Transparency International (TI) is the world’s leading non-governmental anti-corruption organization, addressing corruption and corruption risk in its many forms through a network of more than 100 national chapters worldwide.

Transparency International Defence and Security (TI-DS) works to reduce corruption in defense and security sectors worldwide.

Acknowledgements

This report was written by Michael Picard and Colby Goodman. Jodi Vittori provided critical leadership and insights to an earlier version of this report focused on one of the case studies. Several people within Transparency International provided valuable editorial assistance to this report. They include but not limited to Michael Ofori-Mensah, Ara Marcen, and Scott Greytak. Several Transparency International chapters also provided helpful editorial checks for this report. The authors would like to especially thank outside experts that completed a peer review of the current version of this report. This report was made possible with financial support from Carnegie Corporation of New York.
CONTENTS

1.0 Executive Summary 5
  1.1 Selected Recommendations 8
    1.1.1 Building a Stronger US Government Contracting Regime for PMSCs 8
    1.1.2 Bolstering US Oversight of PMSCs Sales to Foreign Governments 8
    1.1.3 Creating Stronger International Controls on PMSCs 9
  Box 1: What is a PMSC? 10

2.0 Private Military and Security Market and Corruption Risks 11
  2.1 Birth of the Modern PMSC 11
  2.2 US PMSC Global Market 13
    Figure 1: US Recipients of Military and Police Training and Related Corruption Risk Level 13
    2.2.1 US and Foreign Government Demand 13
    2.1.2 US PMSC Structure and Market 15
    Figure 2: Top US PMSCs Commitment to Transparency and Anti-Corruption Standards 15
  2.3 Foreign PMSCs and their Activities 16

3.0 Case Study: Knowledge Point 18
  3.1 An EDGE Company 18
  3.2 Conflicts of Interests 20
  3.3 Regional Conflicts 21

4.0 Case Study: TigerSwan 24
  4.1 US Oil Pipelines 24
  4.2 Afghanistan, Iraq, and Syria 26
    Box 2: Corruption in the Iraqi Kurdistan 27
  4.3 The Delta Crescent Arrangement 29

5.0 US Actions to Regulate PMSCs and Related Gaps 32
  5.1 US Multi-Lateral Efforts to Regulate PMSCs 32
  5.2 US Oversight of PMSC Contracts with the US Government 33
    5.2.1 Main US regulatory actions on PMSCs 34
    5.2.2 Key gaps in US oversight 35
    Table 1: Comparison of US Government guidance on anti-corruption measures by agency 36
  5.3 US Oversight of PMSCs Contracts with Foreign Entities 37
    5.3.1 Main US regulatory actions on PMSCs 37
    Table 2: Comparison of Current and Proposed Definitions of Defense Services 38
    5.3.2 Key Gaps in US Oversight 39
    Table 3: Which PMSC Services Require a US Government Export License? 40

6.0 Conclusion 41

7.0 Recommendations 43
  7.1 Building a Stronger US Government Contracting Regime for PMSCs 43
    7.1.1 For the Executive Branch 43
    7.1.2 For the Legislative Branch 44
  7.2 Bolstering US Oversight of PMSCs Sales to Foreign Governments 44
    7.2.1 For the Executive Branch 44
    7.2.2 For the Legislative Branch: 45
  7.3 Creating Stronger International Controls on PMSCs 46
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AANES</td>
<td>Autonomous Administration of Northeast Syria</td>
</tr>
<tr>
<td>ADAC</td>
<td>Abu Dhabi Aviation Company</td>
</tr>
<tr>
<td>BESC</td>
<td>Babylon Eagles Security Company</td>
</tr>
<tr>
<td>BIS</td>
<td>Bureau of Industry and Security</td>
</tr>
<tr>
<td>BRI</td>
<td>Belt and Road Initiative</td>
</tr>
<tr>
<td>CBO</td>
<td>Congressional Budget Office</td>
</tr>
<tr>
<td>DASD</td>
<td>Deputy Assistant Secretary of Defense</td>
</tr>
<tr>
<td>DDTC</td>
<td>Director of Defense Trade Controls</td>
</tr>
<tr>
<td>DoT OFAC</td>
<td>Department of Treasury’s Office of Foreign Assets Control</td>
</tr>
<tr>
<td>DS</td>
<td>Federal Acquisition Regulation System</td>
</tr>
<tr>
<td>DTAG</td>
<td>Defense Trade Advisory Group</td>
</tr>
<tr>
<td>EAIG</td>
<td>Emirates Advanced Investments Group</td>
</tr>
<tr>
<td>EAR</td>
<td>Export Administration Regulations</td>
</tr>
<tr>
<td>EW</td>
<td>Electronic Warfare</td>
</tr>
<tr>
<td>FARS</td>
<td>Federal Acquisition Regulation System</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal Year</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GDI</td>
<td>Government Defence Integrity Index</td>
</tr>
<tr>
<td>ICoC</td>
<td>International Code of Conduct</td>
</tr>
<tr>
<td>ICoCA</td>
<td>International Code of Conduct Association</td>
</tr>
<tr>
<td>ICRC</td>
<td>International Committee of the Red Cross</td>
</tr>
<tr>
<td>IGG</td>
<td>International Golden Group</td>
</tr>
<tr>
<td>IHL</td>
<td>International Humanitarian Law</td>
</tr>
<tr>
<td>ITAR</td>
<td>International Traffic in Arms Regulation</td>
</tr>
<tr>
<td>IW</td>
<td>Integrated information warfare</td>
</tr>
<tr>
<td>IGWG</td>
<td>Intergovernmental Working Group</td>
</tr>
<tr>
<td>JAC</td>
<td>Joint Aviation Command</td>
</tr>
<tr>
<td>KRG</td>
<td>Kurdistan Regional Government</td>
</tr>
<tr>
<td>MbZ</td>
<td>Sheikh Mohammed bin Zayed al-Nahyan</td>
</tr>
<tr>
<td>MEJA</td>
<td>Military Extraterritorial Jurisdiction Act</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NDAA</td>
<td>National Defense Authorization Act</td>
</tr>
<tr>
<td>PMSC</td>
<td>Private Military and Security Companies</td>
</tr>
<tr>
<td>PSC</td>
<td>Private Security Contractors</td>
</tr>
<tr>
<td>SDF</td>
<td>Syrian Democratic Forces</td>
</tr>
<tr>
<td>SIGAR</td>
<td>Special Inspector General for Afghanistan Reconstruction</td>
</tr>
<tr>
<td>SIPRI</td>
<td>Stockholm International Peace Research Institute’s</td>
</tr>
<tr>
<td>TAA</td>
<td>Technical Assistance Agreements</td>
</tr>
<tr>
<td>TCNs</td>
<td>Third-Country Nationals</td>
</tr>
<tr>
<td>UAE</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UNWG</td>
<td>United Nations Working Group</td>
</tr>
<tr>
<td>UPDF</td>
<td>Ugandan People’s Defense Force</td>
</tr>
<tr>
<td>USML</td>
<td>US Munitions List</td>
</tr>
<tr>
<td>WPS</td>
<td>Worldwide Personnel Protective Services</td>
</tr>
</tbody>
</table>
1.0 EXECUTIVE SUMMARY

As the United States transitions away from wars in Iraq and Afghanistan, US private military and security companies (PMSCs) are seeking new opportunities and foreign clients. Some of these new contracts with foreign governments have resulted in corruption-related scandals and challenges. In 2012, a former CEO of a major US PMSC pled guilty to bribing Nigerian officials for a US$6 billion contract to develop hydrocarbon infrastructure in the conflict-affected Niger Delta. In 2017, a US PMSC provided combat training to the Saudi operatives who would later gruesomely murder Jamal Kashoggi, a dissident journalist, in an attempt to quell perceived political opposition against the ruling Saudi royal family. In 2020, another US PMSC launched a botched incursion into Venezuela, reportedly seeking to topple the regime of Nicolas Maduro on behalf of local dissidents. A former US defense official has raised concerns about a US PMSC’s commercial activities in Somalia creating potential conflicts of interest with its US Government contract to train military units in Somalia.

Many governments around the world argue that PMSCs fill critical, security capability gaps quickly with relatively minimal costs. US PMSCs undoubtedly have provided essential services to the US Government. In Afghanistan and Iraq, for example, US PMSCs successfully guarded senior US officials and provided critical weapons maintenance services. Some of the US PMSCs have strengthened US partner nation military’s knowledge of combat tactics and military ethics. However, governments’ use of PMSCs has led to significant costs overruns and underperformance in US military operations. One US Government watchdog estimated that the United States lost almost one-third of its Afghan reconstruction funds to waste, fraud, and abuse, much of which involved contractors. The watchdog’s report closely examined one such contractor – a PMSC called TigerSwan – which appears to have significantly overcharged the US Department of State. There have also been serious concerns about a PMSC overcharging the United Arab Emirates (UAE) for the delivery of weaponized civilian helicopters.

It is less well known that PMSCs have played a role in fueling corruption and conflict in foreign countries. In 2020, the US Department of Justice ordered DynCorp to pay “[US]$1.5 million to settle fraud allegations that stemmed from a scheme in which DynCorp officials received kickbacks from subcontractors in return for Iraqi police training subcontracts.” In another case, US PMSCs reportedly hired local subcontractors with suspicious connections to armed groups, including adversaries of the United States. In 2010, an Afghan PMSC owned by a relative of the Afghan president reportedly engaged in fake firefights, and even paid local insurgents to attack a NATO supply convoy. These actions, along with the US Government’s support of political and military leaders who participated in or turned blind eye to corruption, led many local Afghans to assume the United States approved the corruption.

Spurred on by the US government’s normalization of PMSCs, US PMSCs are growing their services by working in many fragile countries around the world. US PMSCs account for a leading share of the estimated

9 Hartung 2021.
total annual sales of PMSCs globally, which was nearly US$224 billion in 2020, and is expected to grow to US$457 billion by 2030. An internal study by the US Department of Defense found that only 10-20 percent of US PMSC contracts are with the US Government or its North Atlantic Treaty Organization (NATO) allies. As they modernize their military, intelligence, and surveillance capabilities, countries in the Persian Gulf such as Saudi Arabia and the UAE have become major clients of US PMSC services. In one of the case studies in this report, a former US military officer employed by an UAE company, Knowledge Point, likely played a role in Emirati combat operations in Yemen. US PMSCs are also selling their services in Africa, Asia, and Central America. Some large US PMSCs have a relatively weak commitment to anti-corruption and transparency standards. Other countries, like China, India, Israel, Russia, and Turkey, are making increasing use of their own private military companies.

Despite the end of US involvement in Afghanistan, the US Government’s reliance on PMSCs will likely remain robust as PMSCs are now an integral part of US foreign military operations and foreign policy activities. The US Government is the largest client of US PMSC services, which include weapons maintenance, armed physical security, military and police training, intelligence collection, cybersecurity, and more. These services are delivered both domestically and abroad. The US Government regularly spends US$500 million a year simply on guard services overseas. In Fiscal Year (FY) 2022, the State Department proposed to spend over a billion dollars in foreign military and police training to more than 60 countries through funding accounts that often use PMSCs to deliver such aid. The Defense Department regularly signs multi-million-dollar contracts with PMSCs for military aircraft maintenance, military base security, and logistics. Some US defense analysts are also encouraging the use of US PMSCs in Ukraine to support the maintenance of US delivered weapons systems.

The growth and diversification of the US PMSC industry present profound corruption and conflict risks. Many US PMSCs now operate in countries with weak defense sector institutions and a culture of secrecy around national security issues, all of which provide a fertile environment for corruption to thrive. There are also serious regulatory and transparency gaps in US oversight of US companies and persons engaging in PMSC services for US or foreign governments. In particular, based on our research, US PMSCs run the risk of fueling corruption and/or conflict in the following ways (some of which are illegal in the United States):

- Serving as an advisor to a foreign military or police force unit that procures services for PMSC activities;
- Inflating threat perceptions or security needs in order to secure or prolong contracts, which can encourage authorities to take unnecessarily aggressive action;
- Improving the coercive capabilities of foreign military and security forces in highly corrupt governments, which can intensify repression and strengthen foreign military actions;
- Partnering with foreign government officials who also own private companies providing PMSC services;
- Capturing valuable natural resources, which can drive violent resource competition among local or foreign actors;
- Pushing foreign companies to pay kickbacks to a US PMSC to receive US Government-funded contracts;
- Paying bribes to government officials to influence government decisions or actions, which can inflame corruption dynamics that weaken and undermine state institutions;
- Brokering the sale of foreign PMSCs to fight on behalf of a foreign government in a conflict zone;
- Supporting or strengthening private, local organizations that feed into sectarian or criminal violence; and,
- Engaging in illicit economies such as arms trafficking.

There can also be substantial costs to US foreign policy interests and American lives when US PMSCs engage in corrupt or irresponsible actions, including when foreign citizens believe the US Government condones such actions. Former US intelligence officials working for an Emirati intelligence contractor, DarkMatter, helped spy on foreign and domestic critics of the UAE, including American citizens. The shooting of unarmed civilians by Blackwater employees in Nissour Square, Iraq,

complicated the US government’s efforts to establish an agreement with the Iraqi government on the stationing of US military forces in Iraq.19 The Venezuelan government reportedly accused the United States of supporting the US PMSC that allegedly led an effort to topple the current president.20 In Afghanistan, US PMSCs’ corrupt actions likely contributed to local Afghan resentment towards the US Government and to a weakened legitimacy of the Afghan police.21 PMSCs can also inflame conflict dynamics in countries key to US foreign policy by supporting conflict actors, strengthening corrupt officials, and capturing contested natural resources.22

The United States now has a new opportunity to improve key types of governance and oversight of US PMSCs activities abroad to reduce serious corruption risks. In June 2021, the US Government initiated a new combating corruption strategy, recognizing the role that corruption plays in degrading economic development, undermining citizens’ faith in government, and driving conflict.23 This strategy specifically calls on the US Government to start “reviewing and re-evaluating criteria for government-to-government assistance, including around transparency and accountability.”24 It also encourages efforts to work with “the private sector to improve the international business climate by encouraging the adoption and enforcement of anti-corruption compliance programs by U.S. and international companies.”25 This new initiative provides a critical moment to strengthen oversight of both US PMSC contracts with the US Government and with foreign governments.

The United States will need to address key gaps in regulation and transparency of US PMSC’s contracts with foreign governments. The State Departments’ Director of Defense Trade Controls (DDTC) requires US PMSCs to obtain their approval (via a license) to provide some types of PMSC-related services, such as military training for foreign governments or entities through its arms export regulations. These regulations, however, have wide gaps in oversight when US PMSCs or US persons working with foreign PMSCs seek to provide direct combat support to foreign entities abroad. The US Department of Commerce’s Bureau of Industry and Security (BIS) does not require US PMSCs to seek approval for armed, close personal protection of foreign officials, training of foreign law enforcement, and surveillance support to foreign governments or entities.26

PMSCs lack critical information on certain corruption dynamics in countries key to US foreign policy. However, the development of regulations and policies to oversee PMSCs over the past 15 years has largely been done in a staggered manner. Different US agencies maintain different controls and different degrees of oversight over PMSCs. The State Department’s guidance documents for contracting officers overseeing PMSCs lack critical information on certain corruption risks, ranging from conflicts of interest to kickbacks to help mitigate corruption. Chronic undertraining and understaffing also inhibit the ability of US agencies to assess corruption risks and hold contractors fully accountable when problems or violations exist.

Finally, the US Government’s efforts to address key challenges in regulating US PMSCs will not be fully effective unless it pushes foreign countries to adopt stronger national laws on their PMSCs. Many US PMSCs hire employees from all over the world, including from Africa, Asia, Europe, and Latin America. US individuals are also working for foreign PMSCs. However, many countries have not signed or implemented key non-binding international agreements, such as the Montreux Document and the International Code of Conduct (ICoC). This has created gaps in international and national regulatory efforts. It makes it more difficult and riskier for US PMSCs to vet foreign nationals working for them and for US persons to assess the risks of working for foreign PMSCs that have not implemented the Montreux Document standards. The United States can address these gaps by pushing more countries to agree to the ICoC and by working within the UN Intergovernmental Working Group on PMSCs efforts to establish a new international framework for PMSCs. The United States could also use UN discussions regarding Russia’s invasion of Ukraine to raise concerns about Russian PMSCs. Some of the key recommendations for improving US PMSC oversight are outlined below.

