



MONITORING THE GLOBAL PRIVATE MILITARY AND SECURITY INDUSTRY

What do we know,
what do we need to know,
and how can we know it?

Deborah Avant
Mark Berlin
Karl Kruse

IGCC Occasional Paper No. 4

MONITORING THE GLOBAL PRIVATE MILITARY AND SECURITY INDUSTRY

**What do we know, what do we need to know,
and how can we know it?**

Deborah Avant

Mark Berlin

Karl Kruse

**Report on a conference held at the
University of California, Irvine
January 27–29, 2011**

Sponsored by

UCI's International Studies Program and Center
University of St. Gallen's Center for Security, Economics, and Technology (CSET)
Center for Democratic Control of Armed Forces (DCAF)
Office of Research, UC Irvine
UC Institute on Global Conflict and Cooperation
Center for Global Peace and Conflict Studies, UC Irvine



**IGCC Occasional Papers
on International Security and Cooperation**

Monitoring the Global Private Military and Security Industry

What do we know, what do we need to know, and how can we know it?

Deborah Avant
Mark Berlin
Karl Kruse

Defining the Challenge

Since the 1990s a global private military and security industry has emerged and boomed. The industry offers opportunities for both states and non-state actors to pursue goals that require security services. Activist, analysts, and states all have raised concerns, however, that these forces can operate outside of the law and/or in a manner inconsistent with the obligations of and international laws and norms.

In response to these concerns, a variety of initiatives (by the Swiss government, the U.S. government, the International Committee of the Red Cross, the United Nations and others) have converged around the need for regulation. These initiatives generally agree on appropriate categories of military and security services to be regulated as well as on the responsibilities of contracting states, home states, host states, and companies under international law. Governments, industry officials, and international organizations have similarly supported the principles underlying an International Code of Conduct and indicated interest in developing and supporting global standards for the industry.

A 2009 gathering of experts on the PMSC industry in Geneva noted the convergence among regulatory efforts but bemoaned the fact that the actual behavior of these forces (as well as those who contract with them) is still opaque. Lack of systematic information about the industry poses problems for those researching it, for those attempting to regulate it, and even for industry members seeking recognition for proper behavior. Without access to information it is difficult to evaluate whether companies and their clients are abiding by their legal and ethical responsibilities. Publicly available information is crucial both to the success of regulation and to systematic academic research on the impacts of this industry.

Accordingly, the conference “Information for Monitoring the Global Private Military and Security Industry” was designed to address the issue of information via several steps: 1) assessing what information is needed to support various regulatory initiatives; 2) cataloguing what information is already being collected and by whom; 3) discussing what information can be shared and the best way to share it; and 4) brainstorming about how to collect additional requisite information.

During the introductory session, the conference organizers noted their commit-

ment to transparency and belief that academic institutions could contribute to the regulation of this industry in positive ways via research and analysis. They noted an information wish list that would include information about: consumers of military and security services; suppliers of these services; regulators of these services; and alleged misbehavior and responses to it. More generally, researchers are also interested in information relevant to assessing the effectiveness of the various sorts of regulation—from market power to industry self-regulation to multilateral efforts. Academics are concerned with what is being regulated in different instances (behavior of companies, behavior of clients, behavior of individuals), how regulation is taking place, and through which mechanisms. One of the conference organizers noted that the various stakeholders in regulatory processes thus far had not included academics but now it was time to bring them to the table.

In the discussions that followed, two definitional concerns were raised, one having to do with the industry and the other with the appropriate stakeholders.

Defining the industry

A number of participants pointed out the need to define and classify the universe of companies before talking about regulating them. When we talk about “private security companies” or “contractors,” do we refer only to those services involving armed personnel, or do they include logistics and development services as well? Companies involved in the private military and security services industry provide services that fall into three broad categories. First, logistics and support services aid in the everyday supplying of food, fuel, and other key provisions to military forces. Second, private security services provide protection of persons, places, and things. This protection has been in high demand in Afghanistan and Iraq but there is also an increasing demand for maritime security services in light of the threat of piracy, particularly off the Horn of Africa. Finally, reconstruction services include security sector reform, military training, law enforcement, and development efforts in conflict zones. There are a number of additional services such as intelligence support, risk assessment, and interrogation that do not fit neatly into any of these categories.

Some participants cautioned that the oft-used term “private military companies” might be a misnomer, as they claimed that no legitimate private companies perform actual offensive operations. The conference organizers pointed out their intention to examine the range of services specified in the Montreux Document, which focused on Private Military and Security Companies (PMSCs)—private business entities that provide armed guarding and protection, maintenance and operation of weapons systems, prisoner detention, and advice or training for local military and security forces—as well as those specified by U.S. Commission on Wartime Contracting, which focused on logistics, security, and reconstruction services.

Classifying PMSCs is complicated by variation in a number of structural features of firms. For example, some PMSCs consist of just a handful of employees, while others are large, publicly-traded corporations. Many PMSCs are based out

of large consumer states, such as the United States and the United Kingdom, while others are indigenous to the states in which they operate. Some PMSCs hire mostly ex-military or police personnel from their home states, while others draw heavily on “third-country nationals” (TCNs). Some PMSCs have truly global reach while others are focused on particular regions or countries. Finally, some PMSCs project a high-profile public image, while others remain relatively anonymous. Such variance in the function and character of PMSCs makes attempts at categorization challenging.

