Behavioral Sciences,
University of Twente,
P.O. Box 217, 7500 AE Enschede, The Netherlands
e-mail: p.a.e.brey@utwente.nl

Introduction

Different technologies find themselves at different stages of development and societal uptake. Some technologies have yielded many concrete devices and applications and are used by a many different people in a variety of contexts. For such technologies, ethical analysis has the benefit that many of the ethical issues have already been identified in society. For instance, a large variety of ethical issues in relation to the Internet have been identified not only by ethicists, but also by users and other stakeholders who run into them as they use or deliberate on the technology. Other technologies, however, are still emergent: they are at an early stage of development and have not yielded many applications and societal consequences. They are still largely, or fully, at the research and development (R&D) stage, meaning that they are still at the stage of research into basic techniques, or at an early stage of development which at most has resulted in lab prototypes and experimental applications but little or no serious products that are being used by ordinary users. These technologies will be called *emerging technologies*.

For technologies at the R&D stage, ethical issues relating to their use in society cannot be known reliably, as their impact on society lies in the uncertain future. At the research (R) stage, the stage of fundamental research, the focus is on basic techniques, principles and methods that can be used for later development of concrete devices or processes, whereas development focuses on the actual design and manufacture of devices and processes. At this stage, no knowledge may yet exist

about possible devices or applications that may result from the research, so ethical reflection on future consequences may be wholly speculative at this stage. At the development (D) stage, the focus is on the design and manufacture of actual devices and processes. At this stage, more information is known about possible designs, but there is still considerable uncertainty about the devices and systems that will eventually gain societal acceptance, the ways in which these may ultimately be used, and the societal consequences that their use will bring. So at this stage, also, there is much uncertainty regarding ethical issues and ways in which these may be approached.

The question that is the focus of this essay is how we can identify and evaluate ethical issues for technologies that are still emerging because they are still at the R&D stage. With the accelerated pace of technological change in contemporary society, and the major impact that technology has on people's lives, early identification and evaluation of ethical issues is an important aim. Early identification can help users and other societal actors better prepare for future moral dilemmas, and can also help steer R&D or usage practices so as to avoid or minimize ethically undesirable consequences. Yet, so far very little research has been directed at developing sound approaches and methods for ethical analysis of emerging technologies. It is only in recent years that such research has seriously gotten underway. My aim in this essay is to review some of this recent work and to present a new, integrative approach for the ethical study of emerging technologies.

Ultimately, ethical assessment of emerging technologies concerns the question of what is good and bad about the devices and processes that these technologies may bring forth, and what is right and wrong about ways in which they may be used. Since at the R&D stage many devices, usage patterns and social consequences of the technology are not yet present, ethical assessment turns speculative, as it focuses on particular R&D activities and techniques and then projects possible devices and usage patterns which are then assessed ethically. Such assessments may then be used to make ethical recommendations for R&D practices themselves, so as to increase the likelihood that these practices yield morally desirable devices and uses. Or they may be used for policy.

The paper is structured as follows. In the next section, two approaches within the ethics of emerging technology will be distinguished, based on how they deal with the problem of uncertainty about the future. In section 3, three recent ethical approaches to emerging technology will be discussed and critiqued, and it will be concluded that neither is fully satisfactory. In section 4, my own approach will be presented, which is called *anticipatory technology ethics* (ATE). I will present ATE as a promising new approach that builds on previous approaches, and I will provide examples throughout its discussion how it can be applied in practice.

Ethics, Uncertainty and Forecasting

The central problem for an ethics of emerging technologies is that we do not know the future, and therefore do not know which ethical issues will play out once the technology is fully developed and entrenched in society. Because emerging technology is technology in the making, many questions about its nature, its future use and its social consequences are still undecided. For this reason, many ethical issues in relation to it cannot yet be identified or analyzed reliably. We can speculate about future applications and uses, but as history has shown, speculations about future technology are often way off the mark, meaning that we may end up exploring a misguided or irrelevant set of ethical issues.

The ethics of emerging technology therefore has to deal with an epistemological problem, the *problem of uncertainty* concerning future devices, applications, uses and social consequences [8]. The question is how it can deal with this problem in a responsible manner. On the one hand, it is to be avoided that ethicists lose themselves in idle speculation on future ethical issues in technology that in most cases turn out to rest on mistaken projections on how the technology will actually evolve. On the other hand, it is to be avoided that ethicists feel that they can say nothing about emerging technologies because they do not know which devices and uses will result from them. So the question is how ethicists can come to assessments of emerging technologies that are based on somewhat reliable knowledge of the future.

Two approaches are possible at this point, one more conservative and reliable, the other more uncertain and speculative. The first approach is to restrict oneself to ethical analysis of generic qualities of the new

technology that are likely to manifest themselves in all or most future applications of the technology and that are likely to present ethical challenges. For example, when nuclear energy technology was being developed it was known early on that however it were to be developed, there would be a problem of radioactive waste, which requires ethical deliberation. When genetic technology was being developed it was known from the beginning that it would involve the modification of genetic material, which was considered to be intrinsically morally controversial. So even when particular applications or uses are not yet known, it is often possible to identify generic ethical issues that are likely to manifest themselves as the technology progresses, and these can be discussed at an early stage. I will call this approach the *generic approach*.

A second approach is to speculate on future devices, uses and social consequences. This requires that ethicists either rely on existing forecasting studies or do such studies themselves. They can then use the forecasts to explore ethical issues. For example, ethicists can forecast that nanotechnology will yield applications for targeted drug delivery in the human body using nanoparticles, and that such applications will become widely available to both doctors and patients. They can then analyze ethical issues that are likely to occur when such devices are being used. I will call this the *forecasting approach* to the ethics of emerging technology.

The forecasting approach relies on predictive studies of future technological devices, uses and social consequences. Such studies are undertaken in two related fields. *Futures studies* is a field that aims to study what possible or probably futures may look like [1]. Futures research includes many different forecasting approaches, such as environmental scanning, causal layered analysis, the Delphi method and scenario methods. Some of these, like the Delphi method, rely on the consultation of experts in various fields, whereas others may rely on surveys, time series analysis, regression analysis, or simulations. Some work in futures studies focuses on technology forecasting. It forecasts future technologies, including the development spread of certain types artifacts, and optionally their utilization and social consequences that may result from their use. *Technology assessment* (TA) is a field that studies the effects of new technologies on industry, the environment and society, evaluates such effects and develops instruments to steer technology development in more desired directions [5,12]. It makes such assessments on the basis of known or potential applications of the technology. Thus, TA in part relies on, and in part engages in, futures studies. Both futures studies and TA can hence be useful for forecasting the development of emerging technologies.

The forecasting approach has as an advantage over the generic approach that it is able to consider more ethical issues, by including not only those that are generic to the technology but also those that are specific to projected future devices and their uses. Its potential disadvantage is that its ethical assessments is based on forecasts that are to some degree speculative and that may be incorrect. However, to the extent that forecasts can be reliable, a forecasting approach will be able to anticipate many more ethical issues than a mere generic approach would, and would therefore be preferable. In the next two sections, therefore, I will focus on forecasting approaches. I will first look at three contemporary forecasting approaches to the ethics of emerging technology, which I will critically evaluate. In the section thereafter, I will then present my own approach.

Critique of Existing Approaches

In recent years, forecasting approaches to technology ethics have been gaining attention, although few mature approaches currently exist. In what follows I will consider three promising approaches that have been formulated in recent years: ethical technology assessment, the techno-ethical scenarios approach, and the ETICA approach. For each, I will consider their strengths and weaknesses, after which I will draw a general conclusion.

Ethical Technology Assessment

Ethical technology asessesment (eTA), proposed by Palm and Hansson [7], has as its purpose "to provide indicators of negative ethical implications at an early stage of technological development" (p. 543). Such indicators can subsequently be used to guide design or technology policy. The focus of eTA is on the whole life-cycle of technology development, from initial R&D to ultimate impacts on society. To attain an adequate understanding of future developments, eTA relies on studies in technology assessment (TA)

and on close interactions with developers of technology. The interactions with technology developers are to guarantee an adequate understanding of the technology in question. Studies in TA are to provide insight into both the technology in question and its social consequences, and are also used to organize interactions with technology developers in which eTA is made relevant for the development process. The goal of eTA is not to predict far into the future, but rather to continually assess current practices in technology development and provide feedback to designers and policy makers.

The ethical analysis of an emerging technology takes place by confronting projected features of the technology or projected social consequences with ethical concepts and principles. This yields areas in which a conflict may emerge between the technology and one or more accepted moral principles. This ethical knowledge may then be used to adjust design processes to avoid ethical concerns or to steer decision-making on an emerging technology. Palm and Hansson go on to propose an ethical checklist of nine issues to identify the most common ethical issues in emerging technologies. This list contains issues like privacy, sustainability, issues of control, influence and power and issues of gender, minorities and justice. Not all of these issues are ethical in a conventional sense, but all can be framed as ethical issues.

Palm and Hansson's approach is one of the first ethical approaches explicitly targeted at emerging technologies. It does a good job at advocating the need for ethical TA, and then presents an original approach that seems workable and appears to cover a lot of different issues. Still, the approach has a few limitations. Most importantly, it is rather vague in its methodology, as it does not specify in detail what kind of knowledge needs to be acquired from technology developers and from TA and how it should be acquired, and it also does not spell out in detail how ethical analysis can be performed on the basis of this knowledge. In addition, the ethical checklist of nine items seems somewhat limited, as many recognized moral values and principles are not found on the list, such as autonomy, human dignity, informed consent, distributive justice, and so on. So it would seem one would need a much longer list to be able to do comprehensive ethical assessments of new technologies. Even then, moral issues could be into play for a new technology that are not included in the list. To identify such issues, it would seem that exploring moral intuitions of either stakeholders or the analyst would be in order.

The Techno-Ethical Scenarios Approach

The *techno-ethical scenarios approach* of Boenink et al. [2] aims at ethical assessments of emerging technologies that are intended to help policy makers to anticipate ethical controversies regarding emerging technologies. It relies on *scenario analysis*, which is a well-established approach within futures studies. A unique features of the approach is that it aims to anticipate the mutual interaction between technology and morality, and changes in morality that may result from this interaction. Boenink et al. argue that technology may change the way we interpret moral values and may also affect the relative important of particular moral principles. For example, privacy may become a less important principle in an information society where personal information is ubiquitous, and the concept of human responsibility may change in a society in which human decision-making is supported by expert systems. They want to take such changes into account when ethically assessing new technologies, so that new technologies are not evaluated from within a moral system that may not have the same validity by the time an emerging technology has become entrenched in society.

The techno-ethical scenarios approach involves three steps. The first step, "sketching the moral landscape," aims to describe the new technology in question, as well as current moral beliefs, practices and regulations that are directly or indirectly relevant to the technology, and may optionally provide some historical background on the evolution of these beliefs and practices. The second step, "generating potential moral controversies, using NEST-ethics," aims to identify ethical issues and arguments regarding the new technology. This is done using the approach of NEST-ethics [11], which is an approach for identifying ethical issues and arguments in a new technology using a taxonomy of issues and arguments that have been used in past ethical controversies on technology. ("NEST" stands for "New and Emerging Science and Technology".) The NEST-ethics approach performs three tasks. First, it identifies promises and expectations concerning a new technology. Second, it identifies critical objections that may be raised against these promises, for example regarding efficiency and

effectiveness, as well as many conventionally ethical objections, regarding rights, harms and obligations, just distribution, the good life, and others. Third, it identifies chains of arguments and counter-arguments regarding the positive and negative aspects of the technology, which can be used to anticipate how the moral debate on the new technology may develop. During this step, effects of the moral debate on the development of the technology may also be considered. These different steps may involve literature reviews of technologies, promises and expectations, literature reviews of ethical issues, as well as workshops with policy makers and TA experts.

The third step of the techno-ethical scenarios approach, finally, is "constructing closure by judging plausibility of resolutions". In this step, the multitude of views and arguments from step 2 is reduced by imagining which resolution of the debate is the most plausible. The intention is to use steps 1 through 3 to develop a scenario of how the new technology will develop in the future, how this affects the moral landscape (i.e., moral beliefs, practices and regulations), and how moral closure is eventually reached. The particular scenario they develop, for example, considers how developments in molecular medicine may affect existing moral practices concerning medical experiments with human beings. They project several changes in these practices, based on a scenario study set in Dutch society between 2010 and 2030.

The techno-ethical scenarios approach has some obvious advantages over the eTA approach. It takes into account moral change. It moreover takes on a larger time-frame than eTA, which seems to focus on incremental steps. In addition, it identifies not only ethical issues but also complex patterns of argumentation regarding them. Yet, the techno-ethical scenarios approach has an important limitation as well. This is that it is a descriptive and predictive approach, rather than a normative and prescriptive one. It describes moral issues that are likely to emerge as the technology progresses, not ones that ought to emerge from an ethical point of view, and it considers how these are likely to be resolved, not necessarily how they ought to be resolved.

What this approach may miss, as a result, are ethical issues that are unlikely to collect much public attention but that are nevertheless important. As I have argued in earlier work, important moral controversies may remain hidden because of the complexity or opaqueness of technological artifacts or practices [3]. Such controversies are not likely to be included in techno-ethical scenarios. Conversely, moral controversies may ensue that are based on a false or misguided understanding of the technology or its social consequences. Such moral controversies do not present moral issues that ought to be considered in assessing emerging technologies, because they are based on false premises. In addition, moral controversies may ensue that are based on parochial moral concerns that would not be considered in an ordinary ethical analysis. My point is hence that moral controversies that may emerge in public debate may be different from moral issues that may result from thorough ethical assessments, even though there may be a large overlap in practice between the two. The current approach focuses on the former type whereas I think an ethical analysis of emerging technology should primarily focus on the latter, as its aim should not be to predict moral debate but to identify normative ethical issues.