---

19 Erik Prince, Civilian Warriors: The Inside Story of Blackwater and the Unsung Heroes of the War on Terror, chapter 13, pages 207-231
21 Chayes 2021.
24 United States Office of the Press Secretary 2021a.
25 Ibid.
1.1 Selected Recommendations

1.1.1 Building a Stronger US Government Contracting Regime for PMSCs

- **Strengthen senior level US Government oversight of PMSCs.** The Defense Department should re-appoint a senior official to oversee policy guidance, coordination within it and other US Government agencies, and full implementation of legal and regulatory requirements regarding PMSC oversight. This official could also support efforts to strengthen international standards and foreign national laws on PMSCs. The State Department should also appoint or select a senior official within the Bureau of Management to help oversee State Department contracts with PMSCs. Senior level officials within State Department Bureaus designing foreign military and police training should also have responsibility to review the risks of hiring certain PMSCs.

- **Enhance training and guidance on corruption risks and counter measures.** The Defense and State Departments provide materials, guidance, and training that specifically identify and address the role of and opportunities for corruption in government contracting. However, the State Department policy guidance lacks sufficient information to identify and mitigate corruption. Guidance documents for contracting PMSCs to provide foreign military or police training or armed security should be updated to provide a wider typology of different forms of contractor corruption, as illustrated above as well as guidance on how to identify and address these practices. The State Department should also use this updated guidance in reviewing all types of government-to-government sales of PMSCs services.

- **Require contractors to report the beneficial ownership information for their subcontractors.** Prime contractors should be required to report on all subcontracting when submitting invoices. At the very least, this should include the names of all subcontractors (including those beyond the first and second tier), their business registration and beneficial ownership status, as well as the itemized value of subcontracted services. The definition of beneficial ownership as included in the Corporate Transparency Act should be used. The prime contractors should also submit all information on all potential subcontractors when contractors are submitting their bids for new US contracts. The US Government should make input of this subcontractor information into the publicly available USAspending.com database, which currently only includes information on prime contractors and excludes subcontractors.

- **Mandate agency reporting on PMSC use.** The US Government should provide annual reports to Congress on the value, scope, and composition of PMSCs contracted overseas. At least one DoD geographic combat command – CENTCOM – does so through quarterly reports on PMSC contractor levels in Iraq, Syria, Afghanistan, and throughout its area of operation. Such reporting can be expanded to include the firms hired – particularly those of US origin – as well as the values of their contracts. Other combatant commands should provide similar reports, as well as the various bureaus of the State Department that hire PMSC services. Equally, the State Department should provide annual reports to Congress on the PMSCs it has contracted for work overseas.

1.1.2 Bolstering US Oversight of PMSCs Sales to Foreign Governments

- **Expand oversight of US companies or persons engaged in combat activities abroad.** The State Department’s DDTC should urgently work to propose a rule change to the International Traffic in Arms Regulations (ITAR) requiring US companies or persons to apply for a license (US Government approval) if they wish to participate in combat operations abroad. This license requirement should include in the definition of combat activities US companies or persons services in support of strategic, tactical, and operational activities. The definition could also include intelligence gathering, logistics, and cyberwarfare activities in support of combat operations. DDTC should also add policy guidance to indicate that in most cases a license would be denied.

- **Strengthen scrutiny on subcontracting and beneficial ownership.** As part of DDTC’s requirements for US companies or persons seeking to export some types of PMSC services, US companies must submit foreign-owned signatories to disclose the nature of their ownership. The same should be required for US signatories. DDTC should also stipulate that license applications include information on all potential subcontractors, their business registrations, and beneficial ownership status, as well as the itemized value of subcontracted services. The definition of beneficial ownership as included in the Corporate Transparency Act should be used.

---


• Enhance reporting on exports of PMSC services. DDTC publishes annual reports to Congress on authorized exports of defense articles and services. These reports, often referred to as the 655 reports, provide critical insights into the scope and impact of the US arms trade. Yet, the information on defense services is severely limited by over-summarization by aggregating distinct categories together, such as combining data on sales of license manufacturing, offshore warehousing, and defense services into one amount for each country. This aggregation prevents Congress and the public from performing any type of oversight of PMSC services. Several years ago, DDTC provided more detailed reports on exports of defense services. DDTC should expand on these previous reports and list the specific types of defense services by country.

• Expand export license requirements for armed security and intelligence service exports (outside of direct support to combat operations). Given the risks to US national security from companies providing armed security and intelligence services abroad, Congress should explore ways in which the State and Commerce Departments could strengthen oversight of US PMSCs contracts with foreign governments and entities with weak anti-corruption standards and practices. Current Commerce Department regulations do not require US companies or individuals to apply for a license to actively engage in types of surveillance and countersurveillance for foreign intelligence agencies or companies in most countries. Congress should also consider expanding oversight of US companies that provide protective services to foreign politicians or elites accused of corruption, particularly in fragile or conflict-ridden countries.

• Push the US PMSC industry to adopt stronger anti-corruption and transparency measures. Some large US PMSCs score relatively low on supply chain transparency, conflicts of interest, and oversight of agents and joint ventures, according to Transparency International’s Defence Companies Index. These low scores mean higher risks of PMSCs unknowingly working with individuals or companies who have previously engaged in corrupt or illegal actions. These companies also run the risk of the US Government being misled or defrauded. The State and Defense Departments should work with the PMSC industry to strengthen company compliance systems and transparency in these areas and others to reduce corruption risks. The US Government should also press companies to adopt an explicit policy of non-retaliation against whistleblowers in all circumstances, as well as establish accessible whistleblowing channels and regularly monitor their use, at a minimum.25 The United States must also press defense companies to provide license-by-license reports to the US Government on political contributions, commissions, and lobbying of foreign clients.

1.1.3 Creating Stronger International Controls on PMSCs

• Encourage more countries to fully implement the International Code of Conduct for PMSCs. The International Code of Conduct (ICoC) offers strong standards for regulating PMSCs. As a strong early supporter of the ICoCA, the United States is in a good position to encourage other US security partner countries that are increasingly using PMSCs – such as the UAE, India, Egypt, and others – to agree to and adopt these standards as a means to expand controls over PMSCs in these countries and increase funding for ICoCA. At the same time, the United States should explore ways to encourage more US companies to join ICoCA by requiring US PMSCs seeking a contract with the Defense Department to be an ICoCA member. There is also a critical need to increase funding for ICoCA’s efforts to monitor potential problems with ICoCA membership companies and support strong company whistleblower protections.

• Rejoin the UN Intergovernmental Working Group on PMSCs discussion on establishing an international framework on PMSCs. The Working Groups’ renewed efforts to establish an international framework on PMSCs provides the United States another key opportunity to push foreign countries to establish stronger national controls on PMSCs. The United States can raise some of the concerns they have about the actions of foreign PMSCs by calling for clear restrictions on states hiring PMSCs with a record of engaging in corrupt activities or human rights abuses. Critically, the United States should encourage the Working Group to incorporate a broader definition of PMSCs to include intelligence and cybersecurity activities. The United States could also use this opportunity to talk about some of the ways the PMSC industry has grown and diversified as well as the challenges the US Government has faced in regulating US PMSCs.

What is a PMSC?

The private military security industry is a broad, nebulous sector lacking firm definition. Competing terms and definitions relating to PMSCs complicate efforts to effectively survey the industry. This report defines a PMSC as “private agents or business entities that are contracted to use, possess, direct, train, or enable lethal force or coercive cyber capabilities within or in relation to conflict, fragile, or otherwise unstable environments.” This definition is designed to capture the diversity of services within the sector, while also incorporating the relevance of cyberspace in defense and security domains. This report occasionally uses shorthand stand-ins like “contractor” or “security firm”.

According to the UN Working Group on Mercenaries, PMSCs are “private business [entities], irrespective of how they describe themselves” that deliver two distinct categories of services “on a compensatory basis.” One entails security services, which includes the provision of “armed guarding or protection of buildings, installations, property and people, any kind of knowledge transfer with security and policing applications, development and implementation of informational security measures and other related activities.” The other set entails uniquely military services, which can include the provision of “specialized services related to military actions including strategic planning, intelligence, investigation, reconnaissance, flight operations, manned or unmanned, satellite surveillance, any kind of knowledge transfer with military applications, material and technical support to armed forces and other related activities, whether on land, in the air or at sea, or whether in cyberspace or space.”

While there are several clearly identifiable PMSCs with an explicitly military/security orientation, many companies also straddle the boundaries of PMSC definitions. Many firms that deliver PMSC services present themselves as general government contractors, and they are often hired to provide adjacent services in stabilization missions, such as infrastructure engineering and construction, project monitoring, and facilities support. This report identifies a company as a PMSC when its sales include a significant amount of PMSC services. It generally tries to exclude companies that focus on manufacturing weapons systems; although, some of them have acquired PMSCs over the last 20 years.

31 Ibid.
32 Ibid.
2.0 PRIVATE MILITARY AND SECURITY MARKET AND CORRUPTION RISKS

The global PMSC industry has grown and diversified extensively since the US-led wars in Afghanistan and Iraq. It has grown from an estimated value of US$100 billion in 2003 to US$224 billion in 2020.33 Many US PMSCs now operate all over the globe and are increasingly selling their services to governments in the Persian Gulf and Africa. Some major US companies that offer PMSC services have subsidiaries in countries such as Egypt, Lebanon, Singapore, and Saudi Arabia. However, many of these companies have relatively weak anti-corruption and transparency standards. Many PMSCs provide services traditionally carried out by state military and intelligence agencies. At the same time, foreign PMSCs in Europe, Asia, and the Middle East are significantly expanding their operations domestically and internationally. The industry’s explosive growth and normalization over the past 20 years reveals numerous corruption risks, which can inflame conflict, undermine the rule of law, and put US citizens in danger.

2.1 Birth of the Modern PMSC

In the late 1990s, some US defense analysts began to raise concerns about US companies staffed by former defense, military, intelligence, or law enforcement officials selling their skills in fragile countries and conflict zones.34 One such company, MPRI, reportedly provided combat training to local Croatian forces that went on to indiscriminately attack Serbian communities.35 In 2002, another company, DynCorp, settled charges brought by a whistleblower concerning a “sex [trafficking] ring” in Bosnia.36 The US-led wars in Afghanistan and Iraq greatly expanded the national debate on US PMSCs. The US Government used PMSCs extensively in military operations for operational support, intelligence analysis, threat assessments, and personal and physical security.37 The United States also relied heavily on PMSCs to train military and police forces in Afghanistan and Iraq. However, US officials did not appear to be prepared for some of the ways PMSCs contributed to corruption.

The US Government channeled billions of dollars into the PMSC industry, leading to a massive expansion in both the size and quantity of such companies. According to the US Congressional Budget Office (CBO), the United States “obligated between [US]$3 billion and [US]$4 billion to PSCs [Private Security Contractors] to acquire security services” in Iraq between 2003 and 2007.38 Blackwater, which was founded by former US Navy Seal, Erik Prince, grew from providing firearms training to US law enforcement solely in the United States, to playing a key role in guarding CIA officials in Afghanistan and US Department of State personnel in Iraq.39 From 2003-2004, the company’s profits rose by 600 percent. Triple Canopy, another US PMSC providing armed security in Iraq, was founded soon after the Iraq war began.40 The US Department of Defense also hired foreign PMSCs such as Aegis Defence Services Limited, Erinys International, and ArmorGroup Services Ltd.41 NATO allies such as Germany and the UK also expanded their use of PMSCs in overseas military operations.42

“One of the most significant developments is the emergence of PMSCs in commercial markets,” said Erik Prince43

Although the US Government does not know exactly how many PMSCs supported US operations in Afghanistan and Iraq, the information we do know is staggering. In 2008, the Congressional Research Service stated that the US Government contracted 20 different PMSC firms with around 30,000 employees in Iraq.44 Most of the employees were from “western countries—such as the United States or British Commonwealth countries—with experience in the military or law enforcement.”45 The PMSC firms also hired third-country nationals (TCNs) from countries such as Chile, Fiji, Nepal, and Nigeria as well as in-country nationals.
from Iraq. In 2011, the Defense Department employed an estimated 90,000 contractors in Afghanistan. This includes PMSC contractors and other types of private support to the US Government in Afghanistan.

The US Government accounts for its extensive use of PMSCs with the belief that market competition could provide essential services at reduced cost and increased speed, though many analysts raised serious concerns. Some members of Congress and US military officials said that the extensive use of PMSCs concealed the political costs of engaging in foreign military actions. In 2002, US Representative Jan Schakowsky asked: “Are we outsourcing in order to avoid public scrutiny, controversy, or embarrassment?” Some US military officials were concerned that US PMSCs were contributing to Iraqi resentment against United States after reports of attacks on unarmed civilians and torture by US PMSCs. The shooting of many unarmed civilians in Nissour Square, Baghdad by Blackwater contractors significantly escalated this resentment and contributed to souring relations between the United States and the Iraqi Government.

There were also concerns that “the lack of public information on the terms of the contracts, including their costs and the standards governing hiring and performance,” obscured inefficiencies and led to cost overruns. After 20 years of US operations in Afghanistan and Iraq, many of these early concerns were well justified. Some US PMSCs contributed to serious waste, fraud, and abuse of US Government funding. The US Government, for example, awarded million-dollar contracts to DynCorp to train local police in Afghanistan and Iraq. However, in 2016, the US Department of Justice alleged that DynCorp “knowingly submitted inflated claims” on such contracts. There were also serious concerns about the effectiveness of DynCorp’s Afghan police training; tens of thousands of participating Afghans deserted the police force by 2010. According to US Ambassador Richard Holbrooke, the Afghan National Police was “an inadequate organization, riddled with corruption.”

US officials did not fully grasp how PMSCs fueled corruption and conflict in Afghanistan and Iraq. In some cases, US PMSCs encouraged local companies to engage in corrupt activities to receive US Government contracts. According to the Justice Department, DynCorp employees reportedly received kickbacks from subcontractors in return for Iraqi police training subcontracts. One US PMSC operating a major Iraqi airbase reportedly hired security guards affiliated with an Iran-backed militia, and it used subcontractors controlled by an Iraqi general with suspected links to sectarian armed groups. In 2010, an Afghan PMSC owned by a relative of the president reportedly engaged in fake firefight, and even paid local insurgents to attack a NATO supply convoy as a means of inflating threat perceptions and securing new contracts. These actions, along with US support for corrupt political leaders, led many locals to assume the US Government approved the corruption.
2.2 US PMSC Global Market

The US PMSC industry is a multibillion-dollar industry with an extensive presence throughout the world. US companies account for a leading share of the estimated total annual sales of PMSCs globally and are projected to reach more than US$80 billion in annual sales in the near future. According to Aerospace and Defense News, the global PMSC industry grossed nearly US$224 billion in 2020 and is expected to make US$457 billion by 2030. This includes PMSC services ranging from “the provision of armed guards, to the maintenance of weapons systems to the training of local forces and security personnel,” but it does not fully include cybersecurity sales. Some analysts estimate global cybersecurity services to be worth US$218 billion in 2020.

The US Government dominates the US market, utilizing PMSC services domestically and abroad. US companies are also increasingly pursuing direct commercial sales with foreign governments and entities. This presents clear risks when the recipient country is highly vulnerable to corruption or when the PMSC lacks serious anti-corruption safeguards.

2.2.1 US and Foreign Government Demand

The US Government continues to be a large consumer of US PMSC services abroad. The US Government mainly employs such companies for armed security, weapons maintenance, logistics support, and intelligence. In FY2020, more than 20 US Government agencies obligated US$500 million for private “security guards and patrolling services” abroad. In March 2022, Triple Canopy was awarded a US$1.3 billion contract to provide protective services for the State Department in Iraq over a 10-year period. In FY2022, the State Department authorized US$1.6 billion through just three funding accounts for foreign military and police training to more than 60 countries. Many of these countries have defense and security sectors that are highly or critically at risk of corruption, according to Transparency International - Defence and Security’s Government Defence Integrity Index (GDI) (see Figure 1). Some of this training is provided by US PMSCs. For example, in 2020, the US PMSC Bancroft Global Development provided reconnaissance training to the Ugandan People’s Defense Force (UPDF) in Somalia. The US company Bellator Group Inc. was awarded a contract by the State Department in FY 2020 to deliver anti-terrorism training or equipment to Tunisian security forces.