Relevant stakeholders

One must also define who has a stake in emerging governance structures for the industry. Relevant stakeholders go beyond governments, organizations, and individuals who hire PMSCs. While important stakeholders, these groups represent only a portion of the entities concerned with the regulation of the industry. The populations who live where PMSCs operate, human rights organizations, inter-governmental organizations, as well as domestic and international courts all affect and are affected by the private military and security industries. The input and cooperation of all of these actors are crucial for comprehensive regulation, and thus any information gathering effort must tap this variety of perspectives. The conference hosted stakeholders representing governments, industry groups, human rights groups, the media, the United Nations, attorneys involved with the industry from various perspectives, think tanks, and academia. Voices of the populations who live where PMSCs operate, however, were represented only indirectly through human rights groups. A recurrent theme throughout the conference was the need to better tap input from these populations.

The Current State of Regulation

Addressing a broad and general audience at UCI, the first panel outlined the global PMSC industry as well as the current state of regulation for PMSCs.¹ Outlines of the industry focused on many of the features outlined in the previous section. The current state of regulation addressed the efforts of industry groups, multi-stakeholder initiatives, and U.S. government initiatives.

Some firms and industry groups are making efforts towards self-regulation. Many firms have a code of conduct and internal ethics program in place. Approximately 70 companies belong to one or more industry associations such as the Private Security Company Association Iraq (PSCAI),² ADS Group, the British Association of Private Security Companies (BAPSC),³ or the International Stability Operations Association (ISOA).⁴ Each of these industry associations attempts

1. More information about the panel available at: <http://internationalstudies.ss.uci.edu/node/2025>. Video link available at: <http://ocw.uci.edu/lectures/lecture.aspx?id=439>.

2. <http://www.pscai.org/>.

3. <http://www.bapsc.org.uk/default.asp>.

4. <http://ipoaworld.org/eng/>.

to promote accountability and compliance with existing rules and gives input on the creation and implementation of new ones. ISOA, for instance, has a code of conduct, internal grievance process, and standards board.

Another industry group that deals with security contracting, if not international contracting as discussed here, is ASIS International.⁵ ASIS provides education, training, and guidelines for the private security profession. Currently ASIS does not deal specifically with companies who provide services in conflict zones, but their programs confront similar issues regarding the vetting, training, and certification of private security personnel. ASIS administers a number of its own internationally-accredited certification programs for security practitioners. It is also involved in developing industry standards and guidelines through the ASIS International Standards and Guidelines Commission.

Beyond the industry, several multi-stakeholder initiatives aim to harmonize regulatory efforts, chief among them being the Montreux Document and the International Code of Conduct. The Montreux process was initiated by the Swiss government and the International Commission of the Red Cross (ICRC). It reflects the participation of eighteen country representatives, including the United States, in consultation with industry and civil society groups. The idea was to clearly outline the responsibilities of states in their relations with PMSCs.⁶ The Montreux Document does not establish new law, but instead describes and clarifies the responsibilities of states and PMSCs under existing international humanitarian and human rights law. It also seeks to aid states and PMSCs in meeting their legal obligations by outlining “good practices” for states that contract with PMSCs (contracting states), states where PMSCs operate (territorial states), and states from which PMSCs or their employees hail (home states).

The International Code of Conduct (ICoC) for private security providers is a multi-stakeholder initiative that pledges signatories to the principles articulated in the Montreux Document. The document was the result of an inclusive drafting process initiated by companies and industry associations and coordinated by the Swiss government, with strong support from the United States, Great Britain, and civil society organizations. So far the ICoC pertains only to those companies providing security services,⁷ but it is meant to be expanded to cover the full range of companies providing contingency services in the field. Signatories “affirm that they have a responsibility to respect the human rights of, and fulfil humanitarian responsibilities towards, all those affected by their business activities.”⁸ The ICoC outlines specific rules regarding the use of force, vetting and training of personnel,

5. <http://www.asisonline.org/>.

6. See The Montreux Document, available at: <http://www.eda.admin.ch/psc>.

7. Which it defines as “guarding and protection of persons and objects, such as convoys, facilities, designated sites, property or other places (whether armed or unarmed), or any other activity for which the Personnel of Companies are required to carry or operate away from in the performance of their duties.”

8. See The International Code of Conduct for Private Security Providers, available at: <http://www.icoc-ppsp.org/>.

and the reporting of incidents. The document also initiates a path forward towards the establishment of a third-party governance and oversight mechanism that will eventually monitor, certify, and enforce compliance; field complaints; and investigate violations. It is hoped that clients only hire providers that have signed and comply with the Code and that the Code will improve the human rights performance of the industry. A multi-stakeholder steering committee has been established that will oversee the development of the Code's oversight and governance mechanisms. The goal is to have an operational plan for the oversight mechanism by the end of November 2011. Once in place, the independent governance and oversight mechanism will assume responsibility for the Code's further administration and maintenance. In addition, the ICoC calls on signatories and stakeholders to aid national standards bodies in harmonizing their standards with those established in the Code.

As well, the Voluntary Principles on Security and Human Rights (VPs) provides nonbinding guidelines designed with extractive and energy industry companies in mind. The goal is to provide these companies guidance on how to maintain "the safety and security of their operations within an operating framework that ensures respect for human rights and fundamental freedoms."⁹ The VPs were the result of a cooperative effort by the U.S. and U.K. governments, extractive and energy companies, and human rights and other civil society groups. The VPs focus on ensuring that companies conduct risk assessments and due diligence with regard to both private and public security options. In so doing, the VPs specify a number of good practices to guide companies in their use of private security companies. These guidelines call on companies to ensure that PMSCs they contract: have clear policies on the use of force; do not engage in offensive or any other types of operations that are the responsibility of state forces; do not employ individuals with records of misconduct; are adequately monitored by clients or third parties and any allegations of misconduct or abuses investigated. At a 2009 plenary, participants also adopted a number of measures to facilitate the implementation of the VPs. These included new membership criteria that would make participation contingent on companies meeting reporting requirements. The 2009 meeting also encouraged implementation through "in-country processes" such as training workshops, meetings, and awareness-raising initiatives.