The ETICA Approach

The ETICA approach [9,10] is a recent method for the ethical assessment of emerging information and communication technologies (ICTs).[1] It is so general in scope, however, that nothing prevents its application to other types of technology as well, and it will for this reason be considered as a general approach for the ethical assessment of emerging technology. Thus conceived, the aim of the ETICA approach is to provide comprehensive overviews of ethical issues for emerging technologies that are likely to play out in the medium-term future. The ETICA approach makes use of projections of the future which it derives from futures research. It aims to arrive at a *foresight analysis*, which is a forecasting analysis that considers multiple possible futures, out of which one is chosen as most desirable or important to consider. The ETICA approach relies on multiple futures methods and studies, under the assumption that while individual studies will contain biases and shortcomings, their aggregate use will tend to yield more reliable results.

Ideally the ETICA approach would include doing one's own future studies, as its researchers say. However, in their study of emerging ICT's, limitations in resources limit them to two methods for identifying

[1] See also http://www.etica-project.eu/, especially the deliverables.

ethical issues in emerging technology. The first is to extract ethical issues from texts about particular emerging technologies in which ethical issues are discussed. Such texts include governmental and political sources, scientific sources such as research reports and journal articles, and non-academic sources such as published future visions of companies. The second is to use bibliometric analysis that finds correlations between emerging technologies and ethical values and concepts in a database of texts on ethics of technology in the academic literature.

The results of multiple futures research studies are used to identify a range of projected artifacts and applications for particular emerging technologies, along with capabilities, constraints and social impacts. These data form the basis for ethical analysis. In the first stage of ethical analysis, the identification stage, ethical issues are identified for particular applications, artifacts or technological properties.[2] Most of the ethical values and principles used in this approach are derived from a prior list of ethical issues for ethical evaluation in a European context. The resulting ethical issues are summarized in a *normative issues matrix*, which specifies relevant normative issues in relation to particular emerging technologies and the artifacts and applications that are expected to result from them. For example, an analysis of robots, as an emerging technology, may focus on particular applications such as service robots in households, robots as companions and robots as soldiers, and discuss ethical aspects of each application. The normative issues matrix also contains more general ethical issues with particular technologies that are not bound to particular applications. For example, an analysis of robots may focus on privacy issues in relation to the sensory capabilities of robots, or responsibility issues in relation to the behavioral autonomy of robots, or ethical issues that are specific to humanoid robots.

At a second stage of ethical analysis, the evaluation stage, the ethical issues of the identification stage are subjected to ethical evaluation and are ranked and ordered in relation to each other. In a third and final stage, the governance stage, governance recommendations are developed for policy makers for dealing with the ethical issues described in the earlier stages.

[2] The ETICA project also uses these data to perform social and legal analyses. However, in my discussion I will focus on its use for ethical analysis.

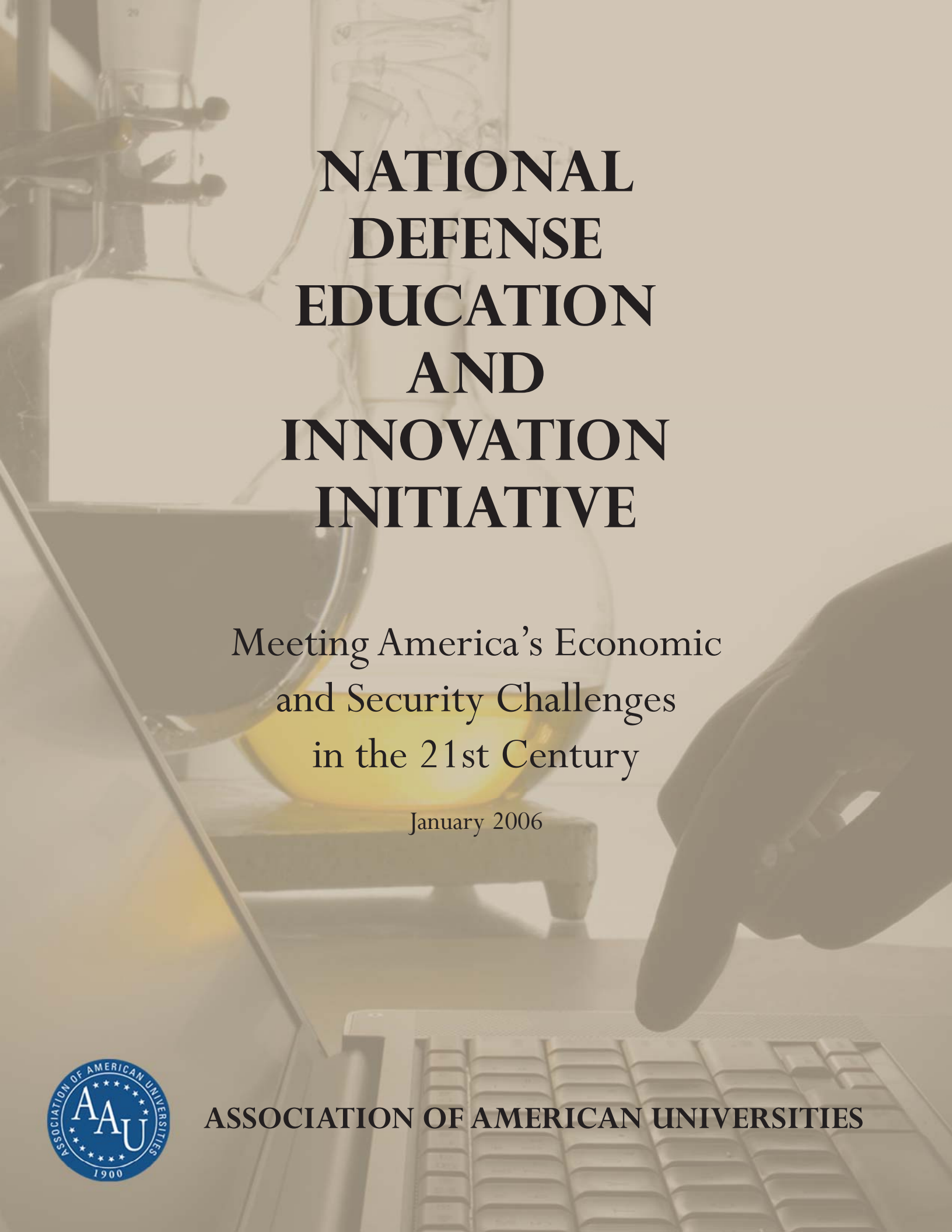
The ETICA approach is possibly the most elaborate ethical approach to emerging technologies that has been developed to date. It aims at thoroughness by considering a wide range of technological properties, artifacts, applications, and ethical issues. It also engages in ethical evaluation and develops recommendations for governance. And it aims to make use of state-of-the-art work in futures studies. Yet, the approach also has weaknesses. First, its claim to adopt a futures studies approach is somewhat dubious. The main sources of the ETICA approach for locating ethical issues are government and political texts, scientific texts, and non-academic texts. Many of the non-academic and government texts will not be based on scientific methods of futures research. Moreover, many of the scientific texts do not seem to be either. Judging from the literature references in the ETICA projects, many of these texts come from ethics and computer science journals, and most of them do not use methods of futures research.

Second, its assumption that "the overall discourse on future[s] technologies provides as good and reliable an understanding of the future as will be possible to achieve" ([10], p. 9) is also dubious. Rather than merely aggregating predictions about new technologies, it would be better if the approach would provide independent critical assessments of such predictions and the methods used for arriving at them before such predictions are used as a basis for subsequent ethical analysis. It should be granted, though, that in the ETICA project some independent foresight research is undertaken to validate some of the predictions that are made. Third and finally, many of the ethical analysis undertaken in the ETICA project appear to refer to generic properties of the technologies that are studied. In the project these are called "ethical issues stemming from the defining features of the technology" ([6], p. 27). The range of artifacts and implications that is considered is often somewhat limited, and elaborate descriptions of possible artifacts and applications are often missing. For example, in the ethical analysis of robotics, most space goes to the consideration of generic ethical issues, and only a few types of robots and application areas of robotics are considered in detail.

Conclusion

My review of the three approaches has revealed strong and weak points in each approach. It has also brought

forward various points to consider in an ethics of emerging technologies. A first point is through what approaches and methods technological forecasts are arrived at. The three approaches use various approaches from futures studies and technology assessment, including approaches developed as part of their own approach. A second point concerns the use of ethics and the identification and evaluation of ethical issues. How should this be done? Here, the three approaches also have different answers, though what they have in common is their drive to identify possible ethical issues or controversies and their heuristic use of ethical checklists in doing so. A final point, which has been more implicit in the discussion, concerns the question what an ethics of emerging technology actually studies: is it whole technologies and techniques, is it possible future artifacts, is it uses of artifacts, social consequences, or yet something else? To this question, also, the three approaches give different answers. These three points for an ethics of emerging technologies provide a good challenge to build and improve on the three approaches discussed above. That is what I will turn to in the next section.



NATIONAL DEFENSE EDUCATION AND INNOVATION INITIATIVE

Meeting America's Economic and Security Challenges in the 21st Century

January 2006

ASSOCIATION OF AMERICAN UNIVERSITIES

ASSOCIATION OF AMERICAN UNIVERSITIES

The **Association of American Universities** (AAU), founded in 1900, is an association of 60 leading U.S. public and private research universities and two top Canadian universities. While AAU universities comprise only about 1.5 percent of all U.S. colleges and universities, they educate annually over one million (approximately nine percent) of the nation's undergraduates and over 450,000 (approximately 20 percent) of the nation's graduate and professional students.

AAU universities award just over one-half of all U.S. doctoral degrees and 55 percent of all Ph.D.s in sciences and engineering. AAU members perform nearly 60 percent of the university research funded by the federal government. The federal investment in research at AAU universities totaled nearly $13 billion in FY2002.

AAU provides a forum for the development and implementation of institutional and national policies promoting strong programs in university research and scholarship and undergraduate, graduate, and professional education. It supports its members' advocacy of national policies in these areas.

Brandeis University
Brown University
California Institute of Technology
Carnegie Mellon University
Case Western Reserve University
Columbia University
Cornell University
Duke University
Emory University
Harvard University
Indiana University
Iowa State University
The Johns Hopkins University
Massachusetts Institute of Technology
McGill University
Michigan State University
New York University
Northwestern University
The Ohio State University
The Pennsylvania State University
Princeton University
Purdue University
Rice University
Rutgers, The State University of New Jersey
Stanford University
Stony Brook University-
State University of New York
Syracuse University
Texas A&M University
Tulane University
University at Buffalo, The State University of New York
The University of Arizona
University of California, Berkeley
University of California, Davis
University of California, Irvine
University of California, Los Angeles
University of California, San Diego
University of California, Santa Barbara
University of Chicago
University of Colorado at Boulder
University of Florida
University of Illinois at Urbana-Champaign
University of Iowa
University of Kansas
University of Maryland, College Park
University of Michigan
University of Minnesota, Twin Cities
University of Missouri, Columbia
University of Nebraska-Lincoln
University of North Carolina at Chapel Hill
University of Oregon
University of Pennsylvania
University of Pittsburgh
University of Rochester
University of Southern California
University of Texas at Austin
University of Toronto
University of Virginia
University of Washington
University of Wisconsin-Madison
Vanderbilt University
Washington University in St. Louis
Yale University

NATIONAL DEFENSE EDUCATION AND INNOVATION INITIATIVE

MEETING AMERICA'S ECONOMIC AND SECURITY CHALLENGES IN THE 21st CENTURY CENTURY

January 2006

ASSOCIATION OF AMERICAN UNIVERSITIES

"[T]he inadequacies of our systems of research and education pose a greater threat to U.S. national security over the next quarter century than any potential conventional war that we might imagine."

— Hart-Rudman Commission on National Security, Road Map for National Security: Imperative for Change, 2001.

INTRODUCTION

Introduction

The United States has exercised global leadership in economic and security matters for more than 50 years, and the American people have experienced extraordinary security and economic progress as a result.

But in this still-young century, the nation faces new challenges to both our security and our prosperity: the danger to our national and homeland security posed by terrorism, the increasing competitive pressure from the growing economies of Asia and elsewhere, and the threat to our economic and national security posed by dependence on Middle East oil. These challenges demand a dramatic, creative response.

[T]HE BURDEN OF MEETING THESE CHALLENGES IS NOT GOVERNMENT'S ALONE . . . RESEARCH UNIVERSITIES AND HIGHER EDUCATION IN GENERAL HAVE KEY ROLES TO PLAY.

Yet they come at a time when the continuous innovation that has been the hallmark of America's economic success and military prowess is threatened at its very foundation. Serious problems in our educational system and a weakening federal commitment to research in the physical sciences and engineering are eroding the nation's innovative edge, with increasingly evident and alarming results.

Nearly 50 years ago, faced with similar challenges following the launch of Sputnik by the Soviet Union, America responded by enacting the National Defense Education Act and by multiplying the nation's investment in university-based research. The Association of American Universities (AAU) believes that today's challenges demand a comparable response.