Figure 1: US Recipients of Military and Police Training and Related Corruption Risk Level

Legend

Defense Sector Corruption Risks:

- F: Critical
- E: Very High
- D: Moderate
- C: Moderate
- Not Rated

60 Ibid.
61 Stockbruegger 2021.
62 Search for security guards and patrolling services awards in countries other than the United States at the website https://www.usaspending.gov/
67 USAspending.gov, advanced search for state department funded contracts in Tunisia.
The Defense Department is also a major client of US PMSCs. Some of the highest dollar-value contracts are to repair and maintain weapons systems both domestically and internationally. In 2019, KBR was awarded a US$530 million contract to provide maintenance and supply chain services for the US Marine Corps in Kuwait and on ships in the Asian Pacific.68 Triple Canopy received a US$198 million contract from the Defense Department in 2020 to provide security support to US military bases in Kuwait.69 The US military also hires PMSCs to provide intelligence analysis for military operations and to enhance electronic warfare skills and capabilities.70 In 2021, CACI International Inc. received a task order worth up to US$785 million from the US Army Special Operations Command to support “integrated information warfare (IW) and electronic warfare (EW) solutions, training, readiness, and modernization.”71 Some US defense analysts are also encouraging the use the US Government to send PMSCs to Ukraine to support the maintenance of US delivered weapons systems and the logistics of getting weapons to the frontline.72

However, the US Government’s influence over the US PMSC market has declined since the mid 2010s. An internal study by the Defense Department found that only 10-20 percent of PMSC contracts are with the US Government or its NATO allies.73 The State Department requires US companies to seek approval before selling defense services abroad, which can include weapons maintenance and various types of direct training to foreign militaries. The State Department is not required to approve sales for armed security and for training of law enforcement and intelligence agencies unless PMSCs also sell controlled technology. In FY2011, the State Department authorized roughly US$7 billion worth of defense service sales.74 This value has likely increased in recent years because of the growth of private PMSC sales to foreign clients. Some of these sales are to countries with weak institutional structures for combating corruption.

Several countries in the Persian Gulf appear to be key clients of US PMSCs. In 2019, the State Department authorized US companies to provide US$1.7 billion in defense services, licensed manufacturing, and offshore warehousing (collectively known as technical assistance agreements, or TAAs) in Saudi Arabia and the UAE.75 Over the past few years, the UAE has hired US companies and US citizens to strengthen their offensive military, intelligence, and cyber capabilities. In 2017, a US PMSC provided military training to the Saudi operatives who would go on to murder Jamal Khashoggi, a dissident journalist.76 In another case, former US intelligence officials working for an Emirati intelligence contractor, DarkMatter, supported a program that actively spied on foreign and domestic critics of the UAE.77 This included foreign journalists, US citizens, and local dissidents, including a prominent human rights activist who was subsequently sentenced to 10 years of solitary confinement for “speech” crimes.78

Some US PMSCs have also found opportunities within African countries. Erik Prince reportedly played a role in helping the UAE send PMSCs to Libya and Somaliland (see Knowledge Point case study). The US company, Global Guardian, provides emergency security for private companies and individuals operating throughout Africa.79 Another US company, AdvanFort Co., appears to provide anti-piracy maritime protection for clients in east and west Africa.80 An Israeli subsidiary of the US company, Verint Systems Inc., reportedly provided surveillance equipment and services from 2015 to 2017 to the South Sudanese government, which has allegedly illegally detained individuals and infringed on press freedoms.81 Academi (formerly Blackwater) reportedly provided security services in Sudan without the required State Department approval.82 In 2012, a former CEO of KBR Inc. pled guilty to bribing Nigerian officials for a US$6 billion contract to develop hydrocarbon infrastructure in the conflict-affected Niger Delta.83

US PMSCs are also active in Latin America, including Honduras, Mexico, Nicaragua, Venezuela, and Ukraine.84 In 2020, a US PMSC launched a botched incursion into Venezuela, reportedly seeking to topple the regime of Nicolas Maduro on behalf of local dissidents.85

70 DW. “Africa Why private security companies are booming in Africa.” March 2020.
72 Cancian 2022.
73 Author interview with former senior DoD contracting official. 22 January 2021.
74 Author interview with former State Department official in 2014. This official said that about 5% of defense services authorizations in the past few years were associated with PMSC services. Here is one of the annual State Department reports on export defense articles and services during this timeframe. https://www.pmloptd.state.gov/ddtc_public/?id=ddtc_public_portal_news_and_events&cat=Report&dp=2
82 Ingram, David. 2012. “Company formerly called Blackwater to pay sanctions fine.” Reuters. 9 August.
Global Guardian has helped protect Americans from extortion attempts in a South American country. The Mozart Group, which was founded by a retired colonel in the US Marine Corps, is training Ukrainian Special Forces in skills such as sniper training, spotting improvised explosive devices (IEDs), and other tactical capabilities in response to the Russian invasion of Ukraine. The US Government, however, has been imploring Americans supporting combat operations in Ukraine to leave the country immediately out of concern that Americans could be targeted or mistreated by Russian forces.

2.1.2 US PMSC Structure and Market

The US PMSC industry includes large corporations making over US$4 billion in annual sales. Several US companies that provide PMSC services are now included in the Stockholm International Peace Research Institute's (SIPRI) top 100 arms-producing and military services companies list. Some of these include Amentum (incl. DynCorp), Booz Allen Hamilton, CACI International, KBR Inc., ManTech International, SAIC, and Vectrus. Booz Allen Hamilton, a management consulting firm specializing in intelligence, defense, and cybersecurity, reportedly played a key role in helping the UAE “build its own high-tech spy agency.” Booz Allen Hamilton has subsidiaries all around the world, including in Singapore, UAE, Egypt, Lebanon, Saudi Arabia, Tanzania, and Indonesia. According to a US federal court, ManTech International, which provides support services to the defense and intelligence communities, was accused by a whistleblower of “improperly billing the US Army under a [US]$3 billion contract for mine resistant vehicles.”

Most of these large firms appear to have a limited or low commitment to corporate transparency and anti-corruption standards, according to Transparency's International Defense Company Index (see Figure 2). DynCorp, ManTech, CACI, and SAIC all scored low on their overall commitment while KBR and Vectrus scored a moderate commitment based on publicly available information. The low scores on supply chain transparency, conflicts of interest, and agents are the most concerning given the context in which US PMSCs operate around the world. Conflicts of interest may arise when former government employees use their contacts to unduly influence government decisions. Companies with poor conflict of interest controls run greater risks of misleading or defrauding clients, including the US Government. Weaknesses in the supply chain could result in US PMSCs unknowingly working with individuals or companies who have previously engaged in corrupt or illegal actions. A lack of reporting to the Executive Branch, Congress, and the public about defense company

Figure 2: Top US PMSCs Commitment to Transparency and Anti-Corruption Standards

---

91 Booz Allen Hamilton, Inc. N.d. International McLean: Booz Allen Hamilton, Inc.
94 Ibid.
political contributions, commissions, and lobbying to foreign customers may also hide bribes and conflicts of interest.

PMSCs frequently merge, rebrand, and rename themselves. These practices can obscure who leads or benefits from the company as well as past associations with controversial actors. Importantly, it can contribute to impunity for companies and those who lead them. When there is significant consolidation of companies, it can result in monopolies that “place individual governments in a weakened negotiating position over costs and timelines.”

Several US companies that provide armed physical security and close protection merged into a large corporation called Constellis. Some of the companies under this umbrella include Academi, AMK9, Centerra, Edinburgh International, Olive Group, and Triple Canopy. In the past few years, CACI International acquired companies in the United States and the United Kingdom (UK) with expertise in cyber solutions, data mapping, and other information technology services. Blackwater changed its name to Xe and then Academi before merging into Constellis. The now shuttered company Total Intelligence Solutions, which reportedly ran spy rings for the US Government overseas, appears to be connected to OODA through an organizational webpage.

The workforce of the US PMSC industry is typically ex-military and heavily internationalized. Most PMSCs are owned and operated by military veterans. However, for contracts delivered abroad, such companies will typically assign Western managers to oversee TCNs or local nationals, who are cheaper to staff the contract. For example, former employees of US PMSCs describe working with nationals from Latin America and Africa. Bancroft Global Development reportedly hired British, European, and South African staff to work with Americans in training the Somali military. A former US defense official has raised concerns about Bancroft’s other commercial activities in Somalia creating potential conflicts of interest with US foreign policy. Many Americans are also working for foreign PMSCs in countries such as the UAE.

### 2.3 Foreign PMSCs and their Activities

Spurred on by the US-led wars in Afghanistan and Iraq, foreign PMSCs are expanding their sales and activities around the world. Some of the PMSCs with the highest annual sales are based in the United Kingdom and other European countries. While it is unclear whether the Wagner Group is a private entity or a clandestine front for the Russian government, they are now operating in more than 18 countries in Africa alone. Chinese PMSC sales are expected to triple by 2030. Chinese PMSCs also operate throughout Africa. Several countries in the Middle East are expanding their use of PMSCs to quell political opposition and pursue foreign interests. There continues to be demand for PMSCs in parts of Latin America. The expanded use of foreign PMSCs has also reportedly led to controversial, corrupt, or illegal activities, such as attacks on civilians, illegally training militias, trafficking in firearms, and spying on political dissidents.

There are several prominent PMSC companies in the United Kingdom and other European countries. The largest PMSC in the world in terms of annual revenue is G4S, making an estimated US$9.7 billion in 2019. G4S “offers a range of services, including the supply of security personnel, monitoring equipment, response units, and secure prisoner transportation” and is based in the United Kingdom with subsidiaries all over the world. G4S has repeatedly been accused of charging migrant workers exorbitant recruitment fees, a practice that often results in debt bondage. The British company, International Intelligence Limited, provides command, control, and intelligence services for militaries and competitive intelligence and counter espionage services for corporate clients. Prosegur is Spain’s largest private security company with over US$3.7 billion in annual sales in 2020 and is operating in over 26 countries. The German company Xeless Group provides military camp support for NATO countries.
Ostensibly private Russian entities like the Wagner Group support the Kremlin’s proxies and clients all over the world, even directly engaging in combat against US troops in Syria.\textsuperscript{111} Wagner-affiliated contractors are engaged in Russia’s violent invasion of Ukraine.\textsuperscript{112} They also operated or are currently operating in at least 18 countries in Africa, including Mali, Central Africa Republic, Libya, and Sudan.\textsuperscript{113} Many of these operations appear to be motivated by mineral wealth and have generated reports of egregious human rights violations. In Libya, Wagner operatives reportedly “plant[ed] explosive booby traps in residential areas and comit[ted] summary executions in support of a warlord vying for control of the country.”\textsuperscript{114} Wagner operatives apparently teamed up with Sudanese soldiers to violently suppress anti-regime protests in exchange for gold mining rights.\textsuperscript{115}

The PMSC industries in Australia, China, and India appear robust. Chinese PMSC sales are projected to grow from US$13 billion in 2020 to nearly US$39 billion in 2030.\textsuperscript{116} Since 2010, Chinese PMSCs have operated in Africa, first to protect its maritime vessels from pirates and now to support its Belt and Road Initiative (BRI).\textsuperscript{117} Chinese PMSCs such as Beijing DeWe Security Service protect railways in Kenya and natural gas projects in Ethiopia and Djibouti.\textsuperscript{118} Some of these PMSCs worked directly with the Sudanese military to rescue kidnapped Chinese workers.\textsuperscript{119} Chinese citizens have also reportedly been arrested in Zambia for “illegally training local military forces in military tactics.”\textsuperscript{120} In India, local private security companies are some of the largest employers in the country. Bombay Intelligence Security Ltd., which provides armed guarding, surveillance services, and electronic security for companies, has some 45,000 employees.\textsuperscript{121} Australian PMSCs such as Unity Resources Group have provided security for the Australian embassy in Iraq.\textsuperscript{122} Some Australian citizens are supporting the UAE’s armed forces.\textsuperscript{123}

PMSCs often operate in developing countries and regions. South African PMSCs provide services throughout the African continent, including in Libya and Nigeria. In 2016, South African PMSCs reportedly played a direct role in Nigerian combat operations against Boko Haram.\textsuperscript{124} The Turkish PMSC SADAT International Defence Consultancy said it aims to “establish a Defense Collaboration and Defense Industry Cooperation among Islamic Countries to help Islamic World take the place where it merits among Superpowers by providing Strategic Consultancy, Defense and Security Training and Supply Services to Armed Forces and Internal Security Forces of Islamic Countries.”\textsuperscript{125} There are reports of PMSCs in Latin America engaging in trafficking and extortion. For example, Brazil’s Federal Police found that almost a third of all firearms held by local security firms in Rio de Janeiro were trafficked to criminals.\textsuperscript{126} In El Salvador, a police investigation found that the MS-13 gang used private security guards to collect extortion rents.\textsuperscript{127} Several of the Colombian contractors allegedly involved in the assassination of Haitian president Jovenel Moise claimed they were deceived about the true purpose of their employment.\textsuperscript{128}

Several countries in the Middle East are also increasingly turning towards new technology, including surveillance software and spyware, to suppress legitimate political dissent. In some cases, these countries have turned to companies that provide powerful cyber intrusion software. Israeli intelligence firms such as the NSO Group have been embroiled in international scandals, from proliferating powerful cyberweapons to spying on and harassing foreign anti-corruption officials.\textsuperscript{129} The countries of Saudi Arabia and the UAE have reportedly used this software to target political dissent domestically and internationally.\textsuperscript{130}
3.0 CASE STUDY: KNOWLEDGE POINT

Knowledge Point is an Emirati company that contracts out former US military personnel to the UAE’s armed forces. PMSCs like Knowledge Point play a critical enabling role in the UAE’s defense sector as brokers and suppliers of US military services. Many US and Western veterans have embedded within the UAE’s armed forces are trainers, advisors, technicians, operators, commanders, and even combatants through PMSCs like Knowledge Point. Yet, these contractors operate in an opaque defense sector, tightly controlled by the UAE’s supreme leader, that poses serious risk of fueling corruption and regional conflict. This defense sector puts PMSCs – whether as contracted firms or hired individuals – in clear conflict of interest situations. Furthermore, US citizens working for Emirati PMSCs (as well as US PMSCs) may support controversial UAE foreign interventions in places such as Yemen, Libya, and eastern Africa. US citizens are required to receive US government authorization for some types of military services to the UAE, but it appears some Americans are going beyond their authorization or not seeking authorization at all.

3.1 An EDGE Company

At the center of the UAE’s defense industry is EDGE, a state-owned defense conglomerate. The UAE's supreme leader and commander of the armed forces, Sheikh Mohammed bin Zayed al-Nahyan (or MbZ) founded EDGE in 2019. The creation of EDGE is part of a broader Emirati effort to develop a semi-indigenous defense industry with three strategic objectives: to diversify its economy away from oil production; to achieve greater autonomy in arms procurement; and to support its regional political and military ambitions. State-owned investment funds, such as Tawazun Economic Council and Mubadala Investment Company, collectively hold owning stakes in most of the industry’s companies, though nominally private funds like YAS Holding also have a stake in the industry. MbZ established EDGE to consolidate 25 national defense companies into five mission “clusters” – platforms and systems, missiles and weapons, cyber defense, electronic warfare and intelligence, and mission support. He awards the leadership of Emirati defense companies to loyal confidantes, who also hold positions within state councils and government bodies. There are apparently few limits within the Emirati defense sector to prevent such conflicts of interest as well as no external oversight of government defense spending. EDGE ostensibly generates US$5 billion in revenue annually and employs 12,000 people. EDGE’s employees are overwhelmingly foreign in order to fill gaps in Emirati human capital, military expertise, and military capability. Even in EDGE’s most Emiratized subsidiary, only 27 percent of the workforce are UAE citizens.

Knowledge Point is part of the mission support cluster. The company was originally funded by Emirates Advanced Investments Group (EAIG – now YAS Holding) in 2009. According to its website, Knowledge Point provides training, consulting, and education services for military, intelligence, and law enforcement agencies throughout the Gulf, but mostly in the UAE. Its consulting expertise ranges from the development of military doctrine to cybersecurity. Knowledge International is the US-based sister company of Knowledge Point, which helps the company comply with US arms export controls. A survey of online profiles of Knowledge Point employees revealed more than 40 former US military personnel, ranging from senior sergeant majors to colonels and generals, embedded with the UAE military. Knowledge Point has also employed Americans who previously worked with the Federal Bureau of Investigations (FBI) and US defense contractors.