More generally, the United Nations "Protect, Respect, and Remedy" Framework for Business and Human Rights (UN Framework) serves as a reference for providers and clients (both state and private) alike. Developed by UN Special Representative and Harvard professor John Ruggie, the UN framework aims to outline the responsibilities of states and companies (including PMSCs and firms that hire them) regarding the potential impact of companies on human rights. The non-binding framework calls on companies to exercise due diligence, that is: "steps a company must take to become aware of, prevent, and address adverse human

9. See The Voluntary Principles on Security and Human Rights, available at: <http://www.voluntaryprinciples.org/>.

rights impacts.”¹⁰ This includes assessing how such factors as a company’s business partners, the local context within which it will operate, and the record of the host state’s government may conflict with its responsibility to respect and protect human rights. While the UN Framework currently lacks compliance or oversight mechanisms, in June 2011 Special Representative Ruggie will submit a set of guiding principles for its implementation.

Thus far, none of these initiatives creates binding obligations for states or other actors, but instead they attempt to establish a common set of principles by which states, companies, and others should operate.¹¹ This type of regulation relies largely on clients to police those they hire. This means that clients need access to several types of information vis-a-vis the personnel and companies they might hire. First, clients conducting due diligence in their contracting practices need access to information about companies’ personnel to ensure that personnel are properly vetted, trained, and certified as stipulated by the Montreux Document and the ICoC. Second, efforts to oversee and prosecute individual violations require information collected from field. As such, the ICoC stipulates procedures for reporting of incidents involving any use of a weapon by contractor personnel. Also, injuries or deaths of contractor personnel are not subject to the same reporting requirements under government rules as are military personnel. Therefore, it is important that additional monitoring mechanisms are in place to guarantee that such information is reported accurately and reliably.

In response to events in Iraq and Afghanistan, the U.S. government has further developed regulations and oversight mechanisms relevant to the PMSC industry. Consistent with the guidance in the Montreux Document, the Department of Defense has issued specific instructions on the use of private security companies (PSCs). These companies must operate according to public law and the laws of land warfare. Their duties are limited to guarding people and places. They are not allowed to engage in “offensive” actions, although there is still an active debate within the U.S. government about appropriate functions for security contractors.

Government contracts for PMSCs are subjected to a pre-award review to ensure that company personnel are properly licensed, trained, and vetted. The United States has also implemented a quarterly census through which it tracks all contracted personnel in contingency operations, and has developed more specific regulation and tracking of those contractors who provide private security functions. The 2011 National Defense Authorization Act extends this more specific guidance to private security contractors operating not only in contingency operations but also in combat operations or other significant military operations around the globe.

10. See The United Nations “Protect, Respect, and Remedy” Framework for Business and Human Rights, available at: <http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf/>.

11. Though the ICoC is currently engaged in a process to build an international oversight and compliance mechanism with which Signatory Companies would be contractually obligated to comply.

During contract execution, companies are subject to existing laws in both the United States and the host nation. For example, the Military Extraterritorial Jurisdiction Act (MEJA) allows the United States to exercise extraterritorial jurisdiction over contractors or civilians under Department of Defense (DoD) contracts and who commit federal crimes in the field. MEJA, however, only applies to individuals accompanying military forces. This has caused difficulty in attempts to prosecute crimes committed by contractors who accompany these other agencies, as demonstrated in the case of the Nisour Square incident.¹²

There remain substantial gaps in the capacity of the U.S. government to oversee the activities of PMSCs. A large and continuing problem is the lack of well-trained contract officers. This problem has been recognized by the GAO, the CRS, the CWC, the Special Inspectors General for Iraq and Afghanistan, and the Department of Defense.

A variety of U.S. efforts are underway to enhance the regulation of PSCs. Some of these are unilateral. For instance, Congress has debated developing a Civilian Extraterritorial Jurisdiction Act (CEJA) in order to apply federal law to contractors accompanying government agencies such as the State Department and USAID just as MEJA applies such law to those accompanying the military. A good amount of U.S. energy, however, is directed toward supporting international and multi-stakeholder initiatives such as the ICoC. The United States is eager for global standards that will “raise the bar” for consumers and providers of security services around the world.

What Information Is Out There?

There are currently numerous data collection efforts of varying scope, depth, and focus that cover the PMSC industry. Conference participants discussed initiatives that address the size and shape of the industry as well as ways to evaluate company performance. They were interested in organizing information with regard to firm responsibilities both to their customers and to their publics.

Much of the existing information is concentrated in the United States. As a leading consumer of military and security services, the United States has collected a variety of data pertaining both to corporations in general as well as government contracts. Some information helps observers understand what sort of work is being done by whom. Upcoming and active contract solicitations can be found at FedBizOps.gov.¹³ Those looking to understand and track trends on U.S. government spending by region or company may find a user-friendly interface at USASpending.gov.¹⁴ The Federal Procurement Data System (FPDS) is a compre-

12. Steve Fainaru and Saad Al-Izzi, “U.S. Security Contractors Open Fire in Baghdad: Blackwater Employees Were Involved in Two Shooting Incidents in Past Week,” *Washington Post*, May 27, 2007, A01.

13. <http://www.fbo.gov>.

