Atlantic Council
GLOBAL ENERGY CENTER

大成 DENTONS

Key Risks Companies Face in Petroleum Investment and Operations

Bud Coote and Karl V. Hopkins

Key Risks Companies Face in Petroleum Investment and Operations

Bud Coote and Karl V. Hopkins

ISBN: 978-1-61977-442-1

Cover photo: Reuters/Ako Rasheed. The Bai Hassan oil facility inside Kurdish-controlled areas in northern Iraq after an attack by militants in July 2016.

January 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report is a collaboration between Dentons and the Atlantic Council that provides analysis on the array of risks and uncertainties faced by international energy firms investing in and operating energy projects worldwide. It focuses on lessons learned from a variety of experiences and offers risk mitigation options.

Risk and uncertainty pervade decisions on petroleum investments and operations, raising the stakes for companies committing to multibillion dollar contracts often extending twenty or more years. The array of risk factors is diverse, requiring multidisciplinary analysis to decipher. New risks arise and others expand, raising the breadth and depth of challenges facing energy operators. "The risk model has changed. It used to be that the risk of physically getting hydrocarbons out of the ground profitably was the principal driver. But now it requires understanding, analyzing, and balancing a host of integrated issues and addressing them with a holistic approach that involves everyone from board members through laborers, contractors, and subcontractors."[1]

To share these risks, there are trends toward the consolidation of major international oil companies into supermajors, growth in state-owned companies including national oil companies, and greater collaboration on major projects worldwide including joint projects between international oil companies and national oil companies. "There is no silver bullet approach to risk. Every country presents a different environment with different challenges. And companies will have different appetites for risk and different experiences and resources to manage them."[2]

Uncertainty fuels market volatility and vice versa. The energy industry is prone to cycles as major investments ebb and flow with price changes, concerns about future demand growth, new environmental regulations, and risks of government-imposed sanctions, which can accentuate market swings before the markets can self-correct. As investors increasingly look toward developing economies for resources, they face questions about the rule of law and sanctity of contract in countries with unproven track records. Lessons from past expropriations, revolutions, and expulsions of companies in Mexico, Iran, Libya, and Venezuela still reverberate.

"Resource nationalism" also continues in the form of increased government shares of oil profits and expanded local content requirements for host country equipment and services companies. In the case of many developing economies, oil wealth has proved difficult to manage, and the revenues become a source of power for authoritarian rulers, corruption, and instability. These ingredients are commonly associated with failed states or failing states, which do not represent sound investments.

Some of the relatively new risk factors companies face include terrorism, cyberattacks, and reputational risks caused, for example, by political criticism from nongovernmental organizations (NGOs) and other private sources. A major cyberattack on western Ukraine's power grid in December 2015 provided a vivid view of the widespread damage cyber warfare can inflict.

Infrastructure and personnel attacks are long-enduring risks with additional threats from terrorists and cyber warfare. A Central Intelligence Agency (CIA) report on infrastructure vulnerability issues during the Iran-Iraq war and a Statoil report on its investigation of the terrorist attack on the In Amenas gas processing facility in Algeria showed the dangerous threats militants pose to infrastructure and personnel security.

Climate change concerns and related policy adjustments could alter the calculus for hydrocarbon investment and development, although such risks are likely to be gradual. Populism also adds to political risk and uncertainty and can have dramatic impacts on the investment decisions and finances of energy companies.

1 Karl V. Hopkins, partner and global chief security officer, Dentons, from an Atlantic Council Global Energy Center conference with Dentons' security experts, November 28, 2016.

2 Arkadiusz Krasnodębski, Head of the Energy and Natural Resources practice team in Poland and Europe, Dentons, from an Atlantic Council Global Energy Center conference with Dentons' security experts, November 28, 2016.

INTRODUCTION

This report will examine key risk factors that influence energy investment and operations worldwide and identify possible ways to mitigate risks and reduce uncertainty. Their impact has risen in importance in recent years as energy companies have invested in more developing countries, violence has grown more widespread, environmental and human rights issues have generated political criticism of companies, and oil prices have fallen.