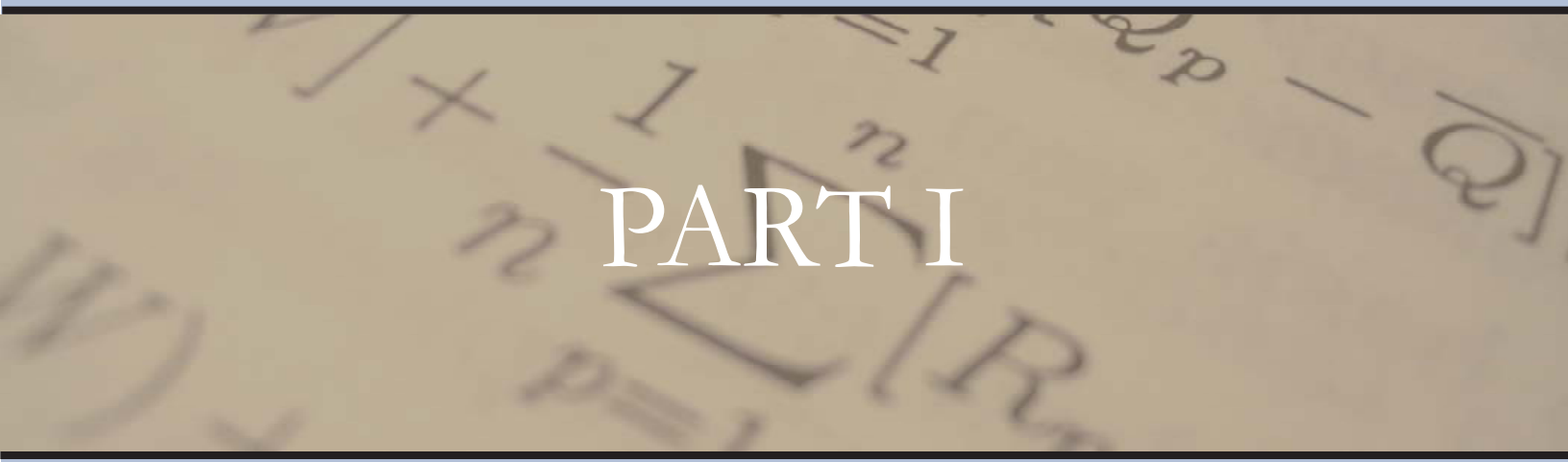
In that spirit, AAU calls on the Administration, Congress, and academia, with the help of the business sector, to implement a 21st Century National Defense Education and Innovation Initiative aimed at meeting the economic and security challenges we will face over the next half-century. Government and America's universities and colleges should implement this initiative now, so that it can be fully in place by 2008 – the 50th anniversary of the National Defense Education Act (NDEA) of 1958.

The Initiative springs from a belief among AAU universities that the burden of meeting these challenges is not government's alone and that research universities and higher education have key roles to play. It therefore calls for action and resources – and change – not only from government but also from the nation's colleges and universities. It also reflects a strong belief that, if we take the right actions, America can maintain its global leadership and that we can ensure our national and economic security for the 21st Century.

This report is in three parts. The first highlights the most significant recommendations contained in the Initiative. The second is a narrative that lays out the challenges, historical background, and a broad description of the Initiative. The third section of the report provides a detailed list of recommendations.

"One thing is certain. Our competitors will not wait for us to come to our senses - they will continue to fuel the changes in education and infrastructure required to spark innovation."

— Craig Barrett
CEO, Intel Corporation
Wall Street Journal
March 4, 2004



PART I

National Defense Education and Innovation Initiative:

Meeting America's Economic and Security Challenges in the 21st Century

HIGHLIGHTS

Objectives of the Initiative

- Enhance America's research capacity in order to sustain scientific and technical innovation.
- Cultivate American talent to enhance the nation's math, science, engineering, and foreign language expertise.
- Continue to attract and retain the best and brightest international students, scientists, engineers, and scholars.

Key Recommendations for Universities and Colleges

Enhance Research and Innovation

- Strengthen the connections between campus-based research and undergraduate education.
- Establish interdisciplinary research and education initiatives that create new combinations of faculty, postdocs, and graduate and undergraduate students to address emerging national challenges.
- Provide top young scientists and engineers – postdoctoral fellows (postdocs) and junior faculty – with independent research opportunities and funding to encourage novel thinking and research.

Cultivate American Talent

- Identify and promote best practices and programs in undergraduate STEM (science, technology, engineering, and mathematics) and foreign language education, especially those that address college freshman attrition and under-representation of minorities and women in STEM fields.
- Continue reexamination of doctoral education, particularly in STEM and language disciplines, to develop ways to shorten time to degree, improve completion rates, and broaden the scope of Ph.D. education.
- Continue to establish and build on professional science masters programs that meet specific science and technical managerial workforce needs identified by the federal government, business, and industry.
- Provide more university research experiences for those training to be K-12 math and science teachers, and for current teachers.
- Create accelerated teacher certification programs for individuals with STEM, foreign language, or area studies expertise.
- Create and sustain stronger partnerships with school districts, state departments of education, and business that focus on training and retraining K-12 teachers to fill the current teacher skills and knowledge gaps in STEM and foreign language education.

Attract and Retain Foreign Talent

- Continue to work with Congress and the Administration to combat the misperception that international students, scholars, scientists, and engineers are no longer welcome in the U.S.
- Continue to work with the Departments of State and Homeland Security to improve the visa process so that bona fide international students, scholars, scientists, and engineers can enter the U.S. in a secure, timely, and efficient manner.

National Defense Education and Innovation Initiative:
Meeting America's Economic and Security Challenges in the 21st Century

Key Recommendations for Government

Enhance Research and Innovation

- Increase federal investment in basic research supported by the NSF, NASA, and the Departments of Energy, Defense, Homeland Security, and Commerce by 10 percent annually for the next seven years placing particular emphasis upon growing federal support for the physical sciences and engineering. Grow investment thereafter to continue driving innovation.

- Sustain basic medical science funding at historical rates of growth to preserve the biomedical research capacity made possible by the recent doubling of the National Institutes of Health (NIH) budget.

- Strengthen federal support for research infrastructure by reinvigorating competitive facilities and equipment programs at NIH and the National Science Foundation (NSF), adequately funding the Department of Energy's 20-year facilities plan, and examining policy changes to strengthen federal support for scientific infrastructure at universities.

Cultivate American Talent

- Increase by 5,000 the number of graduate fellowships and traineeships supported by existing programs at federal science and education agencies, including NSF, NIH, National Aeronautics and Space Administration (NASA), and the Departments of Defense (DOD), Homeland Security (DHS), Energy (DOE), and Education.

- Create a graduate fellowship and traineeship program in the DOE Office of Science that supports 1,000 students annually and that generates talent to help achieve energy self-sufficiency and to enhance the nation's scientific enterprise.

- Expand the DOD National Defense Education Program, which provides scholarships and fellowships to students in critical fields of science, mathematics, and engineering in return for a commitment of national service after their studies.

- Increase federal need-based student aid, especially Pell Grants, to make college possible for the neediest students.

- Build on the Administration's National Security Language Initiative by expanding federal foreign language, area studies, and study abroad programs.

- Revive the NDEA K-12 teacher skills summer workshops to help teachers of math, science, and foreign languages improve their teaching skills and meet teaching standards.

- Improve education research and K-12 education by creating: 1) a competitively awarded extramural grant program in the Institute of Education Sciences at the Department of Education that funds high-quality research on K-12 education and 2) a new graduate fellowship program that supports 500 students per year pursuing Ph.D.s in math and science education.

- Establish a new mentoring and tutoring program in which college students earn a stipend for tutoring K-12 students in STEM and foreign language coursework.

Attract and Retain Foreign Talent

- Reform immigration policies to create clear pathways to permanent residency and U.S. citizenship for top international students who earn U.S. degrees, as well as outstanding scientists and engineers in the U.S. on exchange or work visas.

- Ensure that government policies and contracting practices do not discriminate against or curtail participation by international students and scientists in the conduct of unclassified fundamental research.

The Role of Business

The federal government and universities have a historic relationship in addressing national security and economic challenges through education and research. However, businesses and the business community also have critical roles to play in helping to strengthen our nation's education and research systems. They can contribute significantly by:

- Continuing their individual and collective efforts to educate the public and state and federal decision-makers about the challenges to American competitiveness and security and the need for this type of initiative;
- Identifying and communicating workforce education and training needs and helping to create opportunities to address those needs through partnerships with educational and philanthropic institutions, the federal government, and local and state governments; and
- Increasing participation in partnerships to address the education and research challenges facing our nation.

". . . if trends in U.S. research and education continue, our nation will squander its economic leadership, and the result will be a lower standard of living for the American people. . . . The good news is that America is able to meet these challenges from a position of economic strength."

— Statement of National Summit on Competitiveness: Investing in Innovation, December 2005

CONCLUSION

Conclusion: A Uniquely American Response

AAU member universities are encouraged by other organizations and individuals who have come forward with ideas to meet the challenges facing our nation. The time to act is now. We as a nation must commit to specific solutions.

Orienting American society to the challenges that lie ahead will not be an easy task. It will take serious commitments of university resources and significant federal expenditures. However, as numerous business organizations have pointed out, these are investments that will produce reliable returns that benefit our society. For any of the major actors – universities, business, and government – to look to others to solve these problems without looking first to themselves is to invite failure. American society has never operated by command. Ours is a culture of self-initiative and problem solving. Our greatest successes have been the product of competitive effort accompanied by collaboration. In this way we have met great national challenges that were beyond the reach of any single individual or sector of society.

OUR GREATEST SUCCESSES HAVE BEEN THE PRODUCT OF COMPETITIVE EFFORT ACCOMPANIED BY COLLABORATION.

As an organization of research universities, AAU believes it must focus on its responsibilities to contribute to American competitiveness and security by doing better what only we can do, namely improve education and research. The recommendations AAU offers specifically outline the contributions universities can and should make. We believe that government and business also have important responsibilities. We stand prepared to do our part. We will work with the federal government, business, and the nonprofit sector to maintain and enhance America's leadership position in the world.

It is our hope that this paper, along with the recent reports issued by a host of business, academic, and other organizations, will convince the Administration, Congress, and the American people that our national and economic security – indeed our global leadership – depend on education and innovation. Both of these objectives rely on a new national commitment in the form of a National Defense Education and Innovation Initiative for the 21st Century.

KEEPING SECRETS IN THE CAMPUS LAB: LAW, VALUES AND RULES OF ENGAGEMENT FOR INDUSTRY-UNIVERSITY R&D PARTNERSHIPS

Joshua A. Newberg[*]
Richard L. Dunn[**]

Over the last two decades, the role of private industry in university research has expanded dramatically throughout much of the industrialized world.[1] In the United States, technology transfer

---

[*] Assistant Professor, Robert H. Smith School of Business, University of Maryland.
[**] Visiting Scholar, Robert H. Smith School of Business, on leave from the Defense Advanced Research Projects Agency.

[1] On the subject of industry-university research collaboration outside of the United States, see, for example, TECHNOLOGY TRANSFER SYSTEMS IN THE UNITED STATES AND GERMANY: LESSONS AND PERSPECTIVES (H. Norman Abramson et al. eds., 1997); Jason Boyarski et al., *Japan Promotes University Technology Licensing*, 12 INTELL. PROP. & TECH. L.J. 28 (2000); Steven Collins & Hikoji Wakoh, *Universities and Technology Transfer in Japan: Recent Reforms in Historical Perspective*, 25 J. TECH. TRANSFER 213 (2000); Yannis Caloghirou et al., *University-Industry Cooperation in the Context of the European Framework Programmes*, 26 J. TECH. TRANSFER 153 (2001) ("The importance of university-industry collaboration has generally increased in the industrialized world since the late 1970s."); Stephen J. Franklin et al., *Academic and Surrogate Entrepreneurs in University Spin-out Companies*, 26 J. TECH. TRANSFER 127 (2001) (examining university spin-off companies in the United Kingdom); Razak Grady & John Pratt, *The UK Technology Transfer System: Calls for Stronger Links Between Higher Education and*

through industry-university research collaboration ("IURC") is ubiquitous and actively encouraged both by university administrators and an array of federal and state government policies.[2] Supporters credit such collaborations with significantly enhancing the technological capacity and economic competitiveness of U.S. firms,[3] encouraging the commercialization of advanced university-generated technology,[4] and helping to underwrite the costs of conducting state-

---

Industry, 25 J. TECH. TRANSFER 205 (2000); Douglas H. McQueen & J.T. Wallmark, *University Technical Innovation: Spin-offs and Patents in Goteborg, Sweden, in* UNIVERSITY SPIN-OFF COMPANIES: ECONOMIC DEVELOPMENT, FACULTY ENTREPRENEURS, AND TECHNOLOGY TRANSFER 103 (Alistair M. Brett et al. eds., 1990); Ofer Meseri & Shlomo Maital, *A Survey Analysis of University Technology Transfer in Israel: Evaluation of Projects and Determinants of Success,* 26 J. TECH. TRANSFER 115 (2001); P. O'Brien et al., *University-Industry Strategic Alliance: A British Perspective, in* CHEMICAL SCIENCES ROUNDTABLE, RESEARCH TEAMS AND PARTNERSHIPS: TRENDS IN THE CHEMICAL SCIENCES 28 (1999); Ray Rothwell, *Technology Policy and Collaborative Research in Europe, in* COLLABORATIVE RESEARCH AND DEVELOPMENT: THE INDUSTRY-UNIVERSITY-GOVERNMENT RELATIONSHIP 85 (Albert N. Link & Gregory Tassey eds., 1989).