14. <http://usaspending.gov>.

hensive central database for U.S. government contracts.¹⁵ This resource offers information on U.S. federal government contracts including size, location, and company information. Although some participants pointed out that it is not entirely reliable and prone to mislabeling and entry errors, it nonetheless contains much useful data on the number, cost, and mandate of individual contracts. The Department of Defense's Office of the Assistant Secretary of Defense for Program Support provides information on applicable regulations for contingency contracting, regulatory changes, relevant congressional reports, and quarterly census reports.¹⁶

Other data sources provide insight into the how companies perform while executing their contracts. The Department of Defense has in its possession numerous "SPOT" reports made by military officers in operational areas. As of now, those remain classified and not open for public review. The Department of Labor's Office of Workers Compensation maintains a public database on workplace injuries and deaths for contractors.¹⁷ Statistics here, based on Defense Base Act workers compensation insurance claims, can be sorted by employer, insurer, and by date. But as one panelist noted, without the proper context, it is difficult to know whether such incidents represent irresponsible performance or merely higher-risk work. The Department of Defense Task Force on Wartime Contracting (TFWC) has issued a number of reports that identify and address existing problems with the procurement and oversight of private security companies. The DoD Inspector General's report "Hard Lessons: The Iraq Reconstruction Experience" also highlighted many issues relating to the use of private security companies in reconstruction efforts. The Special Inspector General for Iraq Reconstruction and Special Inspector General for Afghanistan Reconstruction produce periodic reports on contracting activities in those areas.¹⁸ Several participants pointed to the non-partisan Congressional Commission on Wartime Contracting (CWC) as a source of valuable information. Other U.S. government agencies, including the Congressional Research Service (CRS) and the Government Accountability Office (GAO), have also produced useful studies. These reports are particularly valuable in uncovering and presenting information that would otherwise not be publicly available.

Participants noted that governments beyond the United States are engaged in their own efforts to track the industry, though often at arms' length. Some of this occurs through non-governmental or quasi non-governmental organizations. Britain's Security Industry Authority (SIA), for instance, gathers information on the individuals that it licenses while maintaining a register of "approved contractors." It should be recognized that the SIA's principal remit is the improvement of standards in the delivery of unarmed security services within the United Kingdom. The Center for the Democratic Control of Armed Forces (DCAF) is funded in part by the Swiss government, but has 54 other governments as members. The "private-

15. https://www.fpds.gov/fpdsng_cms/.

16. <http://www.acq.osd.mil/log/PS/bio.htm>.

17. <http://www.dol.gov/owcp/dlhwc/IndustryDBAPerformanceResults.htm>.

18. <http://www.sigir.mil>.

securityregulation.net” portion of DCAF’s website features a database of regulations facing PMSCs in 50 countries, as well as toolkits for companies, civil society, and governments seeking to bring greater accountability to the private security sector. DCAF is also instrumental in promoting the implementation of the Montreux Document and the ICoC. The icoc-psp.org website contains a list of the Signatory Companies, which as of this writing numbers 94. The Global Consortium on Security Transformation (GCST), started initially by the Canadians and the British, is also active in broad security sector reform and produces reports along those lines.

Insight from firms and the industry itself is not to be overlooked. Some conference attendees lamented the homogeneity of company websites. However, a few attendees noted that these sites can serve as a good starting point for gathering information about a given company. The websites of industry associations like ADS Group, BAPSC, PSCAI, or ISOA contain general information on association members. The ISOA website in particular contains information on the services particular companies provide at the locations of their offices worldwide.

Much of the initial information on the industry came through the work of journalists. These reports play a critical role both in informing publics and are a resource for some academic work on the industry. The project at the Free University (described below), for instance, is sourced from news publication databases such as LexisNexis. Journalists base their reports on individual sources (often anonymous competitors, disgruntled employees, or government minders), industry sources, publicly available government sources, and personal experience. The best reporting uses all of these and results in concentrated investigative work. A good example is the “Disposable Army” series available through ProPublica, which documents contractor casualties and how the U.S. government is dealing with them.¹⁹

Attendees commented that such nuanced and in-depth information about PMSC operations and performance, as well as information on specific firms, brings to light things that slip through the cracks of structured government reporting mechanisms or academic accounts. Many thought that the work of journalists might be better suited to identifying idiosyncratic or cultural elements of particular firms, which in turn helps observers understand past behavior and get an idea of how firms may behave in the future. Attendees noted, however, that the work of journalists has its own limitations. Informants may be unreliable or driven by personal agendas, such as retaliation against a former employer or undermining the competition. Nevertheless, journalists, especially when embedded with troops or PMSCs, can provide an on-the-ground picture of firms’ behavior that is lacking in many of other sources.

Information has also been provided by human rights advocates. Some of these focus specifically on the global military and security industry. The International Committee of the Red Cross sponsors a project on the privatization of war, publishing reports that focus on international humanitarian law and how it relates to

19. <http://www.propublica.org/series/disposable-army>.

the industry.²⁰ Organizations like Corpwatch.org have been following the industry in the United States for most of the decade and have compiled a number of news stories, reports, and company profiles. Human Rights First has produced a project aimed at “ending contractor impunity,” which contains a number of reports on events, cases, and the legal situation regarding contractors.²¹

Other human rights groups focus more on the corporations that hire either PMSCs or government troops to secure themselves. RAID (Rights and Accountability In Development) is such an organization. It provides information on corporate activity in ill-governed parts of the world. While these organizations can accomplish much when it comes to monitoring, one panelist lamented the fact that many of them work in the EU/UK legal context where, given privacy and libel laws, they can share very little information without the explicit permission of those on whom they are reporting. Thus, only through novel ways of collecting and distributing information can these NGOs have much impact. These organizations may be useful partners, however, for tapping into local voices of populations around whom PMSCs work.