The report will look at eight categories of risk: rule of law, sanctity of contract, infrastructure risk, personnel security, political criticism and reputational risks, financial risks, corruption, and cyberattacks. Climate change-related risk is addressed primarily as a financial risk, and the risk posed by populist movements in petroleum-producing countries is treated separately as a risk that cuts across many of the eight categories of risk listed above. This organization allows us to drill more deeply into the key risks. In fact, they are all interrelated and need to be appreciated and treated as such in any effective risk management program.

Various case studies including the examination of the February 24, 2006, terrorist attack on Abqaiq in Saudi Arabia; the January 16, 2013, terrorist attack on In Amenas in Algeria; the security approach to the Baku-Tbilisi-Ceyhan pipeline constructed between April 2003 and June 2006; pipeline disruptions in Nigeria; the Iran-Iraq war from September 1980 to August 1988; the first Persian Gulf war with Iraq that began in August 1990; and the conflict in Iraq beginning in March 2003 will be examined for lessons.

RULE OF LAW

Adherence to rule of law is critical to support confidence and investments in long-term, high capital-cost projects in the petroleum industry, but it is undermined by poor governance. Risks are often most significant in developing countries with a high dependence on oil and gas revenues, weak public institutions, and a poor record in enforcing the rule of law. A country's high dependence on oil and gas revenues provides a stronger incentive for governments to try to improve its share of revenues through changes in the law or by means of fines. This effort can also include government insistence on a greater role for a national company in a project or a greater share of equipment and services contracts awarded to local firms.

Possible mitigation options include embedding contract terms in national legislation, negotiating the application of the laws from a non-host country, including the right of arbitration in order to resolve disputes and adjudication rights as appropriate for other circumstances, in addition to specific consequences for failure to adhere to the rule of law. In Azerbaijan, for example, petroleum exploration and development contracts with foreign companies signed in the 1990s, after the breakup of the Soviet Union, were made part of Azerbaijani law by combining government guarantees with parliamentary ratification.[3] In 2012, stakeholders in the Trans-Anatolian Pipeline (TANAP) agreed that their relationship would be based on Swiss law rather than Turkish law.[4]

"Arbitration rights offer an added degree of protection to companies, but this also can be undermined when dealing with a government that does not enforce the outcome. An important means of strengthening the role of arbitration is to have a government-to-government investment treaty in place or negotiated before investing."[5]

Another tactic to protect against political risk is to partner with other foreign firms in expensive projects, especially firms from third countries. This can increase the diplomatic pressure that would be brought to bear on the host country for cases in which the government is violating the rule of law; it also spreads the risks of financial losses or host government encroachment on control of operations.

One of the largest political risks is that of nationalization. A predetermined compensation formula for nationalization is one possibility to deter or soften the blow of a nationalization.

3 Ilham Aliyev, "Azerbaijan. The New Source of Energy of the 21st Century," Occasional Paper, Caspian Studies Program, Belfer Center, February 1998, http://belfercenter.ksg.harvard.edu/publication/3041/azerbaijan.html.

4 "Azerbaijan and Turkey Sign TANAP Agreements," Argus Media, June 27, 2012, http://www.argusmedia.com/news/article/?id=803669.

5 Karl V. Hopkins, Atlantic Council Global Energy Center conference with Dentons' security experts, November 28, 2016.

The World Justice Project ranks 102 countries according to criteria measuring the degree to which the rule of law is upheld. The project uses nine categories to measure indexes for major aspects of rule of law, including constraints on government powers, corruption, openness of government, fundamental rights, order and security, regulatory enforcement, civil justice, criminal justice, and informal justice. Each of these major factors is broken down into sub-factors.[6]

Not surprisingly, high-income countries dominate the rankings for the highest indexes for adherence to the rule of law. Lower income countries tend to dominate the lower rankings, with the exception of Russia, which is considered a high-income country but ranks seventy-fifth out of 102 countries in adherence to rule of law. Oil and gas producers are distributed throughout the list, with Nigeria and Venezuela standing out as the lowest ranked significant petroleum producers.[7]

6 World Justice Project, "Rule of Law Index 2015," 2015, http://worldjusticeproject.org/sites/default/files/roli_2015_0.pdf.