[2] *See generally* GOVERNMENT-UNIVERSITY-INDUSTRY RESEARCH ROUNDTABLE (GUIRR), OVERCOMING BARRIERS TO COLLABORATIVE RESEARCH 5 (1999) [hereinafter GUIRR, OVERCOMING BARRIERS] (noting that "university-industry research collaboration is becoming more frequent and extensive" in the United States); David Blumenthal et al., *Relationships Between Academic Institutions and Industry in the Life Sciences – An Industry Survey,* 334 NEW ENG. J. MED. 368, 369 (1996) [hereinafter Blumenthal et al., *Industry Survey*] (reporting that "over 90% of life-sciences companies in the United States had some relationship with academia" and that more than half supported university research).

[3] *See, e.g.*, COUNCIL ON COMPETITIVENESS, ENDLESS FRONTIER, LIMITED RESOURCES: U.S. R&D POLICY FOR COMPETITIVENESS 3 (1996) (arguing that "R&D partnerships," including IUCR, "hold the key" to "future U.S. economic competitiveness"); Evan W. Berman, *The Economic Impact of Industry-Funded University R&D,* 19 RES. POL'Y 349, 353-54 (1990) (empirical study concluding that industry funding of university research leads to increased overall industry investment in R&D); Michael R. Ward & David Dranove, *The Vertical Chain of Research and Development in the Pharmaceutical Industry,* 33 ECON. INQUIRY 70 (1995) (empirical study quantifying contribution of "basic" university research to the pharmaceutical industry); Lynne G. Zucker et al., *Intellectual Human Capital and the Birth of U.S. Biotechnology Enterprises,* 88 AM. ECON. REV. 290 (1998) (empirical study substantially attributing rise of U.S. biotechnology industry to industry-university research collaborations).

[4] *See, e.g.,* Richard Jensen & Marie Thursby, Proofs and Prototypes for Sale: The Tale of University Licensing 3 (Nat'l Bureau of Econ. Research, Working Paper No. 6698, 1998) (survey concluding that "most university inventions could not be developed independently by either the inventor or the firm"); Gina A. Kuhlman, Comment, *Alliances for the Future: Cultivating a Cooperative Environment for Biotech Success,* 11 BERKELEY TECH. L.J. 311, 344-48 (1996) (detailing social and economic benefits of IUCR in biotechnology industry); *see also* Jeff Gerth & Sheryl Gay Stolberg, *Medicine Merchants: Birth of a Blockbuster,* N.Y. TIMES, Apr.

of-the-art university research.[5] On the other side of the debate, critics of IURC argue that the commercial objectives and interests of private firms are fundamentally inconsistent with the academic values of the university,[6] and that the policies that have been implemented to encourage industry-university research collaboration compromise and undermine the academic mission of the nation's institutions of higher learning.[7]

The task of critically evaluating industry-university research collaboration is complicated by the fact that the term encompasses a

---

23, 2000, at A1 (reporting on commercialization of "blockbuster" glaucoma treatment invented at Columbia University and developed by Pharmacia Corporation).

[5] *See generally* Thomas A. Massaro, *Innovation, Technology Transfer, and Patent Policy: The University Contribution,* 82 VA. L. REV. 1729, 1734 (1996) (noting that revenue from inventions arising from industry-university collaboration has supported university medical research for which funding from other sources has not been available).

[6] *See, e.g.*, Charles C. Caldart, *Industry Investment in University Research,* 8 SCI. TECH. & HUM. VALUES 24, 30-31 (positing a fundamental antithesis between the "proper functions of universities" and "the profit motive" and opposing industry-university research collaboration); Rebecca S. Eisenberg, *Academic Freedom and Academic Values in Sponsored Research,* 66 TEX. L. REV. 1363, 1375-77 (1988) [hereinafter Eisenberg, *Academic Freedom*] (arguing that industry-sponsored university research threatens "academic values" by imposing secrecy requirements, creating incentives "for academic researchers to distort their viewpoints . . . in order to please their research sponsors," and distorting "the academic research agenda in favor of research for which funding is available"); Arti Kaur Rai, *Regulating Scientific Research: Intellectual Property Rights and the Norms of Science,* 94 NW. U. L. REV. 77, 90-94, 110-15 (1999) (positing conflict between norms of science favoring public disclosure of scientific knowledge and commercial norms favoring secrecy and proprietary rights in such knowledge).

[7] *See, e.g.*, Wesley M. Cohen et al., *Industry and the Academy: Uneasy Partners in the Cause of Technological Advance, in* CHALLENGES TO RESEARCH UNIVERSITIES 171, 193-94 (Roger G. Noll ed., 1998) (advocating policy changes to prevent IUCR from undermining the public dissemination of university research); Irwin Feller, *Universities as Engines of R&D-Based Economic Growth: They Think They Can,* 19 RES. POL'Y 335, 343-44 (1990) (opposing IUCR directed toward commercialization of university research, in part, because such collaboration is incompatible with the core activities and norms of academic research); William J. Broad, *As Science Moves Into Commerce, Openness Is Lost,* N.Y. TIMES, May 24, 1988, at C1; Colleen Cordes, *A Quiet Debate Emerges: Can a College's Financial Ties Skew Research Backed by U.S.?,* CHRON. HIGHER EDUC., Jan. 20, 1993, at A22 [hereinafter Cordes, *A Quiet Debate Emerges*]; Colleen Cordes, *Debate Flares Over Growing Pressures on Academe for Ties With Industry,* CHRON. HIGHER EDUC., Sept. 16, 1992, at A26; Richard Florida, *The Role of the University: Leveraging Talent, Not Technology,* ISSUES SCI. & TECH. ONLINE, *at* http://www.nap.edu/issues/15.4/florida.htm (1999) (arguing that IURC secrecy and emphasis on applied research compromises universities' primary missions of disseminating knowledge and cultivating academic talent); *see also* Julie L. Nicklin, *University Deals With Drug Companies Raise Concerns Over Autonomy, Secrecy,* CHRON. HIGHER EDUC., Mar. 24, 1993, at A25.

very broad range of organizational forms and institutional mechanisms for ordering such relationships.[8] And while there has been considerable research and commentary on the subject of IURC, much of the literature focuses on a few policy "inputs"—for example, public laws governing federal funding priorities and intellectual property rights—and quantifiable "outputs" of collaborative research arrangements, such as inventions patented, licenses granted, and royalties collected.[9] As important as these factors are, a critical assessment of IURC also requires an understanding of the actual institutional structures and rules governing industry-university research collaboration.[10] It is, after all, in the organizational structures

---

[8] *See generally* INNOVATIVE MODELS FOR UNIVERSITY RESEARCH (C.R. Haden & J.R. Brink eds., 1992); David C. Mowery, *Collaborative R&D: How Effective Is It?,* ISSUES SCI. & TECH. ONLINE, *at* http://www.nap.edu/issues/15.1/mowery.htm (Fall 1998) ("R&D collaboration covers a diverse array of programs, projects, and institutional actors.").

[9] *See, e.g.,* Rebecca S. Eisenberg, *Public Research and Private Development: Patents and Technology Transfer in Government-Sponsored Research,* 82 VA. L. REV. 1663 (1996) [hereinafter Eisenberg, *Public Research and Private Development*]; Brett Frischmann, *Innovation and Institutions: Rethinking the Economics of U.S. Science and Technology Policy,* 24 VT. L. REV. 347 (2000) (critiquing the Bayh-Dole Act of 1980 and related federal technology transfer policies); Peter Mikhail, Note, Hopkins v. Cellpro: *An Illustration That Patenting and Exclusive Licensing of Fundamental Science is not Always in the Public Interest,* 13 HARV. J.L. & TECH. 375 (2000) (same); Rai, *supra* note 6, at 110-35 (same); *see also* Rebecca S. Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research,* 97 YALE L.J. 177 (1987) [hereinafter Eisenberg, *Proprietary Rights*] (exploring the relationship between commercially-valuable biotechnology research and different forms of intellectual property); Irwin Feller & David Roessner, *What Does Industry Expect From University Partnerships,* XII(1) ISSUES SCI. & TECH. 80 (1995) (presenting survey data suggesting that limited focus on quantifiable "outputs" tends to understate the value of industry-university collaboration to private firms).

[10] *See generally* GUIRR, OVERCOMING BARRIERS, *supra* note 2, at 7 (observing that "further study . . . on the way universities successfully structure technology transfer operations would be useful"); David Blumenthal, *Academic-Industry Relationships in the Life Sciences,* 268 JAMA 3344, 3347 (1992) (noting lack of data regarding "scope, consequences, and management" of industry-university collaborations). Notable exceptions in the literature to the typical focus on federal policy "inputs" and quantifiable "outputs" include D. Fennell Evans & Matthew V. Tirrell, *Research Teams at Universities: The Center for Interfacial Engineering, in* CHEMICAL SCIENCES ROUNDTABLE, RESEARCH TEAMS AND PARTNERSHIPS: TRENDS IN THE CHEMICAL SCIENCES 42 (1999); Todd R. La Porte, *Diluting Public Patrimony or Inventive Response to Increasing Knowledge Asymmetries: Reflections on the University of California, Berkeley-Novartis Agreement, in* NAT'L RES. COUNCIL, CHEMICAL SCIENCES ROUNDTABLE, RESEARCH TEAMS AND PARTNERSHIPS: TRENDS IN THE CHEMICAL SCIENCES 66 (1999); Gary Rhoades & Sheila Slaughter, *Professors, Administrators, and Patents: The Negotiation of Technology Transfer,* 64 SOC. EDUC. 65 (1991) (analyzing the development of technology transfer policies at a major research university).

and institutional rules of research collaboration that universities and private firms address, albeit selectively and imperfectly, the crucial matters of assigning rights and responsibilities regarding inventions and discoveries, allocating the benefits and burdens of collaborative research, and reconciling the different concerns, constraints, and objectives of IURC participants. Thus the structures of industry-university research collaboration reflect the complex interaction of the forces that principally shape such ventures: (1) public and private law; (2) university policies, values, and interests;[11] and (3) the commercial values and interests of private firms.

In this paper, we examine rules and organizational forms for structuring industry-university partnerships, with a focus on the problem of protecting confidential information in the context of IURC. The basic question that informs our consideration of IURC confidential information policies may be stated as follows: Can the academic ethos of open inquiry be reconciled with the interests of private firms in appropriating the value of information by restricting its diffusion? We conclude that arrangements can be crafted to accommodate substantially both sets of concerns and thus to secure the benefits of IURC without imposing prohibitive costs on either side of the industry-university partnership.

---

[11] The phrase "*university* policies, values, and interests" is employed here as a shorthand for the values and interests of the university community as a whole. We acknowledge, however, that the values and interests of administrators, faculty and other university stakeholders often diverge in practice.

B. Evolving Role of University Research and the Challenges of Collaboration

In the environment that has been shaped by the legal and economic developments of the 1980s, the role of the research university in the national innovation system has changed significantly.[31] Universities now patent far more technology than they did a generation ago: The number of patents issued to U.S. universities has risen from approximately 250 each year in the early 1970s[32] to 3079 in 1999.[33] Concurrently, transfer of university-generated technology to the private sector, through licensing, start-up companies, and other forms of industry-university R&D collaboration, has also substantially

---

[29] The government retained a royalty-free license to practice, or have practiced on its behalf, the invention made or "first actually reduced to practice" with government support. 35 U.S.C. § 202 (2000).

[30] *See generally* CONGRESSIONAL RESEARCH SERVICE, AN EXAMINATION OF THE ISSUES SURROUNDING BIOTECHNOLOGY PATENTING AND ITS EFFECT UPON ENTREPRENEURIAL COMPANIES (2000) (reviewing legal developments regarding patentability of biotechnology inventions); Rai, *supra* note 6, at 100-104 (reviewing the expansion and strengthening of patent rights under the decisions of the Supreme Court and the U.S. Court of Appeals for the Federal Circuit beginning in 1980); Lawrence Schlam, *Compulsory Royalty-Free Licensing as an Antitrust Remedy for Patent Fraud: Law, Policy and the Patent-Antitrust Interface Revisited,* 7 CORNELL J.L. & PUB. POL'Y. 467, 473 (1998) (noting that the Federal Circuit affirmed district court decisions finding patents valid 89% of the time from 1982 through 1987, compared with 30-40% affirmance rates before the establishment of the Court of Appeals for the Federal Circuit).

[31] For a useful survey of the role of U.S. research universities since the Second World War, see ROGER L. GEIGER, RESEARCH AND RELEVANT KNOWLEDGE: AMERICAN RESEARCH UNIVERSITIES SINCE WORLD WAR II (1993).

[32] SCIENCE & ENGINEERING INDICATORS 2000, *supra* note 16, 6-56.