Humanitarian NGOs have had increasing contact with the PMSC industry given their work on the ground. Some of this has come as these organizations have been compelled to develop their own security planning and have worked with PMSCs to do this. InterAction, for instance, has produced its own compendium on NGO security and risk mitigation.²² Other contact has come as all actors on the ground in conflict zones (NGOs, corporations, governments, and PMSCs) have begun to share information on attacks. There are processes for sharing such information in several conflict ridden areas.²³ Again, InterAction has developed principles for this sort of information sharing.²⁴

A number of academic-led initiatives seek to examine various aspects of the private security industry. At the Free University of Berlin, the “Private Security Database” project gathers information on government actors (such as states, the UN, and NATO) that use PMSCs and has compiled a database lending itself to quantitative analysis. The project data portrays “who consumed private security in Areas of Limited Statehood (where, how long) and what kind of security was consumed.”²⁵ By examining news stories retrieved online, this project breaks down

20. <http://www.icrc.org/eng/war-and-law/contemporary-challenges-for-ihl/privatization-war/overview-privatization.htm>.

21. <http://www.humanrightsfirst.org/our-work/law-and-security/ending-contractor-impunity/>.

22. <http://www.interaction.org/ngo-security>.

23. Abby Stoddard, Adele Harmer and Victoria DiDomenico. “Providing Aid in Insecure Environments 2009 Update” HPG Policy Brief 34 (Humanitarian Policy Group, Overseas Development Institute, April 2009).

24. John Schafer and Pete Murphy, “Security Collaboration: Best Practice Guide,” InterAction Resource Paper, September 2010.

25. <http://www.branovic.com/projects.html>.

contracting relationships between companies and government bodies with each mention of a relationship in a year counted as that company having a link for that year. Each link must be confirmed through three sources, making this a rigorously tested database, sometimes even excluding possible links at the expense of ensuring accuracy.

EUI's PRIV-WAR project looks specifically at legal and regulatory initiatives vis a vis the security industry. Over the past two years, PRIV-WAR scholars have produced multiple publications regarding the status of regulation in the industry, including a large edited volume, *War by Contract*.²⁶ These efforts outline legal requirements that face firms and those who hire and monitor them. They also go into some depth about existing case law in the international context and how it pertains to PMSCs.

Other initiatives discussed include a project organized by Molly Dunigan (RAND) and Ulrich Petersohn (ETH Zurich) called "Markets for Force," which focuses on the different regional dynamics within the global market. The project will hold a workshop and several panels at the 2011 ISA annual meeting in Montreal. Attendees also referred to relevant expertise at the University of Ottawa (Michael Williams and Rita Abrahamsen), DePaul University, National Defense University (TX Hammes and Sean McFate) and Harvard University.

Think tanks and their products surfaced as useful sources numerous times throughout the conference. The Center for New American Security sponsors a project on contracting in conflicts, focusing on evaluating past performance and making concrete recommendations for future policies.²⁷ RAND Corporation researchers have also engaged the issue, offering monographs and Congressional testimony that is available on the organization's website.²⁸ The Center for American Progress offers a series on contracting with regards to the U.S. government and human rights issues in Iraq and Afghanistan.²⁹

Despite all these sources, attendees noted that crucial information shortfalls remain. First, most of this data pertains to PMSCs hired by governments, in particular the U.S. government. Attendees expressed concern that the existing data accounts for only a portion of the total industry at a time when private consumption of PMSC services is growing. A large share of PMSC services are consumed by other private actors, such as extractive service firms. There is little publicly available information on these types of private-to-private transactions. Some PMSCs are publicly traded companies, and thus are more transparent due to reporting requirements. But many PMSCs, as well as their clients, are privately held corporations and are not required to disclose information.

26. Francesco Francioni and Natalino Ronzitti, eds. *War by Contract: Human Rights, Humanitarian Law, and Private Contractors* (Oxford: Oxford University Press, 2011).

27. <http://www.cnas.org/node/3666>.

28. http://www.rand.org/content/dam/rand/pubs/testimonies/2010/RAND_CT349.pdf.

29. <http://www.americanprogress.org/issues>.

Second, participants pointed out that many government consumers of PMSC services are not inclined to dedicate the kind of resources to compile and report relevant information that the United States has. Also, many PMSCs are based in territories that do not have the same disclosure rules as American firms. Finally, there is very little information on PMSC personnel themselves. Do employees have criminal records or histories of mental health problems? Do they have records of negligent behavior? This data is even more limited on host-country personnel or third-party nationals. Even if this information were collected, privacy considerations make dissemination of it difficult.

What Information Do We Need to Make Oversight and Regulation More Effective?

Participants agreed that performance data is necessary at all levels of the process, to ensure consumers can make informed decisions about hiring, to encourage appropriate behavior (by individuals working for PMSCs, PMSCs, and PMSC clients), to enable oversight, and to allow for adjudication of alleged misbehavior. While all who were present agreed on the need for more information than is currently available, there were different views about who needed to know what. There was also some tension about the most important purpose for information. Some tended to see such information as providing better accountability to clients, while others emphasized the need for accountability to populations impacted on the ground. Still others saw information as important not only for oversight but also for putting in place preventative measures to reduce the chances for misbehavior in the first place.