7 Ibid.

Table 1. Country Rankings for Adherence to Rule of Law

Country	Score	Country	Score	Country	Score
Denmark	0.87	Hungary	0.58	Lebanon	0.48
Norway	0.87	Ghana	0.6	Moldova	0.48
Sweden	0.85	Croatia	0.6	Ukraine	0.48
Finland	0.85	South Africa	0.58	China	0.48
Netherlands	0.83	Hungary	0.58	Tanzania	0.47
New Zealand	0.83	Senegal	0.57	Zambia	0.47
Austria	0.82	Malaysia	0.57	Kyrgyzstan	0.47
Germany	0.81	Bosnia and Herzegovina	0.57	Russia	0.47
Singapore	0.81	Jordan	0.56	Ivory Coast	0.47
Australia	0.8	Jamaica	0.56	Ecuador	0.47
Republic of Korea	0.79	Tunisia	0.56	Burkino Faso	0.47
United Kingdom	0.78	Macedonia FYR	0.55	Mexico	0.47
Japan	0.78	Bulgaria	0.55	Turkey	0.46
Canada	0.78	Brazil	0.54	Madagascar	0.45
Estonia	0.77	Mongolia	0.53	Liberia	0.45
Belgium	0.77	Nepal	0.53	Kenya	0.45
Hong Kong, China	0.76	Panama	0.53	Guatemala	0.44
France	0.74	Belarus	0.53	Egypt	0.44
United States	0.73	Philippines	0.53	Sierra Leone	0.44
Czech Republic	0.72	Indonesia	0.52	Iran	0.43
Poland	0.71	Albania	0.52	Nicaragua	0.43
Uruguay	0.71	Argentina	0.52	Honduras	0.42
Portugal	0.7	Morocco	0.52	Ethiopia	0.42
Spain	0.68	Thailand	0.52	Myanmar	0.42
Costa Rica	0.68	El Salvador	0.51	Bangladesh	0.42
Chile	0.68	Sri Lanka	0.51	Bolivia	0.41
United Arab Emirates	0.67	India	0.51	Uganda	0.41
Slovenia	0.66	Serbia	0.5	Nigeria	0.41
Georgia	0.65	Malawi	0.5	Cameroon	0.4
Italy	0.64	Colombia	0.5	Pakistan	0.38
Botswana	0.64	Uzbekistan	0.46	Cambodia	0.37
Romania	0.62	Peru	0.5	Zimbabwe	0.37
Greece	0.6	Vietnam	0.5	Afghanistan	0.35
Ghana	0.6	Kazakhstan	0.5	Venezuela	0.32
Croatia	0.6	Belize	0.49	*Source*: World Justice Project, "Rule of Law Index 2015," http://worldjusticeproject.org/sites/default/files/roli_2015_0.pdf.	
South Africa	0.58	Dominican Republic	0.48		

SANCTITY OF CONTRACTS

Along with rule of law, sanctity of contract is a key concern and risk for petroleum investments involving long-term contracts with high capital costs. While "rule of law" applies to a government's adherence to and enforcement of all the laws within a country and the consistency and fairness of such laws, "sanctity of contract" applies more specifically to a company's contract with a host government or its representative, which may be a national oil company, as well as all of the contracts a company makes with other participants in a project, such as equipment and service companies and labor groups. As such, sanctity of contract concerns are an important factor in decisions about investing in countries without an extensive track record in protecting contracts. This is ameliorated by the practice of some national legislatures to incorporate major contracts into the laws of the country.

Similar to rule of law, sanctity of contract is most likely to come under pressure when circumstances change to provide a windfall of revenues to oil companies or lower revenues to the government, or if political pressures on private firms are created by a change in government or other political force. The increase in oil prices from the beginning of the century to 2014 helped fuel a rise in "resource nationalism" that gave many governments the incentive and confidence to change contract terms in favor of the government. Venezuela provides an especially strong example of such behavior.[8]

In a lower price environment, investors normally have better leverage to insist on more favorable contract terms. But because contracts frequently extend through multiple market cycles, companies tend to lose such leverage before contracts expire. Anticipating the number and range of uncertainties that may arise during the length of a contract is also difficult.