[33] ASS'N OF UNIV. TECH. MANAGERS, AUTM LICENSING SURVEY: FY 1999 SURVEY SUMMARY at 2, 34 (2000) [hereinafter AUTM SURVEY].

increased, particularly in research-intensive industries such as biotechnology, information technology, and pharmaceuticals.[34]

These developments have created new opportunities for universities while also giving rise to tensions and ambiguities regarding the role of the university in society. On the one hand, universities are, with relatively few exceptions, public or non-profit institutions dedicated principally to education and academic research. On the other hand, universities have become important commercial actors in markets for technology.[35] Although universities continue to generate a vast amounts of research that is not at all connected to industry-university partnerships, a significant share of university research is now developed in collaborative relationships wherein universities have become – to varying degrees and in many different forms – the business partners of private firms. For universities, the potential benefits of such partnerships include: (1) access to industry resources including financial support and advanced technology; (2) superior training and placement opportunities for students; (3) the stimulation of exposure to current industry problems; and (4) income from commercially valuable inventions.[36] For industry, such partnerships can offer: (1) access to advanced academic research, expertise, and prestige; and (2) opportunities for recruiting highly-qualified students.[37] For society as a whole, IURC collaboration can generate

---

[34] *See id.;* SCIENCE & ENGINEERING INDICATORS 2000, *supra* note 16, 6-56–6-58.

[35] *See generally* Derek Bok, *Universities: Their Temptations and Tensions,* 18 J. C. & U.L. 1, 14-19 (1992) (discussing the emergence of the "commercialized university"); Kenneth W. Dam, Intellectual Property and the Academic Enterprise 2 (Univ. of Chicago John M. Olin Law & Econ. Working Paper, No. 68, 1999), *available at* http://www.law.uchicago.edu/Publications/Working/index.html (arguing that U.S. research universities "have become, at least in some areas of science and technology, economic enterprises as well as centers for teaching and research").

[36] For discussion of the benefits of IURC for universities, see generally COUNCIL ON GOV'T RELATIONS: A REVIEW OF INDUSTRY-UNIVERSITY RESEARCH RELATIONSHIPS (1996), *available at* http://www.cogr.edu/ [hereinafter COGR, REVIEW] (noting, *inter alia*, that IURC enhances graduate education and increases academia's awareness of industry problems).

[37] For discussion of the benefits of IURC for industry, see generally Jerome H. Grossman et al., *Contributions of Academic Research to Industrial Performance in Five Industry Sectors,* 26 J. TECH. TRANSFER 143 (2001) (reviewing benefits of various forms in industry-university collaboration in the aerospace, financial services, medical devices, network systems and communications, and transportation, distribution, and logistics services); COGR, REVIEW, *supra* note 36 (noting, *inter alia*, that IURC provides industry with access to basic research and

jobs and other forms of economic development,[38] as well as improved products, such as advanced pharmaceuticals and medical technologies.[39]

While the potential benefits are enormous, entering into collaborative research and development relationships with industry partners is not without risks and costs for universities. Thus the establishment of effective legal and institutional structures for such collaboration presents a complex set of challenges. At the risk of some oversimplification, these challenges may be summarized for analytical purposes

---

offers "a means of monitoring new developments in science and technology"); Richard Zeckhauser, *The Challenge of Contracting for Technological Information,* 93 PROC. NAT'L ACAD. SCI. USA 12,743, 12,746 (1996) ("Companies sponsor university research and receive in return subtle information about what fields and researchers are promising and on what types of technologies might prove feasible.").

[38] *See, e.g.*, BANKBOSTON, MIT: THE IMPACT OF INNOVATION 2 (1997) (estimating that in 1997, companies founded by MIT faculty and graduates employed 1.1 million people and accounted for $232 billion annually in sales worldwide); Berman, *supra* note 3; Douglas W. Jamison & Christina Jansen, *Technology Transfer and Economic Growth,* 12 J. ASS'N U. TECH. MANAGERS (2000), *available at* http://www.autm.net/pubs/journal/00/techtransfer.html (arguing that "federal programs -- such as the Bayh-Dole Act of 1980 -- that increase the pay-off from research and development funding (R&D), can be effective agents of economic growth."); Peter B. Kramer et al., *Induced Investments and Jobs Produced by Exclusive Patent Licenses – A Confirmatory Study,* 9 J. ASS'N U. TECH. MANAGERS (1997), *available at,* http://www.autm.net/pubs/journal/97/5-97.html (estimating that exclusive licenses of university patents induced $4.6 billion in private investment and created 27,000 research & development jobs); James D. Adams et al., Industry-University Cooperative Research Centers (Nat'l Bureau of Econ. Research, Working Paper No. 7843, 2000) (finding that industry-university cooperative research centers contribute to increased patenting and research expenditures by industrial laboratories).

[39] *See generally* NATHAN ROSENBERG ET AL., SOURCES OF MEDICAL TECHNOLOGY: UNIVERSITIES AND INDUSTRY (1995); Kuhlman, *supra* note 4 (IURC role in establishing and sustaining the biotechnology industry); Donald G. Rea & Harvey Brooks, *The Semiconductor Industry – Model for Industry/University/Government Cooperation,* 40 RES. TECH. MGMT. 46 (1997); Lucien P. Randazzese, *Exploring University-Industry Technology Transfer of CAD Technology,* 43 IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS) TRANSACTIONS ON ENGINEERING MGMT. 393 (1996); Ward & Dranove, *supra* note 3 (reviewing the contributions of university research to the pharmaceutical industry); Zucker et al., *supra* note 3 (IURC role in establishing and sustaining the biotechnology industry); *see also* Edwin Mansfield, *Academic Research Underlying Industrial Innovations: Sources, Characteristics, and Financing,* 77 REV. ECON. & STAT. 55 (1995); Edwin Mansfield, *Academic Research and Industrial Innovation,* 20 RES. POL'Y 1 (1990); Nathan Rosenberg & Richard R. Nelson, *American Universities and Technical Advance in Industry,* 23 RES. POL'Y 323 (1994) (noting the contributions of basic academic research to industrial development).

as follows: The first and perhaps most fundamental challenge is to structure collaborative relationships to allow universities to maintain control over the research agenda.[40] In this context, control over the university research agenda means that the university's decision to enter into industry-university collaborative relationships is principally based on its independent judgment that the questions to be pursued have intellectual merit, as opposed to entering into collaborations based on other considerations.[41] The second broad challenge is to allocate the benefits and burdens of industry-university collaboration to accommodate the sometimes conflicting goals of furthering the university's core academic mission, while offering sufficient economic incentives to all participants.[42] This second challenge subsumes decisions regarding research funding, intellectual property rights, and the allocation of licensing income and other financial benefits.[43] A third major challenge for universities in creating legal and institutional structures for industry-university R&D collaboration is to maintain a university research environment that is consistent with the

---

[40] We use the term "research agenda" broadly to mean the questions that the university deems worthy of academic inquiry. While there are a great variety of valid research agendas (even within individual universities), the limits of which are not concretely defined in many cases, the class of intellectually worthy subjects for research is not, for most research universities, limitless.

[41] *See generally* William L. Baldwin, *The U.S. Research University and the Joint Venture: Evolution of an Institution,* 11 REV. INDUS. ORG. 629, 651 (1996) (noting concern that the trend toward increased IURC may divert universities away from pursuit of important basic research); Bok, *supra* note 35, at 17-18 (noting concern that the trend toward increased IURC may divert universities away from pursuit of important basic research); Caldart, *supra* note 6, at 26 (raising concern that "industry investment in university research will reduce the university's traditional autonomy over its activities, and thus could operate as a constraint on the exercise of academic freedom"); Robert M. Rosenzweig, *Universities Change, Core Values Should Not,* 16 ISSUES SCI. & TECH. ONLINE (1999), *at* http://www.nap.edu/issues/16.2/rosenzweig.htm (same); Cordes, *A Quiet Debate Emerges*, *supra* note 7, at A22; Nicklin, *supra* note 7, at A25.

[42] *See generally* COGR, REVIEW, *supra* note 36 ("In research relationships with industry, universities must carefully guard their ability to disseminate knowledge to students and the public. Nevertheless, corporate sponsors need to be assured that the results of the research they fund at universities will be available to them for commercial exploitation.").

[43] *See generally* Baldwin, *supra* note 41, at 651 ("Among the new or exacerbated problems that university participants in joint R&D ventures face are . . . decisions made jointly with profit-seeking firms as to how to exploit the results of the venture; . . . [and] sharing in the profits and risks.").

research university's academic mission.[44] A key element of this third challenge is managing actual and perceived conflicts between the relatively "open" research culture of academia and the more secretive research culture of the private sector.[45]

---

[44] *See generally* Bok, *supra* note 35, at 3 ("The principal work of [university] presidents, provosts, and deans is to maintain an environment that fosters learning and discovery."); Wade L. Robinson & John T. Sanders, *The Myths of Academia: Open Inquiry and Funded Research,* 19 J.C. & U.L. 227, 233 (1992) ("It would seem that a university's goals of being an open forum and at the forefront of knowledge cannot be met without compromise, given the necessity for outside funding to pursue research.").

[45] *See generally* Baldwin, *supra* note 41, at 651; Sheila Slaughter & Gary Rhoades, *Renorming the Social Relations of Academic Science: Technology Transfer,* 4 EDUC. POL'Y 341 (1990) (expressing concern that increasingly influential norms of secrecy and ownership have compromised the university research environment); GOVERNMENT-UNIVERSITY-INDUSTRY RESEARCH ROUNDTABLE, OPENNESS AND SECRECY IN RESEARCH: PRESERVING OPENNESS IN A COMPETITIVE WORLD 2-3 (1997), *available at* http://www4.nationalacademies.org/pd/guirr.nsf/238912d6ec6e95b4852566f2006da6f5/6b115e90e851bb34852568bd006067f7?OpenDocument [hereinafter GUIRR, OPENNESS AND SECRECY]("Preserving a balance between openness and proprietary control [in IURC] is vital."); Rosenzweig, *supra* note 41, at 5 (questioning whether faculty and administrators seeking research funding can be "counted on to assert the university's commitment to the openness of research processes and the free and timely communication of research results").

B. Confidential Information Rules for IURC

1. Basis for Concern

One of the most frequently-cited problems of structuring and administering industry-university research collaboration is the treatment of confidential and proprietary information in the university research environment.[67] The issue typically arises when university participants in collaborative research are asked to restrict the dissemination of information that industry partners wish to protect from unauthorized disclosure.[68] Such information can include, for example: (1) confidential and proprietary technical knowledge, materials, or research tools that companies disclose to university

---

[65] *See* MIT Media Laboratory Overview, *supra* note 63.

[66] *See* Interview with Thomas Corsi, Professor of Logistics, University of Maryland at College Park, and Co-Director, Supply Chain Management Center (Mar. 14, 2001) (stating that the Media Lab was the model for the Net Lab).

[67] *See, e.g.*, Wesley M. Cohen et al., *supra* note 7, at 193-94; Bartlett Giamatti, *Free Market and Free Inquiry: The University, Industry, and Cooperative Research, in* PARTNERS IN THE RESEARCH ENTERPRISE: UNIVERSITY-CORPORATE RELATIONS IN SCIENCE AND TECHNOLOGY 3, 9 (Thomas W. Langfitt et al. eds., 1983), Donald R. Fowler, *University-Industry Research Relationships: The Research Agreement,* 9 J.C. & U.L. 515, 523 (1982-83) (noting that the matter of publication of research results is "an area identified by many people responsible for university research as the most difficult in working out research arrangements between university and industry"); Nicklin, *supra* note 7, at A25; Rosenzweig, *supra* note 41.

[68] *See generally* April Burke, *University Policies on Conflict of Interest and Delay of Publication,* 12 J.C. & U.L. 177 (1985); Michael S. Gilliand, *Joint Venturing University Research: Negotiating Cooperative Agreements,* 10 BUS. L. 971 (1985); Fowler, *supra* note 67.

research partners, but not to the general public; (2) data provided by the industry; (3) data generated jointly in the course of research collaboration; or (4) inventions, or other commercially-valuable results, arising from collaborative research.

For many, the protection of confidential and proprietary information in the university research environment brings into conflict two fundamentally antithetical sets of values and interests: the academic versus the commercial. From this perspective, the academic norm of "openness" is juxtaposed against the commercial norm of "secrecy."[69] "Openness" is associated with academic freedom, the disinterested pursuit of truth,[70] and the widest possible dissemination of knowledge.[71] Commercial "secrecy" is associated with narrowly-framed and result-oriented inquiry, the pursuit of profit, and restrictions on the disclosure of commercially-valuable or otherwise commercially-sensitive information.[72]

While the conflict between academic "openness" and commercial "secrecy" is often overstated in discussions of IURC, there can be

---

[69] The norm of secrecy, like the propensity to patent useful knowledge, follows from the commercial imperative to appropriate the value of R&D. *See generally* Richard C. Levin et al., *Appropriating the Returns from Industrial Research and Development,* 3 BROOKINGS PAPERS ECON. ACTIVITY 783 (1987). On the tension between the academic norms of openness and industry norms of appropriation and secrecy, see generally Eisenberg, *Academic Freedom, supra* note 6, at 1375-77; Eisenberg, *Proprietary Rights, supra* note 9, at 197-98; Yves Fassin, *Academic Ethos Versus Business Ethics,* 6 INT'L J. TECH. MGMT. 533 (1991); Rai, *supra* note 6, at 90-94, 110-15. *But see* F. Scott Kieff, *Facilitating Scientific Research: Intellectual Property Rights and the Norms of Science – A Response to Rai and Eisenberg,* 95 NW. U. L. REV. 691 (2001) (arguing that there is no inconsistency between the norms of science and the appropriation of the value of biotechnology research through patenting research results).