The Americans working for Knowledge Point support the UAE armed forces at the highest level, ranging from advising senior Emirati commanders to training combat...
units. A former two-star general helped develop the UAE armed forces’ logistics capability. A former lieutenant colonel mentored the Land Forces’ senior-most military intelligence officer and served as counsel to one of MbZ’s advisors. Another former colonel developed doctrine and training guidelines for senior Emirati military staff, while another is responsible for training artillery units at the brigade level. Knowledge Point’s Chief Operating Officer is a retired US Navy rear admiral, a former director of Lockheed Martin, and directly advised the UAE armed forces’ command staff. A former colonel currently serves as the direct advisor to the commander of the UAE’s Land Forces (analogous to the US Army).

US military veterans provide high-level support to the Emirati defense sector through other EDGE companies as well. A former US Air Force commander is a director at EDGE’s cyber defense and intelligence subsidiary, Beacon Red.144 He was previously a vice president of ManTech, and he operated Beacon Red’s predecessor firm, DarkMatter, which infamously recruited former US intelligence officials to spy on Emirati regime critics.145 Many of Beacon Red’s employees formerly worked for DarkMatter, which targeted foreign journalists, US citizens, and local dissidents, including a prominent human rights activist who was subsequently sentenced to 10 years of solitary confinement.146 Beacon Red also appears to employ former US special forces personnel, FBI agents, as well as various other US veterans who worked for various US, Saudi, and Emirati PMSCs.147

Despite EDGE’s centrality, it closely coexists with a network of ostensibly privately-owned Emirati defense companies and PMSCs. Such companies are often owned by elite families with close ties to the monarchy and positions in government bodies.148 They are nevertheless managed and run by Western military and security professionals.149 These PMSCs appear to play diverse roles for the Emirati government: they act as state-appointed brokers for major defense procurements; they supply embedded contractors to the armed forces; they act as offset partners for foreign defense suppliers; and they operationalize covert aspects of the UAE’s militarized foreign policy.150 For example, Erik Prince reportedly brokered agreements between PMSCs and the UAE government for foreign military activities in Libya and Somalia.151

Knowledge Point is connected with some of these privately-owned UAE defense companies such as International Golden Group (IGG) and Maximus Air Cargo. IGG is reportedly the largest supplier of the UAE armed forces and was initially run by the military’s deputy chief of staff.152 IGG, like Knowledge Point, also embeds Western military contractors in the UAE armed forces, and it employs Australian, British, French, Spanish, Italian, and US citizens.153 Maximus Air Cargo

A survey of online profiles of Knowledge Point employees revealed

> 40 FORMER US MILITARY PERSONNEL

ranging from senior sergeant majors to colonels and generals, embedded with the UAE military

---

144 Additional information gathered from LinkedIn. Intelligence Online. 2021. ‘Successor to Mohamed bin Zayed’s cyberattack outfit DarkMatter teams with ex-Mossad chief’s startup.’


147 Survey of publicly accessible professional profiles conducted online by Transparency International Defence and Security in October 2021.

148 Intelligence Online 2014.

149 For example, see Trust International Group, which is owned by Tahnoon bin Zayed al-Nahyan (brother of the UAE’s supreme leader) and run by a former US Army officer. Intelligence Online. 2011. ‘Tahnoon bin Zayed, Abu Dhabi saymaster, fashion’s security and investment empire.’ Intelligence Online. 2 May.

150 For example, see International Golden Group, discussed below.


153 Survey of publicly accessible professional profiles conducted online by Transparency International Defence and Security in October 2021.
is a contractor of IGG and is run by close associates of MbZ.\textsuperscript{154} The president of Knowledge Point’s mission cluster is a board member of Maximus Air Cargo.\textsuperscript{155} Knowledge Point’s current CEO was formerly a director at IGG. Furthermore, both Knowledge Point and IGG were founded through the same elite fund (EAIG/YAS Holding).\textsuperscript{156} IGG is also part owned by Tawazun, which owns/controls EDGE; the CEO of Tawazun sits on the board of IGG.\textsuperscript{157} These connections demonstrate that much of the Emirati defense industry is interconnected and punctuated by overlapping leadership roles that generate conflicts of interest.

3.2 Conflicts of Interests

These questionable interconnections within the UAE defense sector appear to extend to some of the US contractors working in the Emirates defense sector. Some of the Americans working for Knowledge Point seem to act as buyer and seller of military services as well as advisor and commander within the Emirates military. This blurring of the lines between usually separated roles poses significant risks of procurement abuse and illicit enrichment. It could also implicate Americans in irresponsible or illegal foreign military actions. One such example is Stephen Toumajan, a former US Army aviator and lieutenant colonel. Toumajan reportedly commanded both the UAE’s combat helicopter wing (the Joint Aviation Command, or JAC) and its search and rescue service.\textsuperscript{158} Toumajan appears to have had command influence over the JAC, which extends to procurement programs.\textsuperscript{159} Yet Toumajan is reportedly an employee of Knowledge International (Knowledge Point’s US sister company) and seconded to the UAE armed forces.\textsuperscript{160}

According to official documents acquired by BuzzFeed News, the US Department of State authorized Toumajan as a “Chief Aviation Adviser” to “directly support the UAE [then-]Deputy Supreme Commander,” or MbZ.\textsuperscript{161} However, it appears that Toumajan plays more than an advisory role. While Toumajan insisted to the press that he is a civilian contractor without rank or command in the Emirati military, he identified himself as the “commanding general of the Joint Aviation Command in the UAE” in a video produced and posted by the US Department of Defense.\textsuperscript{162} He holds the title of “Major General” within the UAE armed forces and wears its uniform.\textsuperscript{163} Toumajan reportedly said he ‘does not wear a UAE military uniform’ but ‘does wear the rank insignia for good order and discipline for the unit.” US court documents as well as colleagues interviewed by the press seem to corroborate that he held command influence in the JAC.\textsuperscript{164}

Regardless of how he characterizes himself, Toumajan is involved in JAC procurement decisions while also serving as a board member for several of the companies that JAC contracts. Toumajan’s official online biography states that he sits on the board of directors for several EDGE companies, including Knowledge Point, Horizon Flight Academy, and AMMROC.\textsuperscript{165} Civil complaint documents in a US court case relating to an internal dispute of an Emirati defense supplier, NorthStar Aviation, suggests that Toumajan oversaw contracts on behalf of JAC (Toumajan is not a party in the court case).\textsuperscript{166} JAC contracted NorthStar to supply weaponized civilian helicopters while Horizon Flight Academy ordered a training variant of the same system.\textsuperscript{167} JAC is also a buyer of Knowledge Point and AMMROC services.\textsuperscript{168}

Toumajan’s apparent influence in procurement decisions could present a clear conflict of interest. In the US defense sector, such relationships are strictly prohibited on the basis that Toumajan’s command influence could provide these contractors with proprietary knowledge and an unfair advantage when competing for contracts.\textsuperscript{169}

\textsuperscript{155} Additional information gathered from LinkedIn. EDGE. N.d. Khalid Al Breiki: President – Mission Support, EDGE & Chairman of the Board at AMMROC Abu Dhabi: EDGE.
\textsuperscript{158} National Search & Rescue Center (NSRC). N.d. Director Genera’s Message: Abu Dhabi: National Search & Rescue Center.
\textsuperscript{159} NSRC, n.d.
\textsuperscript{160} Roston, Aram. 2018a. “This American Is A General For A Foreign Army Accused Of War Crimes In Yemen.” BuzzFeed News. 7 May.
\textsuperscript{161} Ibid.
\textsuperscript{162} While Toumajan insisted to the press that he is a civilian contractor without rank or command in the Emirati military, he identified himself as the “commanding general of the Joint Aviation Command in the UAE” in a video produced and posted by the US Department of Defense. Defense Visual Information Distribution Service. 2017. UAE at NTC: Arlington: US Department of Defense. 17 October.
\textsuperscript{163} NSRC, n.d.
\textsuperscript{164} Roston 2018a.
\textsuperscript{165} Horizon is a flight school for helicopter pilots that also provides training to military helicopter aviators. AMMROC is the UAE’s military aviation maintenance, repair, and overhaul (MRO) provider and originated as a joint venture between Sikorsky, Lockheed Martin, and Mubadala. NSRC, n.d.
\textsuperscript{168} Sophia, Mary. 2015. AMMROC secures Dh2.3bn contract with UAE JAC.” Gulf Business. 28 February.
Such conflicts of interest can lead to a variety of corrupt acts. Contractors may use their insider knowledge to unfairly win procurement requests. They can also result in price gouging and unnecessary defense purchases as the procurement officer stands to gain from such transactions. The NorthStar court case is centered on mutual accusations by its two co-directors – one a former US Navy SEAL with ostensible links to Erik Prince, and the other a member of the al-Nahyan royal family – that the other mismanaged the company and received excessive compensation.71 NorthStar’s militarized helicopters are reportedly believed to have been sold to the UAE at more than three times the price of the basic system – far more expensive than comparable purpose-built military helicopters.71

Toumajan’s position within the JAC also embeds him within a defense procurement process with no external oversight that is vulnerable to exploitation by government officials with stakes in defense companies.72 For example, JAC signed a contract in 2021 worth over US$47 million with a local aviation conglomerate, Abu Dhabi Aviation Company (ADAC), for support services.73 ADAC is comprised of several individual aviation companies that contract prominently with the Emirati Government, and it is 70 percent owned by private individuals based in Abu Dhabi (the Abu Dhabi Government owns the remaining stake).74 Knowledge Point’s cluster president is a board member of an ADAC subsidiary, while a close advisor to MbZ sits on the board of ADAC itself.75 This raises the possibility that contractors like Toumajan (and the JAC) are vulnerable to influence and can direct state procurement contracts toward connected elites.

Toumajan’s role as commander of the JAC also puts him at risk of supporting irresponsible or illegal UAE military actions abroad.76 The State Department generally prohibits US citizens from providing “direct command functions, combat troops, combatants, or mercenaries,” as a matter of unofficial policy.77 Yet Toumajan’s official bio says he is “specifically responsible for the combat readiness and execution of all aviation missions and training for UAE forces.”78 Although Toumajan denies he had any involvement in Yemen, his role likely engaged him in JAC actions in the country, where its helicopters were deployed.79 Toumajan reportedly said the UAE’s forces ‘are under a completely separate and distinct commands structure not under the Joint Aviation Command,’ for operations in Yemen. However, Buzzfeed News quoted a former CIA official as saying Toumajan was key to Emirati operations in Yemen.80 The UN documented a 2017 incident where a combat helicopter – likely Emirati – indiscriminately targeted and killed dozens of civilians in the Gulf of Aden.81 Despite Toumajan’s denial of any involvement in this incident, investigators noted the munitions used match those of the UAE, while the UAE admitted it had forces in the area at the time of the attack.82

3.3 Regional Conflicts

The UAE regularly uses foreigners, including Americans, to support foreign military interventions and foreign forces in Yemen, Libya, and throughout East Africa, (see Figure 3). PMSC services provided by US citizens are at risk of enabling these often controversial (even illegal) UAE interventions.83 Erik Prince reportedly brokered deals for the UAE to hire private military contractors from all over the world for several of these interventions, one of which is likely a violation of US arms export control laws.84 US personnel even participated in Emirati combat operations throughout the region.85 Furthermore, Emirati PMSCs that employ US (and otherwise Western) personnel are linked to controversial arms transfers to regional proxies that apparently violate international arms embargoes and US sanctions.86

172 TI-O5-2020.
174 Information gathered from ADAC website.
175 Additional information gathered from LinkedIn, EDGE, n.d.
178 NSRC, n.d.
179 Roston 2018a.
180 Ibid
182 Roston 2018a.
Around 2010, MbZ commissioned Erik Prince to recruit a rapidly deployable combat battalion composed largely of Latin American veterans to face down internal and external security threats. MbZ reportedly specified that recruits should be non-Muslim, believing that Muslims could not be trusted to carry out violence against other Muslims. This force was reportedly deployed to Yemen following devastating attacks that killed dozens of Emirati soldiers, suggesting such forces help conceal military losses overseas and minimize political costs. In 2015-2016, the UAE also hired a group of Western veterans (including former US special forces operators) to kill and capture political opponents in Yemen. The UAE provided them with weapons and temporary ranks within the armed forces’ command structure.

In Libya, the UAE is a prominent sponsor of non-state militias in the country’s east, particularly the warlord Khalifa Haftar. A 2021 UN report described two connected operations in 2019 and 2020 conducted by a UAE-based PMSC, Lancaster6. The “Project Opus” operations, which ultimately failed, were meant to supply Haftar with a team of hired commandos – equipped with helicopters, drones, boats, and cyber capabilities – who would conduct assassinations and kidnappings. Lancaster6 reportedly received at least US$80 million for the operations. This team included a US citizen, and it appears Erik Prince brokered the operation to Haftar. Prince also appears to have supplied several of the militarized aircraft used in the operation, though he denies any involvement. While the extent of the UAE’s role in facilitating this operation is unknown, the UN report found that the PMSC planned to use Emirati equipment during the second operation in 2020. Furthermore, the UAE refused to cooperate with the UN investigators despite being in a unique position to provide critical information on Lancaster6’s corporate and financial connections.

Figure 3: Map of Middle East and North Africa

---

188 Cole 2019.
190 Roston 2018b.
191 Ibid.
192 The PMSC in fact operated through 3 interlinked companies: Lancaster 6 DMCC, L-6 FZE, and Opus Capital Asset Limited FZE. UNSC 2021, pp. 306-334.
193 Ibid. p. 307.
194 Ibid p. 308.
196 Ibid.
197 Ibid pp. 31-32.
198 Ibid p. 324.
The UAE’s use of PMSCs in Libya extends well beyond the failed Project Opus operations. In 2020, the US Defense Intelligence Agency assessed that the UAE provided financing for Wagner Group operations in Libya to support Haftar-aligned forces. Wagner Group appears to have focused on seizing and controlling Libyan oil infrastructure, and it is accused by the UN of committing war crimes. In a separate instance, a Human Rights Watch investigation revealed that the UAE recruited hundreds of Sudanese contractors under a false premise of security jobs in the Emirates, before deploying them to Libya as rearguards in the country’s eastern provinces.

In East Africa, the UAE funded a privately trained militia for the regional government of Puntland (an autonomous region of Somalia) in 2012. The Puntland Maritime Security Force was trained by Sterling Corporate Services, a PMSC registered in Dubai, in an arrangement that was reportedly brokered by Erik Prince. A UN monitor alleged that this training mission violated an arms embargo on Somalia, and it also documented a number of human rights abuses at the hands of this force. If true, Erik Prince would have also likely violated US arms export control laws. The UAE agreed to similarly train Somaliland’s security forces in March 2018 as part of a broader plan to develop a military (later civilian) logistics hub in the region. Somaliland is a separatist region of Somalia that has regularly clashed violently with the central government. Around the time of the training agreement, Somaliland’s armed forces were engaged in deadly border skirmishes with Puntland that threatened a broader war.

Beyond providing, brokering, and training additional boots on the ground, US and Western citizens working for Emirati PMSCs also support more subtle Emirati interventions in regional conflicts. Planes owned by Maximus Air Cargo have flown supply missions to military bases in Eritrea, Ethiopia, Libya, and Yemen either in direct support of the UAE armed forces or for Abu Dhabi’s allies and proxies. For example, the aforementioned UN report on Libya documented numerous flights by Maximus Air Cargo in support of Khalifa Haftar, likely ferrying arms. Associated Press connected several Maximus flights to the UAE’s drawdown of the Assab military base in Eritrea. Maximus aircraft have also been documented supporting a military air bridge to Ethiopia. An interview with a British employee indicates Maximus has flown supply missions to Yemen.

In 2020, the US Defense Intelligence Agency assessed that the UAE provided financing for Wagner Group operations in Libya to support Haftar-aligned forces. Wagner Group appears to have focused on seizing and controlling Libyan oil infrastructure, and it is accused by the UN of committing war crimes.