As with rule of law, the best protection against changes in contracts is to deal with countries and governments that have good long-term track records, which is rarely the case when dealing with low-income, developing economies. One common method investors have used to hedge the risk of contract change and lock in the terms of a contract is to insert "stabilization" clauses intended to anticipate changes in external considerations that generate pressures for contract change. These external changes often relate to changes in oil prices or production, changes in government spending needs, changes in government or legislation, attempts by government to stay in power by boosting spending, and shifts in the perception of a fair split in revenues between the government and investors.[9]

A recent report by The Oxford Institute for Energy Studies that looked at nineteen developing economies plus Mexico found mixed success in the use of stabilization clauses. Historically, stabilization clauses that try to freeze the terms of a contract throughout its life tend not to work very well because governments change, and new governments are less likely to honor commitments made by preceding ones, especially if the fairness of the terms becomes an issue. In addition, legislatures are even less likely than executive institutions to consider themselves bound by commitments made by previous governments.[10]

Stabilization clauses that more flexibly address fairness issues and try to maintain equitable shares of revenue among governments and other stakeholders tend to work better than clauses that try to freeze contract terms, according to some analyses. Such clauses would help provide stability by providing mechanisms allowing adjustments to external factors, such as changing oil prices, which cause an imbalance in the economic benefits envisioned in the original contract.[11] A clause stipulating that no changes will be made in the contract without the consent of both sides is one example of a stabilization clause that allows both parties to guard against unilateral moves that can cause disruption to major projects. A provision that calls for mediation to resolve all contract disputes also reduces the chances for disruption. A dispute could arise, for example, if a project fails to meets projected production rates on schedule leading to lower

8 For examples of projects and property seized by Venezuela under President Hugo Chavaz from foreign energy companies, see Reuters, "Factbox: Venezuela's Nationalizations Under Chavez," October 7, 2012, http://www.reuters.com/article/us-venezuela-election-nationalizations-idUSBRE89701X20121008.

9 Peter Cameron, "Stabilization in Investment Contracts and Changes of Rules in Host Countries: Tools for Oil and Gas Investors, Association of International Petroleum Investors," Rocky Mountain Mineral Law Foundation, July 5, 2006, http://www.rmmlf.org/Istanbul/4-Stabilisation-Paper.pdf.

10 Mario Mansour and Carole Nakhle, "Fiscal Stabilization in Oil and Gas Contracts: Evidence and Implications," The Oxford Institute for Energy Studies, January 2016, https://www.oxfordenergy.org/wpcms/wp-content/uploads/2016/01/Fiscal-Stabilization-in-Oil-and-Gas-Contracts-SP-37.pdf. The twenty countries studied in this report are Angola, Azerbaijan, Chad, Egypt, Equatorial Guinea, Ghana, Ivory Coast, Kazakhstan, Kenya, Kurdistan, Liberia, Mauritania, Mexico, Mozambique, Papua New Guinea, Sierra Leone, Tanzania, Trinidad and Tobago, and Uganda.

11 Ibid.

revenues, or over whether a project has recouped all of its initial capital costs, which would trigger a higher percentage of revenues owed to the government.

More specific clauses might focus on fiscal stability by setting a fixed schedule of taxes and royalties and having the government share in the project's risks. According to the Oxford Institute, one of the more effective stabilization clauses, and one that is often overlooked, addresses a host government's wish to receive a larger share of a project's oil or gas production rather than to receive taxes in cash. In such circumstances, a clause might be adapted to stipulate that the host government or its national oil company is entitled to the additional oil as long as the government or the national oil company assumes the burden of any additional financial obligations, including taxes imposed on the investor beyond the level agreed to in the original contract. This provides fiscal stability for the investor as well as leeway for the government to take a larger share of production.[12]

12 Ibid.

An arbitration option in a contract is another example of a stabilization clause. International arbitration of contract disputes can help mitigate risk and uncertainty, especially if contracts involve the national government as well as any national oil companies. A clause that stipulates a right to arbitration can provide the added benefit of helping to persuade both parties to address a contentious issue without recourse to arbitration.[13] "As with the rule of law, not every government will abide by the outcome of arbitration, even with the added weight of an investment treaty. This underscores the need for thorough due diligence before investing in countries, which can help avoid encounters with some governments who do not care to uphold contractual obligations. It also calls for detailed accounting following investments."[14]

13 Peter Cameron, "Stabilization in Investment Contracts and Changes of Rules in Host Countries: Tools for Oil and Gas Investors, Association of International Petroleum Investors, July 5, 2006, http://www.rmmlf.org/Istanbul/4-Stabilisation-Paper.pdf.