[70] *See generally* Martin Kenney, *The Ethical Dilemmas of University-Industry Collaborations,* 6 J. BUS. ETHICS 127, 129 (1987) (stating that university faculty members are morally obligated "to seek and teach the truth").

[71] *See generally* ROBERT K. MERTON, THE SOCIOLOGY OF SCIENCE: THEORETICAL AND EMPIRICAL INVESTIGATIONS 273-75 (Norman W. Storer ed., 1973); Kenney, *supra* note 70, at 129 ("[T]he professor must make the results of research freely available to all"); Rai, *supra* note 6, at 90 ("One central element of the scientific ethos that promotes the sharing of information in the public domain is the view that scientific knowledge is ultimately a shared resource.").

[72] *See generally* Cohen et al., *supra* note 7, at 186 ("Firms . . . prefer less disclosure of research finding to increase the appropriability of the profits of any process or product innovations that may grow out of the research."); Caldart, *supra* note 6, at 27, 30-31; Kenney, *supra* note 70, at 129 ("The primary and overriding duty for an industrial concern is to make a profit.").

little doubt that the research cultures of universities and private firms can differ.[73] In the university research culture, academics have strong professional incentives to publish research results as quickly and as widely as possible.[74] Academic rewards, such as promotion and recognition, flow to those who publish first on questions that are generally agreed upon among the researcher's peers to have intellectual merit.[75] For industry research, by contrast, merit is ultimately measured by the market. Researchers are rewarded for results that show commercial promise and eventually find their way into successful products.[76] Timely publication of research results may, under some circumstances, be of value to the industrial researcher.[77] But the highest priority for industrial innovation is to confer competitive advantage in markets for the sale of commercial products. Thus

---

[73] *See generally* Harvey Brooks & Lucien P. Randazzese, *Industry-University Relations: The Next Four Years and Beyond, in* INVESTING IN INNOVATION: CREATING A RESEARCH AND INNOVATION POLICY THAT WORKS 361, 377 (Lewis M. Branscomb & James H. Keller eds., 1999) ("Industry often perceives an interest in limiting the disclosure of results from university research that it supports; this places its research style in conflict with the more open culture of universities."). Although university and corporate research cultures differ, particularly at the margins of the continuum running from the most theoretical "basic research" to straight product "development," they also share a great deal of common ground. As set forth in greater detail below, this common ground offers a basis for concluding that the perceived conflict between academic "openness" and commercial "secrecy" can be effectively managed without sacrificing the fundamental interests of industry or the academy. *See infra* Part II.B.3.d and accompanying notes.

[74] *See generally* Partha Dasgupta & Paul A. David, *Information Disclosure and the Economics of Science and Technology, in* ARROW AND THE ASCENT OF MODERN ECONOMIC THEORY 519, 528 (1987) (contrasting the "social imperative" among academic scientists to disclose fully research results and inventions, with the norm among industry technology developers to refrain from fully disclosing research results and inventions); MERTON, *supra* note 71, at 302 ("In the organized competition to contribute to man's scientific knowledge, the race *is* to the swift, to him who gets there first with his contribution in hand."); Dianne Rahm, *US Universities and Technology Transfer: Perspectives of Academic Administrators and Researchers,* INDUSTRY & HIGHER ED. June 1994, at 72, 73.

[75] *See generally* C. Alan Garner, *Academic Publication, Market Signaling, and Scientific Research Decision,* 17 ECON. INQUIRY 575 (1979); Diana Hicks, *Published Papers, Tacit Competencies and Corporate Management of the Public / Private Character of Knowledge,* 4 INDUS. & CORP. CHANGE 401 (1995); Paula E. Stephan, *The Economics of Science,* 34 J. ECON. LITERATURE 1199 (1996).

[76] *See generally* Dasgupta & David, *supra* note 74, at 523 ("Roughly speaking, the [academic] scientific community appears concerned with the *stock* of knowledge and is devoted to furthering its growth, whereas the [industrial] technological community is concerned with the private economic *rents* that can be earned from that stock.").

[77] *See infra* Part II.B.3.d and accompanying notes.

private firms employ mechanisms, principally secrecy and the assertion of intellectual property rights, to appropriate the value of their research and to keep commercially-valuable information out of the hands of competitors.[78] In the public debate over IURC, many academics and university administrators have raised concerns that the use of such appropriation mechanisms in the university research context may compromise the academic norm of "openness," limit the free exchange of ideas and information, and undermine the university's role as the disinterested discoverer and disseminator of intellectually-important knowledge.[79]

2. University Confidential Information Policies

Although there has been little systematic study of confidential information practices in industry-university research collaborations, a general sense of university policies can be gleaned from the limited empirical literature and the formal policy statements of university administrators.[80] Typically, university research policy statements reject secrecy as a matter of principle and insist on the freedom of university researchers to publish any research results of intellectual

---

[78] *See generally* Levin et al., *supra* note 69; Richard Zeckhauser, *The Challenge of Contracting for Technological Information,* 93 PROC. NAT'L ACAD. SCI. USA 12,743 (1996).

[79] *See generally* GUIRR, OVERCOMING BARRIERS, *supra* note 2, at 17 (observing that "publication delays and non-disclosure requirements may impair the openness of the university research environment"); David Blumenthal, *Academic-Industry Relationships in the Life Sciences,* 268 JAMA 3344, 3347 (1992) ("[A]n increase in secrecy is one of the most feared consequences of [academic-industry relationships]."); Rahm, *supra* note 74, at 76 (reporting that in response to a survey on IURC issues, "nearly 38% of [university] administrators [surveyed] remark that firms they have dealt with have placed restrictions on researchers sharing information regarding R&D breakthroughs with . . . colleagues in an attempt to protect the secrecy of a potential commercial product"); Sheila Slaughter & Gary Rhoads, *supra* note 45, at 341 (maintaining that "[I]n accepting the conditions of private work in terms of secrecy and ownership – and in reaping the increased benefits of such work – entrepreneurial faculty have generated and heightened tension with their peers and their graduate students.").

[80] *See generally* Blumenthal et al., *Industry Survey, supra* note 2 (reporting results of survey of senior executives of life sciences companies); Blumenthal, *supra* note 79; David Blumenthal et al., *University-Industry Relationships in Biotechnology: Implications for the University,* 232 SCI. 1361 (1986) [hereinafter Blumenthal et al., *Industry-University Research Relationships*]; Brooks & Randazzese, *supra* note 73, at 377-80 (reviewing the literature on information disclosure restrictions in IURC); Dianne Rahm, *supra* note 74, at 72 (reporting results of survey of university administrators and researchers).

merit, including those generated through industry-university collaboration.[81] Nevertheless, most universities accept some restrictions on the disclosure of some types of information.[82] Perhaps the most common of these restrictions is delaying the publication of research results to allow the university or its industry partners time to file for patent protection.[83] While less prevalent than publication delays to

---

[81] *See, e.g.*, COLO. STATE UNIV., TALKING TO POTENTIAL COMMERCIAL SPONSORS ABOUT RESEARCH, CLINICAL TRIALS, OR SERVICE AGREEMENTS (2000), http://www.research.colostate.edu/policy/ (visited May 26, 2001) ("Freedom to publish results of work by our faculty and students is an inviolable principle at CSU."); DUKE UNIV., UNIVERSITY-INDUSTRY GUIDELINES 3 (1995), http://www.ors.duke.edu/policies/unvind.htm. ("[U]niversity researchers must be free to publish their research results."); THE UNIV. OF N.C., UNIVERSITY RELATIONS WITH PRIVATE ENTERPRISE (1995), http://www.ncsu.edu/roe/policy/university.html ("Faculty and students must have the right to disseminate freely and openly their research findings, and research sponsors may not abridge this basic right."); STANFORD UNIV., RESEARCH POLICY HANDBOOK (1996), http://stanford.edu/dept/DoR/rph/2-6.html ("[T]he principle of openness in research – the principle of freedom of access by all interested persons to the underlying data, to the processes, and to the final results of research – is one of overriding importance.").

[82] *See generally* GIURR, OPENNESS AND SECRECY, *supra* note 45, at 3-5.

[83] *See* Blumenthal et al., *Industry Survey, supra* note 2, at 371 (reporting that publication delays to allow time to file patent applications are "standard practice at most academic institutions"); Burke, *supra* note 68 at 186-88 (same); Gilliland, *supra* note 68, at 981-82. It should be noted in this context that an invention is ineligible for patent protection if it is described in a publication more than one year prior to the filing of a patent application. Patent Act, 36 U.S.C. § 102(b) (2000).

A model publication delay provision for IURC, drafted by the Government-Industry-University Research Roundtable, reads as follows:

> Sponsor recognizes that under University policy, the results of University Project must be publishable and agrees that Researchers engaged in Project shall be permitted to present at symposia, . . . professional meetings, and to publish in journals, theses or dissertations, or otherwise of their own choosing, methods and results of Project, provided, however, that Sponsor shall have been furnished copies of any proposed publication or presentation at least [___] months in advance of the submission of such proposed publication or presentation to a journal, editor, or other third party. Sponsor shall have [___] months, after receipt of said copies, to object to such proposed presentation or proposed publication because there is patentable subject matter, which needs protection. In the event that Sponsor makes such objection, said Researcher(s) shall refrain from making such publication or presentation for a maximum of [___] months from the date of receipt of such objection in order for University to file patent application(s) . . . directed to the patentable subject matter contained in the proposed publication or presentation.

GOVERNMENT-INDUSTRY-UNIVERSITY RESEARCH ROUNDTABLE, SIMPLIFIED AND STANDARDIZED MODEL AGREEMENTS FOR INDUSTRY-UNIVERSITY COOPERATIVE RESEARCH, art. 6.1 (1988) [hereinafter GIURR MODEL AGREEMENT].

file patent applications, universities also agree in some cases to delay publication of research results beyond the time needed for patent filings,[84] or to treat collaborative research results as proprietary information that cannot be published *at all* without the consent of the industry sponsor.[85]

In addition to publication delays, many universities enter into, and/or permit faculty researchers to enter into, non-disclosure agreements ("NDAs") with industry research partners.[86] Under these arrangements, which are modeled on private law mechanisms to protect commercially-valuable information in employment and business-to-business relationships,[87] academic researchers agree to

---

[84] *See* Blumenthal et al., *Industry Survey, supra* note 2, at 371 (reporting that 56% of life science company executives surveyed said that industry-sponsored university research is "often or sometimes . . . 'kept confidential to protect its proprietary value beyond the time required to file a patent'").

[85] *See id.* (reporting that 24% of university biotechnology researchers surveyed said that they had conducted research that was the property of the sponsor and which "could not be published without the sponsor's consent"); Rahm, *supra* note 74, at 76 (reporting that 79% of university administrators and 59% of university researchers surveyed stated that "firms they have dealt with have sought to prohibit or delay researchers from publishing research results coming from university-firm interactions"). An alternative version of the GIURR Model Agreement publication delay provision allows for delayed publication of patentable subject matter *or* "Confidential Information of Sponsor contained in the proposed publication or presentation," and directs the university and the sponsor to negotiate "an acceptable version" before publication or presentation can occur. *See* GIURR MODEL AGREEMENT, *supra* note 83, app. I, art. 6.1.

[86] *See generally* Gilliand, *supra* note 68, at 978-79.

[87] In the employment context, a non-disclosure agreement is a promise by an employee to refrain from disclosing any trade secrets or other confidential information to which the employee has access during his or her employment. *See generally* Zahodnick v. Int'l Bus. Mach. Corp., 135 F.3d 911 (4th Cir. 1997) (reviewing claim of former employer against former employee alleging breach of nondisclosure agreements). Non-disclosure agreements are also commonly used to protect confidential information in a broad range of business negotiations and relationships. *See, e.g.*, STEPHEN ELIAS, PATENT, COPYRIGHT & TRADEMARK: A DESK REFERENCE TO INTELLECTUAL PROPERTY LAW 41 (1996) (sample nondisclosure agreement drafted for purposes of product evaluation); *see also* Hannon Armstrong & Co. v. Sumitomo Trust & Banking Co., 973 F.2d 359 (4th Cir. 1992) (reviewing action against investor for breach of nondisclosure agreement); Carol M. Bast, *At What Price Silence: Are Confidentiality Agreements Enforceable?* 25 WM. MITCHELL L. REV. 627, 629-54 (1999) (surveying the law governing confidentiality agreements); Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech,* 83 CORNELL L. REV. 261, 268-76 (1998) (same); David L. Hoffman & Robert J. Lauson, *Practice Tips Tailoring Nondisclosure Agreements to Client Needs,* L.A. LAW., Oct. 23, 2000, at 57, 57 ("Nondisclosure agreements, also known as NDAs or confidentiality agreements, are vital to the exchange of technological and business

refrain from disclosing confidential information to third parties.[88]

3. Irreconcilable Research Cultures?

Having reviewed some of the principal concerns regarding secrecy in IURC, as well as the primary mechanisms for protecting confidential information, it is appropriate to examine the argument, noted earlier, that there is a fundamental conflict between academic "openness" and commercial "secrecy," and that information restrictions adapted from the commercial research culture are antithetical to the university research culture.[89] While a comprehensive examination of this issue is beyond the scope of the present paper, we can identify four principal reasons for viewing the claim of fundamental irreconcilability with skepticism.

a. *Not All Confidential Information Is Created Equal:*

Although the IURC debate tends to focus on restrictions of the disclosure of research *results*, a significant portion of the material that is protected in IURC arrangements – particularly by non-disclosure agreements -- consists not of research results at all, but of trade secrets and other confidential information disclosed to university researchers by industry research partners, but not to the general public.[90] The

---

ideas."); William L. Kochen, *Securing a Secret Trust,* 38 SECURITY MGMT. 142 (1994) (reviewing law and business practices regarding nondisclosure agreements).