---

201 The company that hired these men, Black Shield Security Services, is reportedly owned by Da’ien Saif Muaded al-Kaabi, who was a colonel in the armed forces and the UAE’s defense attaché to Russia. It is unknown if he is related to any of the other al-Kaabi clan members mentioned in this report. Zayadin, Hiba. 2020. Recruited as Security Guards in the UAE, Deceived into Working in Conflict-Ridden Libya Instead. New York: Human Rights Watch. 1 November.
204 In 2011, the US Department of State amended US arms export control regulations to make it a policy to deny requests by US Citizens or permanent residents to provide defense articles or services to Somalia because of the United Nations arms embargo on Somalia, see US Federal Register Vol. 76, No. 152 August 11, 2011, pages 47992-3; Mazzetti, Mark & Eric Schmitt. 2012. ‘Private Army Formed to Fight Somali Pirates Leaves Troubled Legacy.’ New York Times. 4 October.
205 Cornwall, Alexander. 2018. ‘UAE to Train Somaliland Forces under Military Base Deal.’ Reuters. 15 March.
207 UNSC 2021, pp. 267-268.
209 Al Jazeera. 2021. ‘UAE air bridge provides military support to Ethiopia govt.’ Al Jazeera. 25 November. See also Twitter post dated 23 November 2021 by ‘Gerjon.’
210 Airline Routes & Ground Services. 2018. ‘Handling the complicated.’ Airline Routes & Ground Services. 5 June.
TigerSwan is a US PMSC based in North Carolina. It was founded in 2005 by veterans of the US Army’s elite Delta Force unit, particularly a former lieutenant colonel named James Reese. Under Reese’s leadership, TigerSwan and its affiliate companies received over US$60 million in US Government contracts, almost US$46 million of which were for services delivered abroad. Within the US, TigerSwan provided security for major oil pipeline projects. Outside of the US, TigerSwan provided security or construction oversight for the US Government in countries such as Afghanistan, Iraq, and Syria.

However, TigerSwan has reportedly engaged in various questionable or controversial practices in connection with several of its projects. The most significant of these accusations includes inflating threat perceptions, concealing its affiliations, cost inflation, and working with questionable local partners. Some of these alleged practices have resulted in civil or criminal court cases, including one case involving the bribing of US law enforcement officials. Some of these issues present risks to TigerSwan supporting corruption, fraud, and excessive use of force against civilians. TigerSwan has said many of these accusations are based on “one-sided complaints, disproven allegations, biased ‘news’ outlets, and other unreliable sources.”

TigerSwan continues to provide support for US Government-funded prime contractors in countries such as Syria.

In 2019, Reese apparently used his connections through TigerSwan to co-found a separate company, Delta Crescent Energy, to refurbish oil fields in Northeast Syrian and help sell the oil abroad. The US Government supported this endeavor, and it provided Delta Crescent with a unique sanctions waiver to trade Syrian oil. However, it appears Delta Crescent did not accomplish its goals in part due to pervasive local corruption. Delta Crescent denies that corruption played a role in its failure of the project in Syria and raised concerns about many factual statements in this case study.

### 4.1 US Oil Pipelines

During Reese’s time running TigerSwan, the PMSC was hired by Energy Transfer Partners (ETP) to provide security services in support of their oil pipeline construction projects in Louisiana, Pennsylvania, North Dakota, and elsewhere. The company or its employees reportedly engaged in various questionable or contentious practices that received negative media and legal attention while working for ETP. TigerSwan has been accused of exaggerating threat perceptions of the anti-pipeline protesters. An investigation by *The Intercept* described how TigerSwan employees appear to have used fake identities to infiltrate protest camps and orchestrated social media campaigns denouncing anti-pipeline protesters. TigerSwan also reportedly encouraged law enforcement to take more punitive actions against the protesters. Civil rights groups have accused law enforcement of excessive force against the protesters. Hundreds of protesters were injured and arrested. Some law enforcement and National Guard personnel were also injured.

Some national media, local private security contractors, and protesters accused TigerSwan of inflating threat perceptions about the protesters in North Dakota. Based on internal documents leaked from a TigerSwan contractor, *The Intercept* reported that TigerSwan compared protesters to ‘jihadist fighters.’ TigerSwan also said ‘currently there is no information to suggest...’

---

213 Harp, Seth. 2018. ‘A Year After the End of ISIS Control in Raqqa, a Ruined City Looks to Rebuild.’ The New Yorker. 5 December.
terrorist[-]type tactics or operations’ by the protesters, but stated ‘with the current limitation on information flow out of the camp, it cannot be ruled out,’ according to a leaked TigerSwan situation report. TigerSwan has raised concerns about the accuracy of some of the leaked documents and the one-sided nature of the above accusations. TigerSwan also received scrutiny for orchestrating questionable or misleading public media campaigns in support of pipeline projects. In 2017, James Marks, a retired general and then-chairman of TigerSwan’s advisory board, spoke at public meetings in favor of pipeline projects, published pro-pipeline op-eds, and voiced opposition to protesters in news outlets, without disclosing his affiliation with TigerSwan. One of these contractors alleged that the company made millions from the chaotic situation, and that it even overcharged ETP by claiming costs for personnel who were not present. TigerSwan has raised similar concerns about the one-sided nature of the above accusations.

TigerSwan also received scrutiny for orchestrating questionable or misleading public media campaigns in support of pipeline projects. In 2017, James Marks, a retired general and then-chairman of TigerSwan’s advisory board, spoke at public meetings in favor of pipeline projects, published pro-pipeline op-eds, and voiced opposition to protesters in news outlets, without disclosing his affiliation with TigerSwan. TigerSwan has raised similar concerns about the one-sided nature of the above accusations.

disclosing that he was president of an association to which TigerSwan was a major donor.

TigerSwan’s or its employees used several methods in an apparent effort to influence law enforcement in support of ETP. In December 2019, two TigerSwan employees were criminally charged in Pennsylvania for bribing local constables to guard another ETP pipeline construction site. According to the criminal complaint, ETP’s security manager (who oversaw TigerSwan) stated in an email that it was the company’s “unwritten policy” to hire law enforcement officials as guards, which TigerSwan facilitated. In February 2021, a judge allowed the charges against the two employees to be dismissed as a result of their cooperation with investigators and agreement to participate in a diversionary program for first-time offenders. In North Dakota, TigerSwan embedded liaisons within local police departments and supplied sheriffs with regular situation reports regarding anti-pipeline protests. Much of this information was reportedly gathered by TigerSwan employees who had assumed false identities and infiltrated protest camps. Reese denied such methods were approved, though leaked documents obtained by The Intercept appear to substantiate that such methods were used. TigerSwan reportedly urged police officers to employ more punitive measures against protesters, including arresting protestors and increasing fines for those arrested.

According to CCR, some of these practices can blur the line between public safety and private security.

The American Civil Liberties Union – another American civil rights organization – argued that TigerSwan’s business practices likely led to excessive violence and harm against private citizens, especially those from minority backgrounds, practicing their civil rights.
Standing Rock protesters have said law enforcement agencies confronted them with excessive force, culminating in over 300 wounded and hundreds more arrested.\textsuperscript{236} There were reports of “six law enforcement officers and North Dakota Guard soldiers” being injured.\textsuperscript{237} In 2017, several Pennsylvania residents opposed to pipeline construction on their property filed civil claims against TigerSwan and its employees for orchestrating a disinformation campaign against them, publishing personal information, trespassing on their property, and conducting invasive surveillance.\textsuperscript{238} Several of the plaintiffs were arrested by law enforcement officials on charges that ultimately were not prosecuted, leading to accusations of false arrest.\textsuperscript{239} While TigerSwan and the employees denied these allegations and motioned to have them dismissed, the court refused on most charges; as of July 2022, the trial is ongoing.\textsuperscript{240}

4.2 Afghanistan, Iraq, and Syria

It appears TigerSwan has also used controversial business practices in Afghanistan and Iraq. In Afghanistan, the company reportedly concealed ownership of a subcontractor and failed to justify millions of dollars of costs in a reconstruction project, according to an audit by the Special Inspector General for Afghanistan Reconstruction (SIGAR). TigerSwan also reportedly failed to conduct due diligence in choosing local partnerships in Afghanistan. In Iraq, TigerSwan subcontracted a local PMSC run by an Iraqi government official whose family reportedly engaged in suspicious financial transfers of money outside of the country. The above activities increase the risk of price-gouging on US Government contracts, supporting local corrupt actors, and potentially inflaming local conflict dynamics.

In 2020, a SIGAR audit found that TigerSwan engaged in several misleading practices while overseeing the implementation of construction projects funded by the US Department of State in Afghanistan. It found that TigerSwan subcontracted a company that it had a majority stake in without disclosing this relationship.\textsuperscript{241} The company also failed to prove that its local subcontractors weren’t disqualified or banned from receiving US funds.\textsuperscript{242} The audit also found that TigerSwan failed to justify its costs with verifiable price analyses, and it selected subcontractors without a competitive bid process. As a result, about half of the costs incurred on a US$7 million contract were deemed questionable due to poor subcontractor oversight and that the US Government “may have paid more in costs than is reasonable or appropriate” for what it received.\textsuperscript{243} While TigerSwan disputed the findings and denied any wrongdoing, the company failed to provide sufficient evidence to the contrary when given the chance to do so by the auditing entity.\textsuperscript{244}

The creation of separate, but connected businesses, runs the risk of PMSCs inappropriately winning government contracts. In 2010, several companies protested the awarding of a US$7 million US Navy training contract to a company they alleged was controlled by TigerSwan, which was not eligible for the contract due to its size.\textsuperscript{245} In the course of the company’s appeal against these protests, a court found that TigerSwan’s founders created the company, put it into an opaque corporate holding arrangement in which they were minority (49 percent) shareholders, and that the company was taken over by a fellow Delta Force veteran.\textsuperscript{246} It also found that the company shared a business address with TigerSwan, and that its only previous business was as a subcontractor for TigerSwan.\textsuperscript{247} The company disputed that it was controlled by TigerSwan, arguing these factors alone did not constitute “economic dependence,” that the address had changed, and that its previous work for TigerSwan was too limited to infer a deeper affiliation, which the court accepted.\textsuperscript{248} In an ongoing court case, the US Government accused TigerSwan and DynCorp of misrepresenting TigerSwan’s role in a multi-billion dollar contract to provide Arabic translators for US military operations in Iraq.\textsuperscript{249} TigerSwan’s motion to dismiss the

\textsuperscript{241} ibid
\textsuperscript{243} ibid
\textsuperscript{244} ibid
\textsuperscript{246} ibid, pp. 1-3. Additional information gathered from LinkedIn.
\textsuperscript{247} ibid, pp. 2-3.
\textsuperscript{248} ibid, pp. 3-7.
charges was denied in September 2019; as of July 2022, the trial is still ongoing.\textsuperscript{250}

TigerSwan has also hired subcontractors in Iraq with questionable ties to government officials, which runs the risk of supporting corrupt actors or activities. In 2018, TigerSwan subcontracted a local logistics firm called PowerGate, which is run by a relative of an Iraqi provincial governor, while providing security for an American firm overseeing third party projects in Syria funded by the US Agency for International Development.\textsuperscript{251} The governor’s province, Duhok, lies on the border with Syria and is a prominent part of the autonomous Kurdish region of northern Iraq. Given the corruption concerns within Northern Iraq, (see Box 2), there is a risk that US government funds could inadvertently strengthen corrupt actors or networks in the region.

\textbf{Box 2}

\textbf{Corruption in the Iraqi Kurdistan}

Northern Iraq, which is predominantly Kurdish, is run by the autonomous Kurdistan Regional Government (KRG). The KRG is ruled essentially by two political parties that are closely associated with prominent political families. Nepotism and cronyism are common as these families reward their patronage networks with jobs in the public service, state contracts, and exclusive access to resources.\textsuperscript{252} Foreign companies are required to subcontract local firms run by connected businessmen at inflated rates.\textsuperscript{253} The Barzani family, which holds both the KRG presidency and the premiership under the KDP, dominates key sectors of the KRG economy — including the oil sector and cross-border trade into Syria — through crony monopolies and through state control.\textsuperscript{254}

As such, foreign companies like TigerSwan are highly vulnerable to extortion and corruption when operating in the KRG. The Barzani family is said to control the cross-border economy and access into Northeast Syria.\textsuperscript{255} Politically affiliated traders monopolize cross-border commerce, especially for key commodities where high tariffs can be levied by the KRG.\textsuperscript{256} Furthermore, the KRG security agency responsible for issuing security authorizations to PMSCs like TigerSwan is accused of being highly politicized and loyal to the Barzani’s political party.\textsuperscript{257} Observers note that the KRG’s Prime Minister, Masrour Barzani, has become increasingly authoritarian in his rule, resulting in increasing violence, repression, and emigration from the region.\textsuperscript{258}


251 Harp, Seth. 2018. ‘A Year After the End of ISIS Control in Raqqa, a Ruined City Looks to Rebuild.’ The New Yorker. 5 December.


256 Hatahet 2019.

257 Barawi, Aras. 2018. ‘Security service Asayish of Duhok is corrupted in Iraqi Kurdistan.” eKurd. 3 August.

In other parts of Iraq, TigerSwan partnered with an Iraqi politician named Mudhar Shawkat, who owned a local PMSC called Babylon Eagles Security Company (BESC) and whose family engaged in questionable financial transfers. This partnership supplied TigerSwan with local manpower for its Iraqi operations, which included the provision of armed security and logistics support to the US Government and private clients. It appears Shawkat also connected TigerSwan to Iraqi security institutions through his political clout. Shawkat claims he was “a department head in the Iraqi Ministry of National Defense” during the Saddam era and served in high level government positions after the 2003 Iraq invasion. He was reportedly responsible for securing Iraq’s national telecommunications infrastructure – a task that was carried out by BESC in an apparent case of self-dealing. Leaked emails also show that Shawkat’s family moved over US$170 million outside of Iraq in 2009 through an elaborate corporate mechanism that a financial services provider found “suspicious.” Such partnerships can also divert US Government funds into nebulous patronage networks that empower local armed groups, including US adversaries and barred actors. In Iraq, Shawkat attempted to form a Sunni militia led by Saddam-era military officers, with the goal of establishing an autonomous Sunni region out of former Islamic State territory in 2014. Though Shawkat (unsuccessfully) sought out US support for this militia, other US PMSCs in Iraq have become entangled with more hostile actors through the patronage networks of their local partners. In 2017, a US PMSC that operated a major Iraqi airbase reportedly purchased fuel at inflated rates from a vendor connected to the base’s commander. This commander is apparently related to the leader of a militia aligned with Iran. Members of this militia stole electrical equipment from the PMSC with the alleged approval of the airbase’s commander.

---

263 Ibid
266 Kopplin, Zach. 2021. ‘How the Pentagon Accidentally Funnels Millions to Iraqi Militia Groups It’s Also Fighting.’ American Prospect. 25 March.
267 Ibid
4.3 The Delta Crescent Arrangement

In Northeast Syria, James Reese appears to have used his local connections in Iraq and Syria through TigerSwan to secure oil rights in an arrangement that posed risks to US goals in the region. In 2019, he co-founded an oil company called Delta Crescent Energy, which secured rights with the Kurdish-led Autonomous Administration of Northeast Syria (AANES) to refurbish the region’s damaged oil infrastructure and broker the output internationally.\(^{268}\) To do so, Delta Crescent received a unique license from the US Government, exempting it from US sanctions on Syria.\(^{269}\) Former administration officials argued that the arrangement would provide the US-allied AANES with extra revenue, deny the Assad regime oil access, and give the US leverage over Russia in future negotiations.\(^{270}\) However, it appears that some of these expectations may have been undermined by pervasive corruption within the region.