14 Karl V. Hopkins, Atlantic Council Global Energy Center conference with Dentons' security experts, November 28, 2016.

INFRASTRUCTURE RISK

Risks to critical energy infrastructure are a large concern to investors, governments, suppliers, operators, consumers, workers, and security and military personnel among others. Damages can have widespread consequences for the economy as well as the health, safety, security, and psychological well-being of large portions of a population. Past attacks such as the February 2006 terrorist attack on Abqaiq in Saudi Arabia, the January 2013 terrorist attack on In Amenas in Algeria, pipeline disruptions in Nigeria, the Iran-Iraq war from September 1980 to August 1988, the Iraqi invasion of Kuwait in August 1990, and the conflict in Iraq beginning in March 2003 all provide examples of real and potential risks to infrastructure, as do natural events such as hurricanes and earthquakes.

Addressing and mitigating physical risks to infrastructure requires a complex assessment of numerous factors, options, and possible outcomes as well as integration of implications for an array of related risks such as personnel security and cyberattacks. Critical facilities will also need to be defined by the likely length of disruptions of oil and gas volumes as well as by the size of disruptions, which will require consideration of various scenarios for levels of threat. "An overarching theme is that infrastructure risk needs to be approached as a global and multidisciplinary challenge that is better conceptualized and addressed as an issue of resiliency than security."[15]

An analysis of infrastructure risks should begin with assessments of vulnerabilities, threats, and protection options by knowledgeable professionals. These assessments will need to include options to mitigate damage through jerry-rigging and bypass options for various damage scenarios to create a full understanding of the overall resilience of a petroleum system.

Because not every incident can be protected against or avoided, especially in the case of pipelines, coordinated response plans and capabilities will need to be developed, including identification of and quick access to response and repair equipment and personnel. This will involve the detailed definition of responsibilities for all components involved in detection and response to incidents, including operators, security personnel, and any contractors and other entities involved in

15 Karl V. Hopkins, Ibid.

response operations. Critically, host governments must be aware of and embrace their responsibilities, which importantly include reestablishing security for needed repairs in areas that are attacked. Companies should negotiate responsibilities and liabilities with host governments and ensure that they are spelled out in a host government agreement.

A quick response to infrastructure damage caused by a physical attack underscores one of the key lessons of infrastructure security—the value of a facility or system's operation is often much greater than the value of the facility. Hence, minimizing the downtime becomes the most critical commercial objective. A good example is a pipeline system such as the Baku-Tbilisi-Ceyhan (BTC) oil pipeline from Azerbaijan through Georgia to the Turkish Mediterranean tanker terminal at Ceyhan, a distance of 1,768 kilometers. The entire pipeline took about seven years to plan, design, engineer, and construct at a cost of about $4 billion, including financing. But the value of the oil flowing through the system overwhelms the cost of the pipeline and its associated facilities. At a price of $45 per barrel for crude oil and a flow rate of about 130 million barrels in the first half of 2016, about $4 billion of crude oil passes through the BTC pipeline every four months.[16]

The BTC pipeline also provides a good example of another lesson, which is that protective measures for infrastructure are usually cheaper, and sometimes much cheaper, if incorporated at the time of construction. The pipeline was buried one-to-two meters deep its entire length, even under riverbeds and ravines. In some cases, horizontal holes were drilled under the rivers for the pipe. Sensors and other protective devices were added underground. In addition, the route of the pipeline in Georgia was carefully chosen to locate it in areas where the Georgians could logistically respond more quickly to security incidents. This added about 100 kilometers to the route and cost stakeholders about an extra $100 million.[17]

For protection of critical infrastructure, the principle of multiple layers of security has generally proved more effective than alternative approaches and needs to be observed. In the case of a pipeline system, other main components may include terminals, storage areas, pump stations, pressure-reduction stations, and above-ground block valve stations. The multiple layers would include a guard force inside the perimeter of each surface facility, a dedicated force to monitor and patrol the outside of the perimeter of facilities and the length of the pipeline, and bases of operations for regional forces that could be called upon to respond quickly to security incidents. If necessary, the country's military forces and resources could be called upon if regional forces cannot restore security.