Most attendees agreed that it was important for companies to collect information about personnel to help them exercise scrutiny in their hiring practices. For companies, access to criminal and mental health records would be useful in evaluating potential personnel. Access to information regarding the amount and type of training PSC personnel have received, as well as their service records, would help both clients and providers make more informed acquisition decisions. How to practically share such information, however, was not obvious. The idea that companies might have or share a “blacklist” of employees with a history of poor behavior was discussed, but dismissed due to questions of fairness, transparency, and legality.

Information on companies is also vital to the interests of both clients and publics. Participants pointed out that clients included not only governments but also intergovernmental organizations (like the UN), NGOs, and commercial actors. All of these clients have an interest in hiring PMSCs that will behave properly and all could benefit from knowing how to judge PMSCs and contract with them in a way that will reduce the prospects for poor behavior.

What information might clients want to know? Knowledge about equipment levels, skills, training, tax/license status, and staff turnover were all mentioned as potentially important. At a more abstract level, understanding about company ethos, trade association membership, and relationships with particular governments could also help clients make better acquisition decisions. Several par-

ticipants throughout the conference noted that the “culture” of an organization greatly influences the behavior of its personnel. To this end, some suggested that attention to a firm’s policies regarding alcohol consumption might be useful for gauging the likelihood that its employees would misbehave. Similarly, examining a company’s policies on the use of force may also provide a useful gauge of a company’s commitment to responsible conduct. Finally, one may consider a security firms’ psychological screening process. Because such screening is very costly and not required by most contracts, such policies may serve as indicators as to which firms are more proactive about ensuring responsible conduct.

Discussions regarding information about PSC clients raised a number of issues for the attendees. Some voiced the support for asking companies to identify their customers. This could enable scrutiny of clients that repeatedly hire PSCs that misbehave. Most agreed, however, that gathering and sharing this kind of information might not be feasible.

Some participants noted that industry standards have the potential to encourage proper behavior regardless of client choices and could be very beneficial to clients with less expertise in contracting for security. There was concern among some attendees about how standards should be developed: through national standards processes such as the American National Standards Institute (ANSI) or through multi-stakeholder processes such as the ICoC? Others, however, argued that ANSI processes were actually multi-stakeholder—or at least consultative—and could be complementary to the ICoC process. Some participants remained concerned that ANSI is primarily industry driven and does not have clear decision-making processes that balance power among relevant stakeholder groups.

Several attendees pointed out that the current moment presented a unique window of opportunity for standardizing the PSC industry. As one participant noted, the purchasing power of the United States has led to a “Wal-Mart effect” whereby U.S. practice largely shapes the activities of the whole industry. Because the United States is, at present, very interested in clear and strong standards for private security providers, it could impact the development of standards for this segment of the industry across the globe. U.S. market power, however, may soon be on the wane as it winds down its operations in Iraq and looks forward to doing the same in Afghanistan. Reduced U.S. power could lead to less uniformity in the industry, making it harder to control. Many agreed that the time is ripe to create clear and strong standards now through whatever process was the most expedient rather than waiting for a particular process and risking more challenging circumstances.

Attendees also considered whether information regarding the “outcomes” of private security work merited emphasis. This discussion revealed a tension between those who viewed information as a means to better serve clients and those who viewed information as a means to better serve broader publics. The former view tends to see the issue of accountability through a “contract law frame,” emphasizing the need for information on provider performance and compliance with regulations. “Outcomes” in this sense are more tied to mission success and meeting

client expectations. This view emphasized the use of financial sanctions and other “bottom-line” measures to secure compliance. The latter view tends to see the issue more through a “public law frame,” emphasizing the need for information to ensure criminal accountability and redress for victims of negligent behavior. This latter view emphasized the role of prosecutions in inducing compliance and evaluated “outcomes” in terms of the impact on populations on the ground.

These two views need not be completely opposed. Some attendees emphasized the importance of putting in place robust complaint mechanisms to allow information about security provider practices on the ground—including how they affect individual members of the public—to be available to clients. This could encourage client knowledge about, and concern with, the effect of their choices on those around whom PSCs operate. In this situation, contract law could be a useful vehicle for holding companies accountable and thus changing corporate culture in order to reduce the potential for abuses to more general public concerns.

Industry and government participants generally endorsed the view that some kind of complaint mechanism would be useful. Some participants from the human rights community, however, claimed that any reporting system without a process whereby complaints could be verified and remediated would be problematic. Without a promise of remediation, there would be no incentive to lodge complaints in the first place and without verification reporting mechanisms could be abused by competitors.

There was some general discussion of the need for need for understanding about the long term on-the-ground impact of PMSCs. Several participants noted past problems with PMSCs empowering certain elements relative to others within a community by, for example, opening flows of money, weapons, and ammunition. Many also pointed out that security companies have previously been accused of contributing to a human trafficking industry in the Balkans and Kosovo. Others pointed out that construction projects in Afghanistan sometimes drive the price of cement so high as to make indigenous projects impossible. Some thought it desirable to gather information about results in communities 5-10 years after a company’s engagement to determine that company’s impact on the ground. However, considering the complex mix of factors involved, many participants pointed out problems with directly attributing the success or failure of such efforts to PMSCs alone.

Many agreed that the most important factor for long-term community success and industry accountability is for their customers to do their due diligence and take “ownership” of their contracts. To facilitate this, discussion turned to the idea of centralized information centers through which industry observers, governments, potential customers, and the industry could access the types of knowledge discussed above. Access to such data could enable more thorough oversight and due diligence efforts, thus increasing the accountability of firms and their customers. If firms and their clients are truly interested in improving human rights performance, this kind of information could be useful. Some attendees doubted, however, that voluntary reporting would be a promising avenue toward true accountability. At-

tendees also recognized that the costs of gathering such information and making it accessible, as well as protecting the privacy of individuals and the intellectual property rights of firms would make any centralized effort of this sort especially challenging.