According to the Daily Beast, Reese claims the idea for the company was his originally.\(^{271}\) The Financial Times reported that he learned of the opportunity through his TigerSwan connections with the Kurdish leadership.\(^{272}\) In a 2018 trip on behalf of TigerSwan, Reese met with Nechirvan Barzani, the KRG president and cousin of the Prime Minister, and also visited Northeast Syria. However, Reese says the meeting with Barzani and the KRG had nothing to do with Delta Crescent.\(^{273}\) According to the Daily Beast, Reese says that he introduced the idea to Mazloum Abdi, head of the SDF, around this time.\(^{274}\) Shortly after, Reese partnered with two people who, according to the Washington Institute, were well-positioned within the US political establishment and oil industry to initiate the idea and win US support.\(^{275}\)

James Cain, a prominent donor and former committeeman within the Republican Party, was reportedly well-connected within Washington, while John Dorrier, who ran the oil company that previously operated the oil fields in question, could guide the technical aspects of the arrangement.\(^{276}\)

In order to refurbish the Syrian oil fields, Delta Crescent received a license from the US Department of Treasury’s Office of Foreign Assets Control (DoT OFAC) exempting it from a blanket ban on Syria’s oil trade.\(^{277}\) It appears that through their collective connections, the three Delta Crescent founders won special support within the US political establishment, including from US Senator Lindsey Graham and the US Government’s main envoy to Syria.\(^{278}\) According to former US administration officials, they supported the Delta Crescent license for three key reasons. Firstly, they believed the arrangement would provide needed revenue to the AANES, following the Administration’s sudden decision to end its “stabilization assistance” to the Syrian Kurds.\(^{279}\) Secondly, the Administration believed the arrangement would prevent the SDF from selling crude oil to the Assad regime.\(^{280}\) Third, they believed the arrangement

---

269 Ibid.
274 Rosen 2021.
277 Zaman 2020.
279 Tabler 2021.
280 Ibid
would give US leverage over Russia in future negotiations over the Syria conflict.  

By April 2021, Delta Crescent said it had imported and installed US-origin technology on oil infrastructure in Northeast Syria. Its local partner in Northeast Syria is Jazeera Oil Company, which operates the oil fields. Delta Crescent claimed it had an established presence, including an office with 10-15 staff, in a town called Rmelan. Although it appears TigerSwan employed several hundred personnel in the KRG and Syria around this time, there is little evidence they directly provided security services to Delta Crescent. TigerSwan and Delta Crescent have also told Transparency International that they have not had any business relationship with each other. In May 2021, Delta Crescent reportedly secured two contracts worth about US$2.3 billion to “sell and transport” the oil outside of Syria.

However, it appears Delta Crescent struggled to gain the expected revenue due to substantial, unexpected resistance from the neighboring KRG. Several scholars, experts, and researchers note that the Barzani family, which dominates KRG politics and holds many of the region’s executive functions, controls the flow of Syrian oil into the KRG and dominates the local oil industry. Citing insider conversations, the Daily Beast reported that Mansour Barzani, the brother of the KRG’s Prime Minister, reportedly demanded 70 percent of the revenue from the Syrian oil, leading to a dispute with Delta Crescent and the AANES. Scholars note that the Barzani family effectively controls the border crossings linking the two regions, and the Daily Beast reported that because they already acquire oil from Northeast Syria at very low prices, they are well-positioned to extort Delta Crescent into granting an excessive cut of the deal’s revenues. Delta Crescent reportedly sought to bypass the KRG and export AANES oil through non-Kurdish Iraq, though similar dynamics of patronage and extortion are well-documented in these regions as well.

It also appears the Delta Crescent arrangement did little to stop AANES oil from reaching the Assad regime as the US Government had hoped it would. Much of the oil produced by these fields is reportedly sold to the Syrian regime at well below the market price through local smuggling networks. Hossam al-Qaterji, who is a regime-aligned business magnate, is said to facilitate much of this smuggling. OFAC sanctioned al-Qaterji in November 2020 due to his role in sustaining the
A 2020 investigation by independent Syrian journalists found that the Assad regime was a key recipient of AANES oil through al-Qaterji’s smuggling network.

As a result of the above challenges, it appears the Delta Crescent arrangement accomplished few, if any, of the goals laid out by the US Government. Observers also note that the arrangement could expose the US to war crime accusations relating to pillage. In May 2021, the US Government indicated that it would not renew Delta Crescent’s OFAC license. Former US officials indicated that Delta Crescent continued to operate until at least the end of 2021 as the company was allowed to wind down operations before the end of the year. In May 2022, the Treasury Department announced it “authorized some foreign investment in areas of northern Syria that are outside government control” for the purpose of “defeat[ing] Islamic State through economic stabilization.” This authorization reportedly includes the sale of oil products originating from beyond the Assad regime’s area of control.

300 Rosen 2021.
301 Al-Khair, Waleed Abu. 2021. ‘Private security companies provide facade for Russian hegemony in Syria.’ Diyaruna. 4 February.
303 Zaman 2021.
306 Ibid.
5.0 US ACTIONS TO REGULATE PMSCS AND RELATED GAPS

The US Government has recognized the serious risks of PMSC activities in fragile and conflict environments. It has participated in some multilateral efforts to develop a normative framework governing the international use of PMSCs and neglected other international efforts on mercenaries. The United States has also developed several laws and regulations to oversee PMSC contracts with the US Government, as well as foreign clients. However, this approach spreads oversight throughout the US Departments of Defense, State, and Commerce. There are major differences between the State and Defense Departments on how to award and oversee contracts with PMSCs. The State and Commerce Departments’ efforts to control US PMSC sales abroad are limited in scope and exclude major PMSC services. These limitations and loopholes can be exploited by PMSCs engaged in corrupt activities or with corrupt clients. By examining these US efforts to regulate PMSCs, the main weaknesses in the US regulatory approach to PMSCs can be identified.

5.1 US Multilateral Efforts to Regulate PMSCs

Over the past 30 years, the United States supported some international efforts to regulate PMSCs while neglecting others. The international community generally opposes the use of mercenaries in armed conflicts. In 1989, many countries agreed to the UN Mercenary Convention to expand restrictions on the use of mercenaries, though the United States never ratified the Convention. The United States, however, has agreed to a non-binding agreement, the Montreux Document, which establishes good practices for regulating PMSCs in armed conflicts. Though these efforts produced some positive results, they are beset by challenges. There are only a few countries that have agreed to the international accreditation standards established in the Montreux Document. These standards also struggle to meet the modern PMSC industry’s rapid proliferation and diversification of activities and contexts. The United Nations is seeking to address these gaps through a new international framework.

International law addresses the use of mercenaries. The foundational documents are Article 47 of the 1977 Protocol I Additional to the Geneva Conventions (part of International Humanitarian Law, or IHL) and the 1989 International Convention against the Recruitment, Use, Financing and the Training of Mercenaries (also known as the UN Mercenary Convention). Article 47 defines mercenaries as a person who is recruited to fight in an armed conflict, engages in direct hostilities, and is paid more than the local military. While IHL does not explicitly ban the use of mercenaries, it defines their status as persons who are not entitled to the rights of combatants, such as those afforded to prisoners of war. The UN Mercenary Convention, on the other hand, bans the recruitment, training, use, and financing of mercenaries by signatory states. This document importantly covers situations outside of armed conflicts, such as using mercenaries to overthrow elected governments. Though the United States never formally ratified the UN Mercenary Convention, these documents form the normative basis for subsequent international efforts to regulate PMSCs.

The US Government supports efforts to distinguish PMSCs from mercenaries and carve out a regulated space in which PMSCs can operate. In 2008, an initiative led by the Swiss Government and the International Committee of the Red Cross (ICRC) produced the Montreux Document. This US government-supported, non-binding agreement clarifies the legal obligations of PMSCs under IHL and provides recommended good practices for countries that host and contract such companies. These practices include ensuring that countries do not hire PMSCs that have a record of engaging in bribery and corruption, among other crimes. The Montreux Document defines PMSCs as "private business entities that provide military and/or security services, irrespective of how they describe themselves. Military and security services include, in particular, armed guarding and protection of persons and objects, such as convoys, buildings, and other places; maintenance and operation of weapons systems; prisoner detention; and advice to or training of local forces and security personnel." There are now 58 countries that have stated their support for this agreement.

311 ibid
Similar but separate to the Montreux Document, the 2010 *International Code of Conduct for Private Security Service Providers* (ICoC), which lays out principles of conduct that participating PMSCs must abide by. The ICoC includes PMSC services like maritime security, crowd management, and “operational and logistical support for armed or security forces, including training and advice, intelligence, surveillance and reconnaissance activities.” The ICoC is administered by the International Code of Conduct Association (ICoCA), a Swiss NGO that also acts as a certification body. Association membership is granted to PMSCs who comply with a set of accredited industry standards, allow external review by ICoCA, and submit regular reports. The US Government is a participating state in ICoCA and provides funding to support it. Only 10 US PMSCs are members or are affiliated with the mechanism.

The UN plays a prominent role in these efforts under the Office of the High Commissioner on Human Rights (OHCHR). Specifically, the Working Group on the Use of Mercenaries (UNWG), a group of independent experts mandated to monitor mercenaries and mercenary-related activities in all their forms and manifestations. As such, the UNWG monitors and studies PMSC activities, reports on relevant human rights abuses and humanitarian law violations, and communicates with relevant government and PMSC actors. Parallel to this, an Intergovernmental Working Group (IGWG) on PMSCs acts as the official forum and dialogue process for states on the norms of PMSC use. This working group is in the early stages of drafting a new international agreement that would establish common principles for regulating international PMSC use, but the United States has not been an active participant of this process. The IWG cooperates with the UNWG, ICoCA, and the Montreux Document Forum.

In practice, several weaknesses undermine the effectiveness of this international framework. The definition of mercenaries contained in Article 47 has been criticized for being overly narrow and difficult to apply. Key states like the United States, Russia, and China never ratified the UN Mercenary Convention, greatly limiting its international weight. Meanwhile, the Montreux Document and ICoC’s definition on PMSC services excludes activities such as cybersecurity and some intelligence activities. ICoCA membership was supposed to act as a stamp of quality control and therefore provide participating PMSCs with a competitive advantage. However, ICoCA participation membership stagnated with less than 70 participating companies and only seven participating governments – none of which are located in conflict-affected countries. This stagnation of ICoCA members, as well as the lack of funding streams for their type of activities, has led to a funding shortfall that severely restricts the body’s ability to monitor PMSC activities and detect abuses. Finally, the scope of the Montreux Document only applies to armed conflict situations, though there are serious concerns about PMSCs activities in non-conflict countries.

5.2 US Oversight of PMSC Contracts with the US Government

Government contracting is the most direct means in which the US Government regulates the PMSC industry. Yet contracting regulations arose in a reactive manner, responding to high-profile abuses by contractors in Iraq and Afghanistan. Efforts to boost contracting regulations helped expand government control over PMSCs and promoted some accountability measures. However, there are still weaknesses within this regulatory mechanism that undermine contractor accountability. These loopholes could become more pronounced as the United States transitions away from the Global War on Terror and the industry grows and diversifies.


314 ibid


319 ibid


324 Author interview with current ICoCA board member in June 2022.
5.2.1 Main US regulatory actions on PMSCs

Following the 2007 Nissour Square Massacre, the US Government sought to improve oversight of the PMSCs it hires. The US Congress developed a framework for regulating contracted PMSCs in the 2008 National Defense Authorization Act (NDAA). It mandates that the US Department of Defense (DoD), in coordination with the US Department of State (DoS), develop a management system for monitoring and controlling the activities and standards of contractors in designated combat zones. Specifically, Section 862 requires that the Secretary of Defense establishes PMSC training and vetting standards for all US Government agencies contracting PMSCs in designated combat zones, develops a registry for contractor personnel and equipment (now known as SPOT-ES) as well as an incident reporting mechanism, conducts independent reviews and investigations of contractors when misconduct is identified, and makes agency-specific policy guidance readily available. This framework also added obligatory contract clauses to the Federal Acquisition Regulation System (FARS).

Stemming from this framework, PMSCs must possess industry accreditation to compete for US Government contracts. This entails a certification called ANSI PSC.1 (known as ISO 18788 internationally), which certifies that a PMSC has a proven quality management system that is in line with national and international laws, including International Humanitarian Law (IHL). PMSCs are subject to external audits to acquire and maintain accreditation. In the United States, this accreditation is administered by an industry-oriented certification body that is run as a private company and is funded by the PMSC industry through membership fees. ANSI PSC.1 addresses corruption, bribery, and conflicts of interest: accredited PMSCs must maintain a code of ethical conduct that forbids corrupt practices; address conflicts of interest with subcontractors; provide staff training on ethical and humanitarian issues that can include corruption; and keep auditable records.

The Defense Department assigned several offices with oversight of PMSC contracts and issued updated regulations on inherently governmental roles that cannot be contracted out. The Office of the Under Secretary for Defense for Acquisition and Sustainment plays a key oversight role by issuing guidance on and monitoring the visibility of PMSCs. Geographic Combatant Commanders are tasked with developing area-specific requirements for the internal vetting, training, and conduct of contracted PMSC personnel. They must also track and monitor the personnel and weaponry deployed by PMSCs in their areas of responsibility, and investigate PMSC-related incidents when they occur. Individual military units and DoD offices must identify their contracting needs and ensure they do not include inherently governmental functions. Contracting officers and their representatives assigned to these units or offices establish the contract clauses and monitor contracts with PMSCs.

In 2008, the State Department, Defense Department, and USAID made a conscious effort to coordinate contracting processes in designated combat zones, culminating in the adoption of a joint memorandum of understanding. In such areas, US Government agencies can coordinate contracting requirements, harmonize vetting and data collection standards, and operate joint databases. Despite localized coordination efforts, different agencies nevertheless maintain different standards and protocol of contractor oversight at the departmental level. For example, the State Department requires that any PMSC contracted in a security role must be a member of IGoCA and accredited with ANSI PSC.1, whereas the Defense Department only requires the latter.

There are also many offices within the State Department that oversee PMSCs. Two key offices are the Office of...
5.2.2 Key gaps in US oversight

There are several important gaps in US efforts to effectively oversee PMSC contracts with the US government. Staff reductions within both the US Departments of Defense and State pushed some PMSC oversight functions to less qualified personnel over the last few years. From 2017-2020, the Defense Department eliminated the Office of the Deputy Assistant Secretary of Defense (DASD) Program Support, which oversaw interagency coordination with other US government agencies to ensure that DoD contractor policy and regulations were consistent with the overall US national security strategy.\(^\text{341}\) It reduced the main DoD policy office tasked with PMSC contracting in combat zones to two civilian staff (with contractor support).\(^\text{342}\) As a result, PMSC oversight fell overwhelmingly on low level contracting officer representatives, who are often overtasked and inadequately trained for this role. It also led to a breakdown of critical oversight functions, such as the verification that senior commanders had developed and implemented PMSC contracting guidance in their areas of responsibility. A 2019 report by the State Department Inspector General also found that staff overseeing State Department contracts suffered from manpower shortages and undertraining.\(^\text{343}\)

The creation of different standards and guidance for the Defense and State Departments poses challenges to effectively identifying and mitigating corruption risks both before and after a contract is awarded. The Defense Department contracting officer handbook provides extensive guidance on identifying and preventing various corrupt practices (conflict of interest, bribery, corruption, etc.) among contractors. Furthermore, internal Defense Department regulations describe several examples of contractor conflicts of interest that oversight staff can use. By contrast, the State Department contract officer guidance documents just briefly mention corruption types and provide scant guidance on corruption examples (see table 1). Furthermore, the State Department requires PMSCs to be a member of ICoCA and receive ANSI PSC-1 accreditation whereas the Defense Department only requires ANSI PSC-1 accreditation.

There continues to be key gaps in how the Defense and State Departments vet subcontractors. According to a review by the Government Accountability Office (GAO), 12 percent of PMSC personnel hired as security guards by the Defense Department were from companies that did not have proper certification for this role.\(^\text{344}\) The Defense and State Departments rely on prime contractors to do the vetting of second and third-tier subcontractors. US regulations require prime contractors to only show their first-tier subcontractors to the Defense Department when bidding for a government contract.\(^\text{345}\)

---

338 ibid. pp. 41-42.
341 Author interview with former senior DoD contracting official, 22 January 2021.
342 Author interview with former senior DoD contracting official, 22 January 2021.
344 GAO 2021.
Table 1: Comparison of US Government guidance on anti-corruption measures by agency

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidance on Internal Conflicts of Interest</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Guidance on Contractor Conflicts of Interest</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Guidance on fraud, waste, and abuse</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Guidance on pricing evaluation</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Guidance on gifts</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Guidance on agents</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Defines corruption terminology</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Gives theoretical examples of corruption</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Gives real-world examples of corruption</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Mentions of conflict of interest</td>
<td>57</td>
<td>47</td>
<td>4</td>
</tr>
<tr>
<td>Mentions of kickbacks</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>


As seen in TigerSwan’s contracts in Afghanistan and Iraq, prime contractors can apparently fail to conduct effective due diligence. Relying on them to do these checks can create subcontractor dependence on the prime contractor, facilitate corruption, and hide conflicts of interest and dangerous partnerships. The 2021 NDAA added a requirement for US Government contractors and subcontractors accused of malfeasance (criminal or administrative proceedings, fines, etc) to disclose their beneficial ownership. This new requirement could improve oversight, but it is still narrow.