As shown in Iran during the Iran-Iraq war, an additional level of protection can be achieved by dispersing or burying critical equipment, and operations can be maintained by jerry-rigging or bypassing damaged equipment or by other innovative measures such as the tanker shuttle Iran established to ferry oil from Kharg Island to a transshipment point outside the Persian Gulf.[18] Iran also benefitted from the large surplus capacity in its oil export system due to the significant drop in exports after the Iranian Revolution in 1979. As a result, Iran's oil exports remained resilient throughout the war.

Iraq's oil exports were more seriously reduced by the loss of its major Persian Gulf oil terminals, damaged early in the war, and the loss of use of its pipeline to Syria's Mediterranean coast when Syria backed Iran in the conflict in 1982. Iraq's oilfield facilities also suffered some damage during the war. However, Baghdad was able to increase the capacity of its export pipeline from northern Iraq to Turkey's Mediterranean port at Ceyhan to more than 700,000 barrels per day (b/d), establish a new pipeline link to Saudi Arabia's pipeline to the Red Sea, and manage to transport about 70,000 b/d of oil to Jordan using tanker trucks.[19] Over the course of the eight-year Iran-Iraq war, both participants were able to find ways to get oil to market despite the fighting; global oil prices actually declined dramatically during this period.

Even without a war, the advantages of hardening facilities and maintaining redundancy and surplus capacity are evident, often for both financial and security purposes. Having multiple export options can lower costs by creating competition and serve to avoid disruptions to exports when some routes are not

16 BP website, "Baku-Tbilisi-Ceyhan Pipeline," http://www.bp.com/en_az/caspian/operationsprojects/pipelines/BTC.html.

17 S. Frederick Starr and Svante E. Cornell (eds), "The Baku-Tbilisi-Ceyhan Pipeline: Oil Window to the West," Central Asia-Caucasus Institute Silk Road Studies Program, 2005, http://www.silkroadstudies.org/resources/pdf/Monographs/2005_01_MONO_Starr-Cornell_BTC-Pipeline.pdf.

18 Rob Johnson, *The Iran-Iraq War* (New York: Palgrave-Macmillan, 2011), 164-165, https://books.google.com/books?id=0yYdBQAAQBAJ&pg=PA164&lpg=PA164&dq=iran+tanker+shuttle&source=bl&ots=s0H2phliW1&sig=HAQDidFfJQ7atDpPoUPOsvy-Q84&hl=en&sa=X&ved=0ahUKEwituLzMxbTOAhXC2B4KHV_HAYYQ6AEIPzAI#v=onepage&q=iran%20tanker%20shuttle&f=false,

19 Helen Chapin Metz (ed), "Iraq: A Country Study," Library of Congress, Federal Research Division, May 1988, https://cdn.loc.gov/master/frd/frdcstdy/ir/iraqcountrystudy00metz_0/iraqcountrystudy00metz_0.pdf.

Iranian military personnel participate in war games in southern Iran near the Strait of Hormuz. About seventeen million barrels of oil transits the Strait of Hormuz daily, making it the world's most important oil transportation chokepoint. *Photo credit:* Reuters.

available. Even within individual routes, redundancy in critical equipment such as pumps, drivers, compressors, and generators can keep systems operating at capacity when some equipment malfunctions or is down for maintenance. In some cases, maintaining a stockpile of critical spare parts and critical equipment is cost-effective, because it can greatly limit the downtime of operating systems such as pipelines. This is especially important for equipment that is custom designed and has a long manufacturing lead time. In addition to spare replacement parts and critical equipment, ready access to construction equipment and transportation options is also needed to respond to serious damage and disruption scenarios. For situations calling for rapid and large-scale responses, equipment availability and transportation options will need to be planned and coordinated in advance.