Finally, there was widespread consensus that information should not be collected for its own sake. Information is power and can be misused. For example, as one participant observed, a database that documented instances of weapon discharges by security personnel could be seen as providing a useful mental shortcut for gauging the discipline of a company—but if knowledge about weapons discharges is gathered via self-reporting, it could also be seen as punishing those companies that take their self-reporting most seriously. While many in attendance thought information about improper weapons discharges would be valuable, collecting that data in a reliable way that would not be subject to misuse would require careful thought.

Challenges to collecting and sharing information

Discussions then turned more fully to the prospects for and challenges of information collection. It was generally agreed that access to knowledge was uneven. Though many wished for more publicly accessible information, most agreed that significant hurdles exist in the collection and/or sharing of publicly accessible data. Some obstacles, alluded to above, included practicality, privacy, and reliability. More fundamentally, debates about what different types of information would be used for continued to generate debate in the group.

There was consensus that uniform access to information was absent in the current situation. Participants cited Wikileaks data to point out that the US government has access to a wealth of information through various mechanisms including SPOT reports from the field. However, due to operational security concerns, much of this data is classified and deemed not suitable for distribution. PMSCs are likely to be slow to share information regarding employees or other firms because of employment or libel laws. Publics in the US and other western countries have access mostly to information available in the media. And publics around whom security forces work as well as human rights groups have only anecdotal information. While full and free information sharing could bolster both the democratic bona fides and effectiveness of regulatory initiatives, it is likely that existing statutes and institutional structures will preclude sharing everything with everybody.

Participants discussed a variety of models for collecting and sharing industry information. One approach modeled itself after the Better Business Bureau (BBB). In such a system, the complainant is put directly in touch with company management, encouraging the parties to resolve disputes on their own.³⁰ Also mentioned

30. This model was discussed in contrast with the project-centric monitoring system used by the International Finance Corporation (IFC) which applies to any company who is a member of that WorldBank Group and is based on issues of cultural appropriateness and retribution prevention.

were models drawn from professional associations such as the U.S. State Bar Associations or American Medical Association. Some acknowledged that these may be useful for serving the interests of clients. There was substantial debate, though, as to whether business or professional models were appropriate for collecting complaints from affected publics in the field. Those most concerned with protecting human rights were skeptical about these models given the severity of harms inflicted, the absence of mechanisms for reviewing and verifying claims, and the violent environments in which private security companies generally operate.

When looking at hurdles to data collection, funding and practical problems were two primary concerns. While industry has a lot to gain from information that sorts compliant companies from non-compliant ones, an industry-funded initiative was seen by some as unreliable given the potential for undue industry influence. Practically, the geographic dispersion of PMSCs (where they are based, and where they operate) creates a unique challenge for gathering information. This is true for both clients, who may not be able to adequately oversee the PMSCs they contract with, and publics, who may not know about or be willing to participate in complaint mechanisms geared to western practices. Without a mechanism for verifying complaints such a database would be of limited value to clients.

A final set of challenges centered on two issues of legitimacy. The first, noted above, was over the legitimacy of a professional monitoring system for PMSCs that pose risks to basic human rights. Some pointed out that the very focus on professionalism betrayed a design centered on client wishes and might be contrary to the spirit and aims of protecting human rights.

The second, also noted above, was over the role of the United States. Some raised concerns about any standards or monitoring regime that might appear to be “lopsidedly American.” What incentives, some wondered, would non-U.S. firms with no aspirations to solicit American work have to participate in an American-dominated initiative? The obvious answer to this concern was to call for more involvement from the international community in developing a truly multilateral standards and monitoring regime. Echoing the earlier discussion, however, other participants pointed out that time is an issue. Multilateral regulatory bodies, such as the International Organization for Standardization, can take up to four or five years to issue new standards. The National Defense Authorization Act for Fiscal Year 2011 requires U.S. Secretary of Defense to determine whether the private sector has developed operational and business practice standards applicable to private security contractors as well as to develop a third-party certification process for determining whether private security contractors adhere to such standards.³¹ The law also requires the Office of the Secretary of Defense to (within 270 days) establish its own criteria for defining standard practices for the performance of private security functions and for weapons training programs for contractors performing private security function. Further, the Defense Department may require independent third-party certification to these standards as a factor in the evaluation of proposals

31. See Section 833.

for award of a covered contract. Some held that the time line imposed by Congress thus does not lend itself to more glacial multilateral processes. Other participants worried about the development of gaps between the United States and other actors if the United States created codes and enforcement mechanisms that could conflict with international ones.

The ensuing discussion led to some resolution of these legitimacy concerns. Professional standards were explained as a forward-looking way of managing risks. Setting client expectations to create conditions less likely to generate human rights abuses in the first place was portrayed as a complement to more traditional concerns with punishing human rights abuses. As far as the U.S. role was concerned, participants explained that the initial moves by the United States could be seen as a pilot initiative on which later initiatives could build.

As for the role of information, as one attendee pointed out, the duty of prime contractors or customers to oversee their own contractors cannot be seen as relieved by the International Code of Conduct or other oversight body. There were acknowledged to be numerous ways that information relevant to oversight could be useful for this purpose. Also, participants began to recognize that there might be many different informational tools relevant to different goals.