It also appears there are flaws in the use of private organizations for accrediting PMSCs. As noted above, in order to contract with the US Government, PMSCs must possess an industry accreditation that attests to a code of ethics, quality assurance, and recognition of IHL. However, the private associations that administer such accreditation are funded in part by PMSCs, presenting clear conflicts of interest. This potentially waters down the value of such certification, as contentious PMSCs like TigerSwan are able to receive accreditation despite numerous legal issues. Furthermore, the international protocols endorsed by the United States are voluntary, non-binding instruments that have little impact on the PMSCs and clients that do not ascribe to them. For example, membership in ICoCA is stagnant, with only 66 PMSCs and 7 participating governments (none of which are conflict-affected, fragile states) in December 2021.

Lastly, the US government lacks an effective means for monitoring its overall use of PMSCs between government agencies and geographic areas of operation. The Defense Department is the only agency that generates...
regular data on its use of PMSCs, though even this is fragmented as the various structures within the agency maintain their own datasets with differing definitions, indicators, and categorizations. This makes data aggregation on PMSC use impossible beyond mission-specific and geographic contexts. Furthermore, while most federal contracts are publicly reported through searchable databases like USASpending.gov, this database only shows the prime contractors. The lack of information on subcontractors obscures potential conflicts of interest in the subcontractor supply chain and conceals the true extent to which PMSCs receive US Government funding as subcontractors.

5.3 US Oversight of PMSCs Contracts with Foreign Entities

The US Government also regulates certain commercial sales by US PMSCs directly to foreign entities through both the State and Commerce Departments. These regulations largely focus on controlling the US export of military and sensitive technology, but there are specific instances in which US companies or US persons are required to seek US Government approval to export services. The US Government’s focus on controlling the export of technology, however, has resulted in clear gaps in US oversight of PMSC sales of military training, combat activities, armed guarding, and intelligence services abroad. Ambiguity in how the US Government monitors and verifies the end-use of such services also weakens oversight. There are few, if any, checks on subcontractors of PMSC services by the US Government and hardly any relevant information on PMSC sales is provided to Congress in State and Commerce Departments’ annual reports.

5.3.1 Main US regulatory actions on PMSCs

The United States has sought to reduce oversight of some PMSC exports, such as military training, while strengthening oversight of others, such as combat and intelligence services, to foreign clients over the past ten years. These initiatives have focused on the types of PMSC services that would require US Government pre-approval (a license) before export. The State Department provides oversight of US companies and US persons (US citizens or permanent residences) that want to export defense articles and services as defined in the International Traffic in Arms Regulation (ITAR; see below for definition) and the US Munitions List (USML). PMSC services that fall within the definition of defense services include training and advice to foreign militaries and repairing and maintaining weapons systems. DDTC has also narrowed the circumstances in which it requires US companies and US persons to obtain approval or a license through changes to the definition of brokering in ITAR. The Commerce Department regulates US companies that want to export certain surveillance technology and goods and services to military intelligence agencies. 350

From 2011 to 2015, the State Department’s Directorate of Defense Trade Controls (DDTC) proposed several changes to the ITAR definition of defense services. 351 Notably, these proposed changes would have limited the circumstances in which PMSCs would need a DDTC license to sell military training and weapons maintenance services directly to foreign entities (see table 2). For instance, a US company would not need a license to provide training on the basic operations of a US weapons system to foreign entities under the proposed rule change. However, the definition changes would have also strengthened oversight of US persons seeking to provide direct combat skills to foreign governments or entities.

While these definition changes were ultimately not approved, the Defense Trade Advisory Group (DTAG), a group of defense industry and other experts that formally advises the DDTC, continues to push for similar changes. In a 2018 DTAG White Paper, they proposed

---


351 US Federal Register, International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions proposed rule by the State Department, June 3, 2015.
Table 2: Comparison of Current and Proposed Definitions of Defense Services

<table>
<thead>
<tr>
<th>Current Definition</th>
<th>Excerpts from Proposed Definition in 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>The furnishing of assistance (including training) to foreign persons, whether in</td>
<td>The furnishing of assistance (including training) to a foreign person, whether in the United States or</td>
</tr>
<tr>
<td>the United States or abroad in the design, development, engineering, manufacture,</td>
<td>abroad, in the production, assembly, testing, intermediate- or depot-level maintenance, modification,</td>
</tr>
<tr>
<td>production, assembly, testing, repair, maintenance, modification, operation,</td>
<td>demilitarization, destruction, or processing of a defense article, by a U.S. person or foreign person</td>
</tr>
<tr>
<td>demilitarization, destruction, processing or use of defense articles.</td>
<td>in the United States, who has knowledge of U.S.-origin technical data directly related to the defense</td>
</tr>
<tr>
<td></td>
<td>article that is the subject of the assistance, prior to performing the service.</td>
</tr>
<tr>
<td>The furnishing to foreign persons of any USML-controlled technical data, whether in</td>
<td>The furnishing of assistance (including training) to a foreign person, whether in the United States or</td>
</tr>
<tr>
<td>the United States or abroad.</td>
<td>abroad, in the development of a defense article, or the integration of a defense article with any other</td>
</tr>
<tr>
<td></td>
<td>item regardless of whether that item is subject to the ITAR or technical data is used.</td>
</tr>
<tr>
<td>Military training of foreign units and forces, regular and irregular, including</td>
<td>The furnishing of assistance (including training) to a foreign person, regardless of whether technical</td>
</tr>
<tr>
<td>formal or informal instruction of foreign persons in the United States or abroad</td>
<td>data is used, whether in the United States or abroad, in the employment of a defense article, other than</td>
</tr>
<tr>
<td>or by correspondence courses, technical, educational, or information publications</td>
<td>basic operation of a defense article authorized by the U.S. government for export to the same recipient.</td>
</tr>
<tr>
<td>and media of all kinds, training aid, orientation, training exercise, and military</td>
<td></td>
</tr>
<tr>
<td>advice.</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>Participating in or directing combat operations for a foreign person, except as a member of the regular</td>
</tr>
<tr>
<td></td>
<td>military forces of a foreign nation by a U.S. person who has been drafted into such forces.</td>
</tr>
</tbody>
</table>

Sources: US Department of State, International Traffic and Arms Regulations, 22 CFR 120.9, access online on June 16, 2022. US Federal Register, International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions proposed rule by the State Department, June 5, 2015.

a new definition of defense services that would exclude US companies from applying for a license to train foreign entities on basic level maintenance of a US weapons system and the installation of any parts or components. US companies or persons would also not need DDTC approval to provide training to a foreign military based simply on their knowledge, training, or work experience. DTAG pushed to limit the definition of combat operations to just foreign governments rather than any foreign person. In a separate White Paper in 2021, DTAG encouraged DDTC to change the way defense companies must report any political contributions, commissions, and marketing fees in connection with a proposed export of defense articles or services from license-by-license reporting to annual reporting.

The State Department reduced its regulations and coordination on arms brokering, weakening US oversight of some PMSC activities abroad. In 2019, the State Department exempted US PMSCs providing defense services for US Government contracts from DDTC export licensing requirements. In an earlier regulation change, the State Department also limited the circumstances in which individuals covered by ITAR would need prior DDTC approval to connect buyers and sellers (often referred to as brokering) of some PMSCs services. For instance, a person or company would only need DDTC authorization if they were brokering a foreign PMSC service to a foreign government or entity as Erik Prince did for the UAE in Somalia. In contrast, Erik Prince would not need approval to broker the sale of PMSC services originating in the United States with a foreign government.

By compaison, the Commerce Department has added new elements to its Export Administration Regulations (EAR) to improve oversight of US companies exporting cyber intrusion tools and goods and services to certain foreign intelligence agencies. The Commerce Department, for instance, announced a rule in October 2021, requiring US companies to obtain a license from

353 Ibi
354 DTAG propose to raise the threshold for when defense companies must do this reporting from a sale worth US$600,000 to a sale worth US$1 million or more. They also suggested annual reporting on political contributions, commissions, and marketing fees instead of transactional reporting. US Department of State, Defense Trade Advisory Group, White Paper on Part 130 Reporting, May 20, 2021, https://www.pmddtc.state.gov/sys_attachment.do/sysparm_refering_url=/ear_ofview=1&sys_id=5da265d0be1b411d11eead054bdee7
the Commerce Department’s Bureau of Industry and Security (BIS) for the export of certain intrusion software or IP network communication surveillance to many countries. This requirement is in addition to other restrictions on the export of surveillance equipment found in the Commerce Control List. The Commerce Department also put restrictions on US companies working with US and foreign companies engaged in irresponsible cyber intrusion activities, such as the NSO Group (Israel), Candiru (Israel), Positive Technologies (Russia), and Computer Security Initiative Consultancy PTE. LTD (Singapore). In 2021, the Commerce Department strengthened regulations requiring US companies to seek a license before entering into or supporting business relationships with military intelligence agencies from ten countries such as Belarus, China, Iran, Russia, and Syria.

5.3.2 Key Gaps in US Oversight

The State and Commerce Departments still face several major gaps in their efforts to effectively oversee US PMSC sales to foreign entities. These gaps cover US regulations, vetting, and congressional and public reporting. The State Department does not have the regulations to effectively control US companies and US persons that want to engage in direct combat activities abroad. It also appears to give short shrift to vetting proposed PMSC sales of military training and weapons maintenance to foreign governments or entities. There is no requirement for PMSCs applying for a license to list all of their subcontractors. The Commerce Department’s new efforts to regulate US exports to certain foreign military intelligence agencies is laudable, but the regulations are limited to too few countries. The Commerce Department does not require PMSCs to obtain a license before providing armed security or police training to many highly corrupt officials, (see Table 3).

At the moment, there is no US law or regulation that requires all US persons to obtain US Government approval before engaging in combat activities abroad. It also appears to give short shrift to vetting proposed PMSC sales of defense services, but it does not appear that they assess any subcontractors that PMSCs may use for defense articles, but it does not appear that they assess any subcontractors that PMSCs may use for defense services. When US companies or persons apply for a license to export defense services, they must submit a TAA, which is essentially a contract that addresses the nature, scope, and duration of the contracted defense service, between the principal supplier(s) and the end-user. They must also submit a transmittal letter that explains the purpose and context of the agreement; relevant exhibits, appendices, annexes, and supporting documentation; and a letter from a

358 https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear
362 When applying for a DDTC license, for instance, a US company must certify that it has not been indicted or convicted for a full range of US laws and must provide information on foreign buyers and subsidiaries.
representative designated by the supplier certifying the supplier’s good legal standing and contracting eligibility. All US companies supporting the contract must co-sign the TAA and the principal applicant must declare any parent/subsidiary relationships with any of the other cosignatories. However, the principal is not required to disclose subcontractors – foreign or domestic – unless they are being licensed to directly use USML-controlled technology.

As mentioned in the previous sections on US PMSC contracts with the US Government, subcontractors are a critical conduit for embezzlement, self-dealing, and bribery. DDTC already scrutinizes other key pathways for corruption, such as offset arrangements, commissions, fees, political contributions, foreign ownership, and brokering. This scrutiny must extend to subcontracting as well, regardless of whether the subcontracted entities are foreign or domestic. In general, ownership information should be required of all TAA parties – including subcontractors – as the foreign ownership of a company is relatively easy to obscure through convoluted ownership chains. In some countries, the purchasing government may require the PMSC to hire a politically connected subcontractor as a way to channel government funds to a political leader’s close supporters.

DDTC employs Blue Lantern verification checks to assess risks in proposed defense sales, but there is no evidence that they conduct these checks for defense services in recent annual reports to Congress. These checks would help prevent PMSCs from participating in unauthorized activities.

Finally, Congress does not receive the critical information it needs to oversee US PMSC exports. DDTC sends annual reports to Congress regarding all US defense exports for that year. These reports provide Congress and the public with summary information on the types of exports DDTC has authorized. While it is possible to see the categories of weapons approved for countries, there is very little disaggregation regarding approved defense services. The report only shows a total dollar amount of authorized agreements (license manufacturing, offshore warehousing, or defense services). This may be in part why US Senator Bob Menendez (D-NJ), Chairman of the US Senate Foreign Relations Committee, proposed last year an amendment to the National Defense Authorization Act for FY2022 for the State Department to send a report on all authorizations of US persons engaged in mercenary activities abroad. This amendment was not included in the final law, but there will likely be new efforts in the NDAA for FY2023.

Table 3: Which PMSC Services Require a US Government Export License?

<table>
<thead>
<tr>
<th>Services that require a US government license</th>
<th>Services that DO NOT require a US government license</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military training, weapons maintenance and repair, how to use defense articles, support to military intelligence agencies and 10 countries such as China and Russia, and the transfer of technical data or classified information</td>
<td>Intelligence training and services for most countries, armed protection of people and property, police training, how to use semi-automatic firearms, and direct combat activities</td>
</tr>
</tbody>
</table>

suppliers, brokers, and buyers. DDTC may also send State Department officials to the purchaser’s or recipient’s address in a foreign country to verify information given in the license application. They could also check with the recipient during or after the delivery to verify compliance with US regulations and contract requirements. However, DDTC does not publish information on Blue Lantern checks for defense services in recent annual reports to Congress. These checks would help prevent PMSCs from participating in unauthorized activities.

Finally, Congress does not receive the critical information it needs to oversee US PMSC exports. DDTC sends annual reports to Congress regarding all US defense exports for that year. These reports provide Congress and the public with summary information on the types of exports DDTC has authorized. While it is possible to see the categories of weapons approved for countries, there is very little disaggregation regarding approved defense services. The report only shows a total dollar amount of authorized agreements (license manufacturing, offshore warehousing, or defense services). This may be in part why US Senator Bob Menendez (D-NJ), Chairman of the US Senate Foreign Relations Committee, proposed last year an amendment to the National Defense Authorization Act for FY2022 for the State Department to send a report on all authorizations of US persons engaged in mercenary activities aboard. This amendment was not included in the final law, but there will likely be new efforts in the NDAA for FY2023.

Which PMSC Services Require a US Government Export License?

364 Ibid, pp. 18-19, 78.
367 https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=06f22f571be4bc90bdc3866a54bcb3e
368 See this example of a State Department annual report on exports defense articles and defense services. US Department of State, Annual E55 Report, https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=06f22f571be4bc90bdc3866a54bcb3e
6.0 CONCLUSION

The US-led wars in Afghanistan and Iraq irreversibly changed the PMSC industry and the way the United States and other governments conduct foreign military operations and foreign policy. US PMSCs grew and expanded their services to meet the demands of military operations and counterterrorism efforts around the world, providing extensive support for intelligence analysis, weapons maintenance, military and police training, as well as physical security. They are now integral parts of many US operations and efforts to strengthen foreign military and police forces. Yet US PMSCs have not scaled back their global services since the US Government has downsized its operations around the world. Instead, estimated annual sales are expected to grow to more than US$80 billion in the near future. They are also providing between 80 to 90 percent of their sales to governments and entities outside of the United States and NATO allies. Many foreign PMSCs are expanding their sales and services as well. These changes have introduced significant new challenges to curbing corruption and conflict dynamics, but these challenges can be minimized if the United States reprioritizes oversight of PMSCs.

As US PMSCs seek new opportunities to maintain or gain profits, they are providing their services to countries that have weak institutional structures and processes for curbing corruption in the defense sector. A case in point is the UAE’s massive push to hire foreign PMSCs and former US military, intelligence, and law enforcement contractors to strengthen its domestic military and intelligence capabilities which presents significant risks. These include enhancing the capabilities of the Emirati government to engage in foreign conflicts and spy on dissidents, including US citizens. US companies or their foreign subsidiaries are also supporting repressive governments in Africa with surveillance techniques and physical protection of corrupt actors. The proclivity of some PMSCs to exaggerate threat perceptions or ignore conflict dynamics to win or maintain a contract – as it appears happened with TigerSwan – is another major risk and something the US Government must monitor.