[88] A model IURC non-disclosure provision drafted by the Government-Industry-University Research Roundtable reads, in relevant part, as follows:

> Anything in this Agreement to the contrary notwithstanding, any and all knowledge, know-how, practices, process, or other information . . . disclosed or submitted in writing or in other tangible form which is designated as Confidential Information to either party by the other shall be received and maintained by the receiving party in strict confidence and shall not be disclosed to any third party . . . . The parties may disclose Confidential Information to employees requiring access thereto for the purposes of this Agreement provided, however, that prior to making any such disclosures each such employee shall be apprised of the duty and obligation to maintain Confidential Information in confidence . . . .

GIURR MODEL AGREEMENT, *supra* note 83, app. I, art. 1.1.

[89] *See supra* Part II.B.1 and accompanying notes.

[90] *See generally* Brooks & Randazzese, *supra* note 73, at 379 (noting difference between collaborative research results and the proprietary information of firms participating in IURC, and further noting the fact that the empirical literature makes no such distinction).

distinction bears emphasis because there is no necessary inconsistency between protecting such information and the academic imperatives to pursue and publish original research of intellectual merit.[91] The academic norm of "openness," moreover, offers no philosophical justification for a "freedom" to publish, or otherwise disclose, proprietary knowledge of private firms that predates, or is otherwise separate from, the jointly-developed fruits of IURC.

b. *Secrecy in University Research Is Not Unique to IURC*:

When considering the place of confidential information policies in the university research culture, it is also important to acknowledge that, IURC aside, secrecy is a familiar and generally-accepted part of that culture. For example, names of university research subjects and interviewees are routinely withheld to protect their privacy.[92] University researchers agree in some cases to refrain from revealing certain information in a public figure's private papers as a condition of gaining access to other materials of scholarly significance.[93] Academics exercise discretion to delay or avoid presenting new ideas, methodologies, or the results of research in progress in order to keep information from rivals in the race to publish, or to reserve material for future projects.[94] Indeed, even peer review of submissions to

---

[91] *See* Fowler, *supra* note 67, at 525 (arguing that protecting a company's confidential information "is an entirely different matter from agreeing to delay or to keep confidential the results of a research project, and therefore, the overriding principles of publishing research do not apply"). Some have suggested, based on anecdotal evidence, that confidentiality agreements for industry-provided inputs are as threatening to the academic research environment as confidentiality provisions relating to IURC research results. *See, e.g.*, Steven A. Rosenberg, 334 NEW ENG. J. MED. 392 (1996) (in an untitled commentary, a National Cancer Institute official condemns industry-university confidentiality agreements for both research results and industry-provided research inputs); Lawrence K. Altman, *Medical Research Hurt By Secrecy, Official Says,* N.Y. TIMES, Feb. 10, 1996, at 9. However, such arguments tend to weigh the perceived costs of confidentiality agreements, while failing to consider the *net* benefits of industry contributing proprietary inputs to the university research enterprise that would be otherwise unavailable. These arguments also fail to address the legitimate intellectual property rights of industry research partners.

[92] Nicholas H. Steneck, *Whose Academic Freedom Needs to be Protected? The Case of Classified Research,* 11 BUS. & PROF. ETHICS J. 17, 24 (1992).

[93] *Id.*

[94] *See generally* Sissela Bok, *Secrecy and Openness in Science: Ethical Considerations,* 7 SCI. TECH. & HUMAN VALUES 32, 34-37 (1982); Hicks, *supra* note 75, at 408.

academic journals – a confidential process that can go on for many months after potentially significant research has been completed – can be understood as an academy-sanctioned publication delay.[95]

In each of the above-mentioned circumstances, information restrictions in the university research culture are accepted because they are generally thought to serve a "greater good" that is of value to the academic mission of the university. Withholding the names of research subjects can be justified as a necessary concession to help persuade people to participate in important human research studies. Strategic delay or withholding of information by academics is protected under the rubric of the academic freedom of the individual researcher to judge when and what to offer for publication.[96] Publication delay for peer review is justified as the price to be paid for assuring that the research published by academic journals is of intellectual merit. The point here is not that secrecy is, or should be, a pervasive element of the university research culture. It is, rather, that quite apart from IURC, university researchers regularly and appropriately employ information restrictions based on a calculation that the net benefits of such restrictions for the academic enterprise outweigh the costs. It follows that the same cost/benefit calculus should apply to the evaluation of the information restrictions that accompany IURC.

c. *Universities Are Capable of Protecting Their Interests:*

One of the premises of the fundamental irreconcilability argument is that universities are unable or unwilling to protect their values and interests in collaborative relationships with industry.[97] However, this premise seems questionable in light of the university's bargaining position and the record of IURC to date.

---

[95] *See* Steneck, *supra* note 92, at 24.

[96] Of course, the academic freedom to delay or refrain from publishing important research results can be abused. This potential for abuse is generally accepted, however, as a tolerable aspect of an otherwise salutary deference to the judgment of the individual researcher.

[97] *See, e.g.*, Eisenberg, *Academic Freedom, supra* note 2, at 1374 (arguing that university "[f]aculty members who are financially dependent on research sponsors may not be counted on to uphold academic values on their own"); Kenney, *supra* note 70, at 130, 134 (suggesting that because universities are not well-equipped to protect their values and interests in IURC, "national guidelines" are needed to prevent the "destruction of the values of the university").

Universities have considerable leverage in the negotiation of collaborative relationships with industry. Private firms typically enter into IURC not because of eleemosynary impulses, but in pursuit of the commercially-valuable knowledge and other resources universities have to offer.[98] It will be recalled, moreover, that although industry support of university research has been increasing rapidly in recent years, it still amounts to just seven percent of all university R&D expenditures.[99] To be sure, all other things being equal, most schools are likely to welcome industry resources and participation in the university research enterprise. Moreover, the aggregate seven percent figure may understate the importance of industry support in many specific cases. Nevertheless, because they offer something of considerable value to industry partners, and ninety-three percent of university R&D funds come from sources other than industry, most research universities are in a position to negotiate terms for IURC that are substantially consistent with their institutional values and interests.[100]

Consider the record of IURC to date. Although there has been no shortage of expressions of concern regarding information restrictions in IURC, among thousands of industry-university collaborations, there have been very few documented cases of important collaborative research results being held in secret to the detriment of the academy or the public-at-large.[101] To be sure, this may simply reflect

---

[98] *See supra* Part I.A and accompanying notes.

[99] *Id.*

[100] *See generally* Brooks & Randazzese, *supra* note 73, at 379 ("[I]n the spectrum of research universities and firms, the best seem quite capable of protecting their traditional values of openness, with only modest concessions to the practical needs of industry, while other institutions are quite willing to undertake more proprietary work which calls for more traditional industrial restraints on disclosure."); Blumenthal et al., *Industry-University Research Relationships, supra* note 80, at 1366 ("Most universities are in a strong bargaining situation with respect to potential industrial sponsors.").

[101] *See generally* David Blumenthal et al., *Withholding Research Results in Academic Life Science: Evidence From a National Survey of Faculty*, 227 JAMA 1224, 1227 (1997) (concluding on the basis of a national survey of 2167 life science academics: "our findings suggest that data withholding is not widespread"). Of the 2167 respondents surveyed by Blumenthal et al., 19.8% reported having delayed the publication of research results by at least six months, at least once during the previous three years. *Id.* at 1226. Of the 410 respondents reporting such delays, 46% reported that the delays were to allow time to file patent applications, while 28% reported delays "to slow dissemination of undesired results." *Id.*; *see also* Rhein, *supra* note 57, at 1 (an NIH official, reporting on a study of 375 government-funded research collaboration agreements, concluded that "[f]or the most part, we did not find unreasonable

difficulties in detecting and reporting such circumstances. Moreover, the reported cases of inappropriate disclosure restrictions raise quite legitimate concerns.[102] But the very small number of cases is at least consistent with the interpretation that IURC confidential information policies have not, in practice, excessively restricted the diffusion of collaborative research results on a regular basis. That is to say, the record supports the inference that universities have generally been able to negotiate IURC agreements without, so to speak, "giving away the academic store."

---

restrictions, publication delays or constraints of university researchers from consulting or collaborating with other parties.").

[102] In one recent case, Immune Response Corporation ("IRC") sponsored clinical trials at the University of California at San Francisco to evaluate a medication -- "Remune" -- the company had developed for the treatment of AIDS. After UCSF researchers concluded that Remune was not an effective treatment for the disease, IRC tried to persuade the lead researcher not to publish an article reporting the unfavorable results of the clinical trials. The company stated that it opposed the publication because the researchers omitted favorable data and disclosed proprietary information they had agreed to keep confidential. When the UCSF researchers published the article over IRC's objections, the company brought an action for damages against the researchers and the University before the American Arbitration Association. *See* J. O. Kahn et al., *Evaluation of HIV-1 Immunogen, an Immunologic Modifier, Administered to Patients Infected with HIV Having 300 to 549 x10(6)/L CD4 Cell Counts: A Randomized Control Trial*, 284 JAMA 2193 (2000); Katherine S. Mangan & Goldie Blumenstyk, *Company Seeks $10-Million From Scientist and University*, CHRON. HIGHER ED., Nov. 17, 2000, at A48; Karen Young Kreeger & Paula Park, *When Corporations Pay for Research*, SCIENTIST. COM (May 28, 2001), http://www.the-scientist.com/yr2001/may/prof_010528.html. In another case, also involving a UCSF research team, another pharmaceutical company – Boots – sponsored a university study to determine whether three cheaper drugs were the bioequivalents of Boots' market-leading hypothyroidism drug, Synthroid. After the UCSF research team determined that the three other drugs could be effectively substituted for Synthroid at a savings of hundreds of millions of dollars per year in health care costs, Boots asserted its contractual right to bar publication of the research results. In contrast to the IRC case, the University of California refused to defend the researchers who had conducted the study and the research results were never published. *See* Ralph T. King Jr., *Bitter Pill: How a Drug Firm Paid for University Study, Then Undermined It*, WALL ST. J., Apr. 25, 1996, at A1. Significantly, the agreement that the UCSF researchers had entered into with Boots, which stated that the research results could not be published without the company's written consent, violated the University's policies regarding sponsored research. *Id.* Thus the principal problem revealed in the UCSF/Boots case would appear to lie not with the university's confidential information policies, but rather in the failure of a university researcher to follow those policies.

d. *Industrial and academic cultures' common ground:*

A final point that bears particular emphasis in the evaluation of arguments positing a fundamental divergence between the academic and commercial research cultures is that, with regard to the diffusion of research results, the two cultures have more in common than is often assumed.[103] As noted earlier, although academic researchers have powerful incentives to publish research quickly and widely, scholars also exercise discretion in deciding how much to publish and when. On the other side of the academic/industry divide, industrial researchers often have strong incentives to publish and, in fact, contribute extensively to the academic literature, particularly in science and engineering.[104]

Given the commercial imperative to appropriate the value of knowledge for competitive advantage, why would companies want to publish research results? The explanation lies in the crucially important "market signaling" function of publication. First, firms publish, in part, to compete more effectively in the market for highly-skilled employees. Publication helps a company attract and retain talented employees by signaling that the firm is doing important R&D

---

[103] *See generally* Dasgupta & David, *supra* note 74, at 524-25; Hicks, *supra* note 75, at 406 ("[I]n many areas neither science and technology, nor corporate and academic research interests can be clearly distinguished."); Stephan, *supra* note 75, at 1209 (noting that "the research of some scientists and engineers in companies like IBM, AT&T, and Du Pont is virtually indistinguishable from that of their academic counterparts"); DONALD E. STOKES, PASTEUR'S QUADRANT: BASIC SCIENCE AND TECHNOLOGICAL INNOVATION (1997) (discussing the nature and significance of "use-inspired basic research," which straddles the traditional division between "pure basic" and "pure applied" research).

[104] *See generally* Hicks, *supra* note 75, at 402-03 (noting that private firms publish extensively in the science and technology research journals, with some companies contributing "as much to the public literature as medium-sized universities"); Stephan, *supra* note 75, at 1210 (reporting that industry produces one-sixth of the articles published in chemistry and physics and one-fourth of the engineering and technology literature); Iain Cockburn & Rebecca Henderson, Public-Private Interaction and the Productivity of Pharmaceutical Research 14 (Nat'l Bureau of Econ. Research, Working Paper No. 6018, 1997) (noting that in the 1970s, some pharmaceutical firms "began to actively encourage publication and to hire researchers at the leading edge of their fields with the promise that they would reward them to continue doing cutting edge scientific research").

work of intellectual merit.[105] Second, and more importantly, firms publish in order to establish and maintain reputations that facilitate their participation in the informal market for the exchange of valuable tacit knowledge.[106] Particularly where sophisticated technology is concerned, many firms require not only the types of explicit knowledge that can be written in an article or a patent application, but also on tacit knowledge that may be of equal value.[107] A key source of such tacit knowledge for companies is the exchange of know-how through informal networks of researchers with complementary areas of expertise.[108] In these informal networks, researchers understandably prefer to share their valuable tacit knowledge today with organizations that are likely to be in a position to offer valuable tacit knowledge reciprocally tomorrow.[109] By publishing in scholarly journals, firms signal that they possess valuable tacit knowledge and that they are therefore worthy players in the ongoing exchange of such knowledge across organizational boundaries.[110]

Of course, this is not to say that firms have an interest in publishing *all* of their research results. Companies are obliged to "manage the process" of selective disclosure "by establishing procedures to reconcile publication with appropriation."[111] Nevertheless, contrary to the notion of academic "openness" fundamentally opposing commercial "secrecy," the market signaling functions of publication can offer material incentives for private firms to support the publication of the results of IURC.