How to acquire and share information

Discussions about how acquire and share information focused on three ideas: 1) encouraging a marketplace of information; 2) whether gathering information about public grievances made sense; and 3) how to mine existing media and information sources to create more widely and publicly available short cuts to interested parties.

Encouraging a marketplace of information requires incentives that motivate companies and their clients to self-report. Ideas for such incentives included demands by governments that a PMSC be required to publicly disclose particular information in order to bid on contracts. Another focused on creating an information clearinghouse that, while geared towards consumers of PMSC services, would be open to outside scrutiny. Both providers and clients would contribute information about their own partners in exchange for access to information about others. Loosely based on the BBB model, participation in such a clearinghouse would help providers differentiate themselves based on quality. Consumers would have access to such information to inform their purchasing decisions. Also similar to the BBB model, a complaint mechanism could be introduced to this clearinghouse to increase accountability to other stakeholders. Some participants remained skeptical of how useful such a mechanism would be.

Some attendees were most interested in redressing public grievances. Some of them questioned, however, the usefulness of pursuing such complaints as an information-gathering exercise. Addressing public grievances, they suggested, is a process entirely separate from anything like an industry information clearinghouse. Security companies are not selling cars or consumer goods. PMSCs bring services to market that, if not monitored closely, can infringe on fundamental hu-

man rights. As such, some saw value in a grievance mechanism that would be accessible to people in areas where PMSCs operate but questioned the usefulness of linking such a mechanism to industry standards. Generally, attendees agreed on the importance of protecting the rights of individuals around whom PMSCs operate but did not settle on how or whether information about public grievances would contribute to that goal.

Finally, attendees called for systematic mining and presentation of existing data to keep track of the numbers and behavior of PMSCs. There was consensus that all in attendance had learned from one another. The creation of a one-stop website with up-to-date links to existing regulations, reports, publications (perhaps searchable by key words) and data about the industry would provide huge benefits. Also, a more digestible reporting system using the information gathered by the U.S. government to keep track of the deployment of contractors was endorsed by all. A PMSC index issued quarterly or biannually, modeled after the Brookings Institution's "Iraq Index" but much shorter and simpler, could simultaneously increase the transparency and visibility of contractors and demonstrate (or not) progress in managing them.

Sharing Information and the Ways Forward

Attendees recognized that it did not make sense to try to develop a single information-gathering or sharing strategy to address all the issues with industry oversight. One noted that an effective reporting device from a journalistic level might not be effective in addressing the needs of a government or industry actors. It was agreed that there were likely many different strategies that would be useful for different goals. Four concrete ideas emerged:

1. An online portal to connect all existing information sources

Many participants agreed that there was more information available than they had known about before the conference and that it would be very useful to have a one-stop online portal from which to link existing and emerging sources of information about the industry. While large amounts of information are available on the websites of DCAF, PrivWar, and the Global Consortium on Security Transformation,³² these efforts are not sufficiently linked, nor do they lend themselves to cross-referencing or compilation. And none of these make good use of the wealth of U.S. government sources. Currently, few outside of a select number of industry observers know of the existence of much of this information. Rather than re-invent the wheel, participants seized upon the idea of building a centralized information portal (perhaps in conjunction with existing sites that host clearinghouse portals for related information) through links with these and other projects. The organizers agreed to work together and consult with various clearinghouses to develop a proposal to create and maintain such a portal.

32. <http://www.dcaf.ch/Topics/Detail?lng=en&cid=121492>, <http://priv-war.eu/>, <http://www.securitytransformation.org/index.php>.

2. A PMSC Index

There was enthusiasm among both academic and think tank participants for the development of a PMSC index to track U.S. use of and control over PMSC personnel around the world. This would rely on the information available through the U.S. Departments of Defense and Labor on number of contractors, contractor injuries and deaths, and (available publicly as of April 2011) contractor performance. Several participants affiliated with think tanks expressed interest in working with the organizers to create the categories and a proposal for such an index.

3. Collecting information about complaints in areas where PMSCs operate

There was some interest in collecting information about public complaints in areas where PMSCs operate. Some suggested efforts to connect via human rights groups with local NGOs and others who might provide a trusted mechanism for gathering information from the field. This might be relevant to the future decisions of clients but it could also be a mechanism through which local populations could be educated about tools for redressing their concerns. Although there were doubts about whether competencies for such an effort were present in the group, some participants affiliated with human rights groups expressed interest in working with the organizers and others to develop a pilot proposal based in one country or region to work toward this goal.

4. An annual conference as a way of maintaining a network of interested parties

Many participants noted that the conference itself had been a tool for sharing information and connecting people familiar with different portions of this interconnected industry. Continued annual meetings of this group—perhaps expanded a bit—could do a good deal to maintain momentum on this important topic.

ABOUT IGCC

Since 1983, the University of California Institute on Global Conflict and Cooperation (IGCC) has facilitated innovative work on the causes of international conflict and cooperation. Based at UC San Diego, IGCC uses its UC-wide networks to build project teams that cross both disciplinary and institutional boundaries. IGCC is committed to educating the next generation of international problem-solvers and peacemakers through its research and training activities.

IGCC brings scholars together with diplomatic, military, and policy leaders to address critical global issues such as nuclear, biological, and environmental threats and regional security. Participants include representatives from the U.S. government, foreign governments, nongovernmental organizations, international organizations, think tanks, foundations, and universities at home and abroad.

IGCC disseminates the results of its work through publications, conferences, and policy seminars and briefings held at the UC Washington Center. IGCC builds bridges between the theory and practice of foreign policy by strengthening the intellectual foundations for effective policymaking, injecting fresh ideas into the policy process.