The US Government, however, does not have the tools it needs to oversee US PMSCs working with foreign clients. The laws, regulations, and policies used by the State and Commerce Departments to oversee PMSCs are largely focused on controlling the export of military goods rather than services. This focus needs to be expanded to include key PMSC services. There are still large loopholes in US regulations for PMSC contracts to foreign governments or entities for combat activities, law enforcement and intelligence service training, personal or building security, and surveillance support. There are very limited efforts to ensure US PMSCs engage in corrupt actions while providing military training or weapons maintenance to foreign governments. Some US officials and industry experts argue that one can effectively control PMSCs services by controlling the export of technology. PMSCs, however, can still provide dangerous services without exporting controlled technology by using foreign technology already in the country. Focusing on the technology can also hamper US law enforcement investigators trying to establish clear violations of US export regulations.

The US Congress increasingly seeks to enhance oversight of PMSC sales to foreign governments, but these efforts need to be expanded. Congress was instrumental in pushing the Commerce Department to adopt new regulations on US sales of goods and services to military intelligence agencies in a select few countries such as China and Russia, which improved US oversight. Some congressional members also sought reports from the State Department on certain types of PMSC exports abroad, but apparent concerns about the release of proprietary information that could impact companies’ competitiveness often prevent the release of such information or reports. This challenge can be overcome by increased pressure from Congress or with new legislation. Congress must reverse the trend within the State and Commerce Departments to only provide broad summary information on exports of services, which essentially provides limited or no meaningful information on PMSC sales to foreign countries.

The US policy community has given significant attention to the risks of US PMSCs inflating costs and attacking unarmed civilians when PMSCs contract directly with the US Government. However, there is less focus on the risks of PMSCs fueling corruption in foreign countries or on side businesses conflicting with US interests.
In one case, a US PMSC encouraged local companies to engage in corrupt activities to receive US Government funds by requesting kickbacks from the local companies. In the case of TigerSwan, it partnered with an Iraqi official who reportedly moved over US$170 million outside of Iraq through an elaborate corporate mechanism that a financial services provider found “suspicious.” There are also concerns about PMSC commercial activities in countries where they are associated with the US Government. US PMSCs have also enhanced foreign military and police units’ combat skills, which can be used to repress minorities or political opposition groups. These actions too often contribute to corruption dynamics that inflame or perpetuate conflicts. They can also increase resentment towards the United States.

The US Government increasingly recognizes the critical role of corruption in fueling global instability. However, it has yet to fully develop or implement laws, regulations, and policies needed to oversee PMSCs acting on its behalf with foreign governments. US Government efforts to address key challenges emanating from PMSCs will not be fully effective unless they push for stronger foreign national laws on PMCSs. Many US PMSCs hire employees from countries all over the world, including from Africa, Asia, Europe, and Latin America. US individuals are also working for PMSCs in the UAE. However, many countries from these regions have not signed the Montreux Document nor participate in the ICoCA mechanism. These gaps can make it more difficult and riskier for US PMSCs to vet foreign nationals working for them. US persons working for non-participant countries run more risks of engaging in corrupt actions or human rights abuses. The United States can address these gaps by pushing more countries to use the ICoCA certification process and by working within the UN IGWG on PMSCs’ efforts to establish a new international framework for PMSCs.

The activities of Russian PMSCs such as the Wagner group have ignited new efforts to create an international framework for regulating PMSCs within the UN IGWG on PMSCs. Some countries (within Europe in particular) are increasingly open to such a framework, and intergovernmental dialogue about regulating PMSCs is increasingly fruitful. The United States must rejoin these UN discussions to address the challenges mentioned in the previous paragraph and to help put pressure on the actions of the Wagner Group to better comply with international legal obligations. While discussions within the UN system are still at an early stage, the United States could use this opportunity to increase support for national and international restrictions on using PMSCs that have engaged in human rights abuses and corrupt actions. This effort could also help level the playing field for US PMSCs operating in an increasingly competitive environment with foreign actors.
7.0 RECOMMENDATIONS

7.1 Building a Stronger US Government Contracting Regime for PMSCs

7.1.1 For the Executive Branch

- **Strengthen senior-level US Government oversight of PMSCs.** The restructuring and downsizing of offices and personnel within the Defense Department weakened key US oversight functions of PMSCs contracts with the Department. The Defense Department should re-appoint a senior official to oversee policy guidance, coordination within the Defense Department and other US Government agencies, and full implementation of legal and regulatory requirements regarding PMSC oversight. This official could also support efforts to strengthen international standards and foreign national laws on PMSCs. It makes the most sense to be within the Office of the Under Secretary for Defense for Acquisition and Sustainment. The State Department should also appoint or select an official within the Bureau of Management to help oversee State Department contracts with PMSCs. Agencies should assess their contract management needs – particularly as the US now transforms its role in the conflicts of the past two decades – and establish a baseline of personnel needs and indispensable roles to ensure contracts are properly managed and enforced.

- **Enhance training and guidance on corruption risks and counter measures.** While the Defense and State Departments provide materials, guidance, and training that specifically identify and address the role of and opportunities for corruption in government contracting, the State Department policy guidance lacks sufficient information to identify and mitigate corruption. The Defense Department’s policy guidance includes robust examples on the many ways contracting officers may see corruption. Contracting Officer and Contracting Officer Representative handbooks should be updated to provide a wider typology of different forms of contractor corruption as well as guidance on how to identify and address these practices. Contract oversight bodies must train their staff to recognize the detrimental effects of security sector corruption in host nations and in the domestic establishment. The State Department should also use this updated guidance in reviewing all types of government-to-government sales of PMSCs services.

- **Require reporting on beneficial ownership and subcontracting.** Extensive supply chains provide corrupt contractors with opportunities to siphon off funds through obscure subcontractors. Subcontractors can serve as fronts for bribes or self-dealing or be connected to actors working against US national security interests. Prime contractors should be required to report on all subcontracting when submitting invoices. At the very least, this should include the names of all subcontractors (including those beyond the first and second tier), their business registration and beneficial ownership status, as well as the itemized value of subcontracted services. The definition of beneficial ownership as included in the Corporate Transparency Act should be used. The prime contractors should also submit all information on all potential subcontractors when contractors are submitting their bids for new US contracts. The US Government should make this subcontractor information publicly available on the USAspending.com database, which currently only includes information on prime contractors and excludes subcontractors. Contract oversight bodies should take full advantage of the 2021 NDAA which mandates a beneficial ownership database maintained for all US-registered companies.

- **Improve coordination and database management of PMSC contracts.** The Defense and State Departments have many offices that hire and oversee PMSCs for various needs. Without coordination, this results in different approaches and mechanisms to oversee and manage PMSCs contracts with the US Government. Many of these offices maintain databases with different information and metrics. These differences make it harder for contracting officers from various offices to assess the risks of hiring potential PMSCs because they cannot see potential problems with other US offices. As such, a PMSC that could be disqualified from competing for one contract with one office could qualify for another office. The Defense and State Departments also have

---

difficulty pulling together reports on department wide use of PMSCs. US agencies should jointly assess the utility of developing interagency, interlevel databases as a means of enhancing information sharing on suspect contractors and vendors.

7.1.2 For the Legislative Branch

- **Monitor the implementation of anti-corruption measures in NDAA contracting requirements.** The 2008 NDAA mandates training and vetting requirements in private security contracting. These requirements must be updated and integrated with subsequent understandings of the national security threat posed by corruption as well as the evolving nomenclature and skillset of the PMSC field. The 2021 NDAA provides a robust new tool for combating corruption in the form of a beneficial ownership database. Congress can make the most of this critical resource by studying its use in government contracting processes. Furthermore, the 2008 NDAA requirements are specifically geared toward private security functions. The scope of these requirements must be expanded to cover the services integral to the PMSC industry, such as military training and consulting.

- **Mandate agency reporting on PMSC use.** US agencies are legally required to report on certain critical national security aspects, such as defense exports. Congress could require US government agencies – namely Defense and State Departments – to provide annual reports on the value, scope, and composition of PMSCs contracted overseas. At least one DoD geographic combat command – CENTCOM – does so through quarterly reports on PMSC contractor levels in Iraq, Syria, Afghanistan, and throughout its area of operation. Such reporting can be expanded to include the firms hired – particularly those of US origin – as well as the values of their contracts. Other combatant commands should provide similar reports, as well as the various bureaus of the State Department that hire PMSC services. Finally, USAID should provide reporting on the degree to which its funding goes to private security subcontracts.

- **Expand contract transparency.** The US Government already maintains a useful and accessible database on its contracting activities – USAspending.gov. This website is an invaluable investigative tool and means of monitoring the direct contracting history of particular firms. However, this database maintains a critical blind spot in terms of subcontracting. Congress can legislate contract reporting requirements relating to subcontracts, which could be accommodated on this public database. This would provide a critical level of visibility into how public funds are disseminated beyond the principal contract awardee and would discourage abuse. This database could also be improved by providing the initial call for proposals/invitation to bid associated with each contract.

7.2 Bolstering US Oversight of PMSCs Sales to Foreign Governments

7.2.1 For the Executive Branch

- **Expand oversight of US companies or persons engaged in combat activities abroad.** The US Government has gaping holes in its oversight of US PMSCs that contract directly with foreign governments or persons to engage in combat services. The State Department should urgently work to propose a rule change to International Traffic in Arms Regulations (ITAR), requiring US companies or persons to apply for a DDTC license if they wish to participate in combat operations abroad for a foreign person. This license requirement should include in the definition of combat activities US companies or persons services in support of strategic, tactical, and operational types of combat activities. This definition could also include intelligence gathering, logistics, and cyberwarfare activities in support of combat operations. DDTC should also add policy guidance to indicate that in most cases a license would be denied.

- **Strengthen scrutiny on subcontracting and beneficial ownership.** The DDTC requires US companies and persons to submit detailed information when applying for a defense export license. As part of the Technical Assistance Agreement (TAA), DDTC only requires foreign-owned signatories to disclose the nature of their ownership; the same should be required for US signatories. Furthermore, DDTC should stipulate that license applications include information on all potential subcontractors, their business registrations, and beneficial ownership status, as well as the itemized value of subcontracted services. Once again, the
DDTC should take full advantage of the 2021 NDAA, which mandates a beneficial ownership database maintained for all US-registered companies. The definition of beneficial ownership as included in the Corporate Transparency Act should be used.\(^{371}\)

- **Elevate Blue Lantern checks on defense services.** Over the past few years, there have been several examples in which US PMSCs provided risky sales to countries in the Persian Gulf. This includes the US company that trained the Saudi operatives who later murdered Jamal Khashoggi. DDTC should revisit its risk assessment methodology for selecting when to conduct a Blue Lantern check and determine what types of defense services should be included in these checks. This risk assessment review should factor in the likelihood that PMSCs could fuel corruption, conflict, and human rights violations. The proposed export of defense services to Saudi Arabia and the UAE should receive particular scrutiny, including the connections between the PMSC requesting a license and other PMSCs in the country to prevent supporting nefarious actors.

- **Push the US PMSC industry to adopt stronger anti-corruption and transparency measures.** Some large US PMSCs score relatively low on supply chain transparency, conflicts of interest, and oversight of agents and joint ventures, according to Transparency International’s Defence Companies Index. These low scores mean higher risks of PMSCs unknowingly working with individuals or companies who have previously engaged in corrupt or illegal actions. These companies also run the risk of the US Government being misled or defrauded. The State and Defense Department should work with the PMSC industry to strengthen company compliance systems and transparency in these areas and others to reduce corruption risks. They should also press companies to adopt an explicit policy of non-retaliation against whistleblowers in all circumstances, as well as establish accessible whistleblowing channels and regularly monitor their use, at a minimum.\(^{372}\) The United States must also continue press defense companies to provide license-by-license reports to the US Government on political contributions, commissions, and lobbying of foreign clients.

### 7.2.2 For the Legislative Branch:

- **Expand export license requirements for armed security and intelligence service exports (outside of direct support to combat operations).** Given the risks to US national security from companies providing armed security and intelligence services abroad, Congress should explore ways in which the State and Commerce Departments could strengthen oversight of US PMSCs contracts with foreign governments and entities with weak anti-corruption standards and practices. Current Commerce Department regulations do not require US companies or individuals to apply for a license to actively engage in types of surveillance and counter surveillance for foreign intelligence agencies in most countries. Congress should also consider expanding oversight of US companies that provide protective services to foreign politicians or elites accused of corruption, particularly in fragile or conflict-ridden countries.

- **Enhance reporting on exports of PMSC services.** DDTC publishes annual reports to Congress on authorized exports of defense articles and services as well as Blue Lantern verification checks. These reports, often referred to as the 655 reports, provide critical insights into the scope and impact of the US arms trade. Yet the information on defense services is severely limited by over-summarization through aggregating distinct categories together, such as combining data on sales of license, manufacturing offshore warehousing, and defense services into one amount for each country. This aggregation prevents Congress and the public from performing any type of oversight of PMSC services. Critically, it is nearly impossible to monitor the types of defense services exported to specific countries. Congress has also struggled getting basic information on specific types of defense services sales abroad. Several years ago, DDTC provided more detailed reports on exports of defense services. DDTC should expand on these previous reports and list the specific types of defense services by country.

---


• **Pass the Civilian Extraterritorial Jurisdiction Act and Mandate Reporting on Enforcement of the War Crimes Act.** The US relies on MEJA to hold PMSCs and other contractors assigned to support US military operations accountable. However, no comparable law exists outside of military operations, meaning that PMSCs working for the US Government in other contexts operate in a gray area of accountability. Additionally, the investigation of alleged war crimes by US contractors has historically not been prosecuted under the War Crimes Act even though that statute provides jurisdiction over such crimes no matter where they occur. Congress should revive and reassess the Civilian Extraterritorial Jurisdiction Act so that PMSCs operating outside of US military operations are held to a similar degree of accountability.

• **US persons comply with ICoC standards.** Congress should legislate that any US PMSC must comply with ICoC standards at all times, regardless of whether the PMSC is contracting with the US Government or any other entity. Congress should further legislate that any US citizen or permanent legal resident can only be employed by PMSCs that are in full compliance with ICoC standards. Anyone employed, subcontracted to, an agent of, or otherwise conducting PMSC activity with firms which do not meet these standards should be considered to be engaged in mercenary activity.

### 7.3 Creating Stronger International Controls on PMSCs

• **Share intelligence information on PMSCs engaged in illicit activities.** The activities of the Wagner Group in many countries in Africa and other parts of the world are increasingly alarming. The United States should consider working bilaterally or in small groups with countries that share these concerns to identify ways to help stem their egregious human rights abuses and corrupt activities. There may be other equally concerning PMSCs engaged in similar behavior. This effort could also encourage more countries to adopt targeted sanctions and restrictions on those individuals that are financing and supporting bad actors. The United States should also consider expanding the number and seniority of US embassy staff in key US partner countries in Africa.

• **Encourage more countries to fully implement the International Code of Conduct for PMSCs.** The International Code of Conduct offers strong standards for regulating PMSCs. As a strong supporter of the ICoCA, the United States is in a good position to encourage other US security partner countries that are increasingly using PMSCs – such as the UAE, India, Israel, and Egypt – to agree to and adopt these standards as a means to expand controls over PMSCs in these countries and increase funding for ICoCA. At the same time, the United States should explore ways to encourage more US companies to join ICoCA by requiring US PMSCs seeking a contract with the Defense Department to be an ICoCA member. There is also a critical need to increase funding for ICoCA’s efforts to monitor potential problems with ICoCA membership companies and support strong company whistleblower protections.

• **Rejoin the UN Intergovernmental Working Group on PMSCs discussion on establishing an international framework on PMSCs.** The Working Group’s renewed efforts to establish an international framework on PMSCs provides the United States with another key opportunity to push foreign countries to establish stronger national controls on PMSCs. The United States can raise some of the concerns they have about the actions of foreign PMSCs, by calling for clear restrictions on states hiring PMSCs with a record of engaging in corrupt activities or human rights abuses. Critically, the United States should encourage the Working Group to incorporate a broader definition of PMSCs to include intelligence and cybersecurity activities. The United States could also use this opportunity to talk about some of the ways the PMSC industry has grown and diversified and the challenges the US Government has faced in regulating US PMSCs.