---

[105] *See* Hicks, *supra* note 75, at 413; Stephan, *supra* note 75, at 1209 ("The reputation of the lab, which is directly related to publication activity, also affects the ability of the company to hire scientists and engineers.").

[106] Hicks, *supra* note 75, at 414-21.

[107] *Id.* at 413-14; *see also* Eric von Hippel, *Cooperation Between Rivals: Informal Know-how Trading*, 16 RES. POL'Y 291 (1987).

[108] *See* von Hippel, *supra* note 107, at 294-96; G. E. Pake, *Business Payoff from Basic Science at Xerox*, 29 RES. MGMT. 35 (1986); S. Schrader, *Informal Technology Transfer Between Firms: Cooperation through Information Trading*, 20 RES. POL'Y 153 (1991).

[109] *See* von Hippel, *supra* note 107, at 292-95.

[110] *See* Hicks, *supra* note 75, at 414-21.

[111] *Id.* at 409. Publications can inform the world that a firm knows how to make a better mousetrap without providing competitors with instructions for constructing that mousetrap on their own. *See* Stephan, *supra* note 75, at 9 ("[P]ublication is not synonymous with replicability").

The Militarization of US Higher Education after 9/11

Henry A. Giroux

Abstract
Subject to severe financial constraints while operating within a regime of moral panics driven by the 'war on terrorism', higher education in the United States faces both a legitimation crisis and a political crisis. With its increasing reliance on Pentagon and corporate interests, the academy has largely opened its doors to serving private and governmental interests and in doing so has compromised its role as a democratic public sphere. This article situates the development of the university as a militarized knowledge factory within the broader context of what I call *the biopolitics of militarization* and its increasing influence and power within American society after the tragic events of September 11, 2001. Highlighting and critically engaging the specific ways in which the forces of militarization are shaping various aspects of university life, this article focuses on the growth of militarized knowledge and research, the increasing development of academic programs and schools that serve military personnel, and the ongoing production of military values and subject positions on US campuses. It also charts how the alliance between the university and the national security state has undermined the university as a site of criticism, dissent and critical dialogue.

Key words
■ 9/11 ■ America ■ higher education ■ militarism ■ military ■ neoliberalism ■ pedagogy

War is the motor behind institutions and order. In the smallest of its cogs, peace is waging a secret war. To put it another way, we have to interpret the war that is going on beneath peace; peace is coded war. We are therefore at war with one another; a battlefront runs through the whole of society, continuously and permanently, and it is this battlefront that puts us all on one side or the other. There is no such thing as a neutral subject. We are all inevitably someone's adversary. (Foucault, 2003: 50–1)

■ *Theory, Culture & Society* 2008 (SAGE, Los Angeles, London, New Delhi, and Singapore), Vol. 25(5): 56–82
DOI: 10.1177/0263276408095216

The Militarized Knowledge Factory: Research, Credentials and the CIA

> While the Cold War and Sovietology are gone from the scene, a parallel project is now underway: the launching of large-scale initiatives to create a cadre and set of institutions that penetrate our campuses and link them to national security, military, and intelligence agencies. The aim is nothing less, as Congressional hearings show, than to turn back opposition on our campuses to imperial war, and turn campuses into institutions that will, over the next generation, produce scholars and scholarship dedicated to the so-called war on terror. These programs are part of a broader effort to normalize a constant state of fear, based on the emotion of terror, while criminalizing anti-war and anti-imperial consciousness and action. As in the past, universities, colleges and schools have been targeted precisely because they are charged with both socializing youth and producing knowledge of peoples and cultures beyond the borders of Anglo-America. (Martin, 2005)

Now that the war on terrorism and a gradual erosion of civil liberties have become commonplace, the idea of the university as a site of critical thinking, public service and socially responsible research appears to have been usurped by a manic jingoism and a market-driven fundamentalism that enshrine the entrepreneurial spirit and military aggression as the best means to produce the rewards of commercial success and power. Not only is the militarization of higher education made obvious by the presence of over 150 military-educational institutions in the United States designed to 'train a youthful corps of tomorrow's military officers' in the strategies, values, skills and knowledge of the warfare state, but also, as the American Association of Universities points out, in the existence of hundreds of colleges and universities that conduct Pentagon-funded research, provide classes to military personnel, and design programs specifically for future employment with various departments and agencies associated with the warfare state (Turse, 2004; see also Johnson, 2004: 97–130). The intrusion of the military into higher education is also on full display with the recent announcement by Robert Gates, the Secretary of Defense under George W. Bush, of the creation of what he calls a new 'Minerva consortium', ironically named affter the goddess of wisdom, whose purpose is to fund various universities to 'carry out social-sciences research relevant to national security' (Brainard,

2008). Without apology, Gates would like to turn universities into militarized knowledge factories producing knowledge, research, and personnel in the interest of the Homeland (In)Security State. Faculty now flock to the Department of Defense, the Pentagon and various intelligence agencies either to procure government jobs or to apply for grants to support individual research in the service of the national security state. At the same time, as corporate money for research opportunities dwindles, the Pentagon fills the void with millions of dollars in available grants, stipends, scholarships and other valuable financial rewards, for which college and university administrators actively and openly compete. Indeed, the Department of Homeland Security is flush with money:

> [It] handles a $70 million dollar scholarship and research budget, and its initiatives, in alliance with those of the military and intelligence agencies, point towards a whole new network of campus-related programs. [For instance,] the University of Southern California has created the first 'Homeland Security Center of Excellence' with a $12 million grant that brought in multidisciplinary experts from UC Berkeley, NYU, and University of Wisconsin-Madison. Texas A&M and the University of Minnesota won $33 million to build two new Centers of Excellence in agrosecurity. . . . The scale of networked private and public cooperation is indicated by the new National Academic Consortium for Homeland Security led by Ohio State University, which links more than 200 universities and colleges. (Martin, 2005)

Rather than being the object of massive individual and collective resistance, the militarization of higher education appears to be endorsed by liberals and conservatives alike. The National Research Council of the National Academies published a report called *Frameworks for Higher Education in Homeland Security* (2006), which argued that the commitment to learning about homeland security is an essential part of the preparation for work and life in the 21st century, thus offering academics a thinly veiled legitimation for building into undergraduate and graduate curricula intellectual frameworks that mirror the interests and values of the warfare state. Similarly, the Association of American Universities argued in a report titled *National Defense Education and Innovation Initiative* (2005) that winning the war on terrorism and expanding global markets were mutually informing goals, the success of which falls squarely on the performance of universities. This group argues, with a rather cheerful certainty, that every student should be trained to become a soldier in the war on terror and in the battle over global markets, and that the universities should do everything they can 'to fill security-related positions in the defense industry, the military, the national laboratories, the Department of Defense and Homeland Security, the intelligence agencies, and other federal agencies' (Martin, 2005).

More and more universities are cooperating with intelligence agencies with few objections from faculty, students and other concerned citizens (Price, 2005). In the aftermath of the 11 September 2001 terrorist attacks,

many academics are enthusiastically offering their services for the plethora of expert personnel positions, which according to National Intelligence Director John Negroponte in 2006 were available among the 16 federal intelligence agencies and programs that employ over 100,000 personnel (*USA Today*, 2006). The *Wall Street Journal* claims that the CIA has become a 'growing force on campus' (Golden, 2002), while a November 2002 issue of the liberal magazine *American Prospect* published an article by Chris Mooney calling for academics and the government intelligence agencies to work together. As he put it, 'Academic–intelligence relationships will never be problem free. But at present, the benefits greatly outweigh the costs' (Mooney, 2002). Such collaboration seems to be in full swing at a number of universities. For example, major universities have appointed former CIA officials as either faculty, consultants or presidents. Michael Crow, a former agent, is now president of Arizona State University and Robert Gates, the former Director of the CIA, was until recently president of Texas A&M. The collusion among the Pentagon, war industries and academia in the fields of research and development is evident as companies that make huge profits on militarization and war, such as General Electric, Northrop Grumman and Halliburton, establish crucial ties with universities through their grants, while promoting their image as philanthropic institutions to the larger society (see Roelofs, 2006). As the university is increasingly militarized, it 'becomes a factory that is engaged in the militarization of knowledge, namely, in the militarization of the facts, information and abilities obtained through the experience of education' (Armitage, 2005: 221). The priority given to such knowledge is largely the result of the huge amount of research money increasingly shaping the curricula, programs and departments in various universities around the country. Money flows from the military war machine in the post-9/11 world, and the grants and research funds that the best universities receive are not cheap. In 2003, for example, Penn State received $149 million in research and development awards while the Universities of California, Carnegie Mellon and Texas received $29.8 million, $59.8 million and $86.6 million respectively, and they are not even the top beneficiaries of such funds (see Turse, 2004). The scale, sweep, range and complexity of the interpenetration between academia and military-funded projects is as extensive as it is frightening. Nicholas Turse explains:

> According to a 2002 report by the Association of American Universities (AAU), almost 350 colleges and universities conduct Pentagon-funded research; universities receive more than 60% of defense basic research funding; and the DoD is the third largest federal funder of university research (after the National Institutes of Health and the National Science Foundation). . . . the Department of Defense accounts for 60% of federal funding for university-based electrical engineering research, 55% for the computer sciences, 41% for metallurgy/materials engineering, and 33% for oceanography. With the DoD's budget for research and development skyrocketing, so to speak, to $66 billion for 2004 – an increase of $7.6 billion over 2003 – it

> doesn't take a rocket scientist to figure out that the Pentagon can often dictate the sorts of research that get undertaken and the sorts that don't. (Turse, 2004)

Along with the money that comes with such defense-oriented funding is a particular assumption about the importance of ideas, knowledge and information and their relevance to military technologies, objectives and purposes. Of course, this is about more than how knowledge is obtained, shaped and used by different elements of the military-industrial complex; it is also about the kind of pressure that the Department of Defense and the war industries can bring to bear on colleges and universities to orient themselves towards a society in which non-militarized knowledge and values play a minor role, thus removing from higher education its fundamental purpose in educating students to be ethical citizens, learn how to take risks, connect knowledge to power in the interests of social responsibility and justice, and defend vital democratic ideals, values and institutions. In this context, it would be worthwhile to heed the warning of Jay Reed:

> Universities are not only hotbeds of military activity, they are adversely affected by the ethical compromises and threats to academic freedom that accompany a Department of Defense presence. The dream of the University as a place of disinterested, pure learning and research is far from reality as scientists and administrators from across the country are paid directly by the military to sit on Department of Defense scientific advisory boards and perform other research. It is naive to think that an abundance of funding from the military does not affect the projects chosen to be worthy of scientific inquiry. University research is not the result of objective decisions made in the spirit of an enlightened quest for knowledge; rather, these scientists' agendas are determined by the bloodthirsty architects of military strategy. (Reed, 2001)

For instance, the Department of Defense, along with a number of other departments and agencies invested in the process of militarization, largely support two main areas of weaponry: space-based armaments and so-called Future Combat Systems. The space weapons being researched in universities around the country include 'microwave guns, space-based lasers, electromagnetic guns, and holographic decoys' while the future combat weapons include 'electric tanks, electro-thermal chemical cannons, [and] unmanned platforms' (Reed, 2001). Such research is carried out at universities such as MIT, which gets 75 percent of its funds for its robotics program from the Department of Defense. How these funds shape research and development and the orientation of theory towards the production of militarized knowledge is evident in MIT's design and production of a kind of RoboMarine called 'the Gladiator', which is a tactical unmanned ground vehicle containing an MT40G medium machine gun, surveillance cameras, and slots for launching paint balls and various smoke rounds, including 'tear gas, or stingball and flashbang grenades' (Cole, 2003). One Pittsburgh paper called it:

> . . . a remote-controlled 'toy,' [with] some real weapons . . . [and] containers for hand grenades that can be used for clearing obstacles and creating a footpath on difficult terrain for soldiers following behind. It also features what looks like organ pipes to produce smoke, and it has a mount on top for a medium-size machine gun or multipurpose assault weapon. (Shropshire, 2005)

Critical commentary apparently not included. In fact, the Gladiator is designed for military crowd-control capabilities, reconnaissance, surveillance, and direct fire missions. Carnegie Mellon University received a $26.4 million Defense Department grant to build six Gladiator prototypes. The University of Texas received funding from the Department of Defense for its Applied Research Laboratories, which develop in five separate labs everything from Navy surveillance systems to 'sensing systems to support U.S. ballistic missile targeting' (Reed, 2001). MIT, one of the largest recipients of defense research money, has also been using its talented research-oriented faculty and students to develop remote sensing and imaging systems that would 'nullify the enemy's ability to hide inside complex mountain terrains and cityscapes' (Edwards, 2006). Universities around the country are funded to do similar military-oriented research, producing everything from global positioning systems to undersea surveillance technologies.