One of the lessons learned from past attacks on infrastructure is that damages to equipment and facilities can be vastly increased by the amount of time an attacker stays on the target site. That is, the longer an attacking force controls and occupies a petroleum facility, the more damage it can inflict and the more time, expense, and effort will be needed to restore or rebuild the facility. This is illustrated by the Iranian commando raid on Iraq's Mina al-Bakr tanker-loading sea island terminal on the Persian Gulf during the Iran-Iraq war. On November 7, 1980, Iran landed commandos on the Mina al-Bakr sea island and at al-Faw.[20] According to a CIA declassified intelligence assessment, two years would be needed to completely repair and restore operations at Iraq's sea islands. Baghdad accepted a US firm's proposal to build makeshift facilities to support loading tankers from single point mooring buoys, which could restore partial capacity more quickly.[21] The sea island terminals remained unrepaired and unusable through

20 *Global Security,* "Iran-Iraq War (1980-1988)," August 11, 2016, http://www.globalsecurity.org/military/world/war/iran-iraq.htm.

21 Central Intelligence Agency, "The Iran-Iraq War: Some Vulnerability Issues," 1982 (declassified April 2002), https://www.cia.gov/library/readingroom/docs/DOC_0000764182.pdf.

the remainder of the war, however, because security conditions did not allow restoration.

In contrast with Iran's commando raid on Iraq's Persian Gulf oil export facilities, air attacks by both Iran and Iraq were less effective in disrupting oil exports. Despite repeated attempts by Iraq to damage Iran's major tanker loading facility at Kharg Island, the onshore Gurreh pump station complex that supplies oil to Kharg Island, and other oil facilities, the damage inflicted by Iraq never posed much more than a short-term inconvenience to Iran's oil export operations, according to a 1982 CIA assessment. This failure to seriously disrupt Iranian oil exports continued throughout the rest of the war. Iraq's biggest success against Iran's oil sector was the destruction of the Abadan oil refinery, which is Iran's largest refinery and located near the Iran-Iraq border, but this was done early in the war using ground artillery barrages. Iran's air attacks against Iraq's Persian Gulf export facilities were also ineffective leading up to the commando attack, but as of late July 1982, Iran had knocked out three of fourteen units at a large processing complex in the Kirkuk oilfield in northern Iraq, according to the CIA report.[22] This reduced Iraq's oil production capacity, but there is no indication that it further reduced Iraq's already constrained export capacity.

An important implication of the increased damage that longer occupation of a facility allows attackers to inflict on oil equipment and facilities is the magnified importance it underscores for a rapid response. A rapid response can dramatically affect the cost-benefit analysis for decisions on the value of investing in equipment and other assets needed to respond to an attack. It also underscores the needs for detection equipment and alert systems that can shorten response times, and especially amplifies the importance of preplanned communications and coordination involving a host government and appropriate security and military forces for a successful response.

Another key factor determining the extent of damage an attack on a petroleum facility can inflict is whether the facility is operating or not. It is easy to imagine how this principle would apply to offshore oil and gas drilling rigs and production platforms, gas-oil separation and stabilization plants, pipeline systems, tanker loading facilities, refineries, and other processing facilities. A recent example is the terrorist attack on the In Amenas gas facility in Algeria on January 16, 2013. As the investigation report prepared for Statoil's board of directors indicates, the loss of forty lives of employees was horrific and overwhelms other considerations. The terrorists' ire at finding the plant shut down, their efforts to force hostages to turn the power back on, and the heroic resistance of the hostages all point to the terrorists' frustration that they were denied the devastation to the facility that they apparently intended.[23]

Dealing with an event the scale of the In Amenas attack is difficult, as the Statoil report makes clear. The post-event recommendations made by Statoil are all appropriate and are summarized by Statoil as follows:[24]

- **Security at In Amenas:** Improve the joint venture's ability to detect, delay and stop potential attacks by reinforcing electronic and physical protective measures, enhancing its security risk management capability and developing a coherent programme of security training and exercising.
- **Organization and capabilities:** Develop a clearly defined ambition for the company's security capability. Strengthen the total security organization. Ensure an holistic approach to security.
- **Risk management systems:** Develop a security risk management system that is dynamic, fit-for-purpose and geared towards action.
- **Emergency preparedness and response:** Coordinate and standardise emergency response planning consistent with the principles of the Incident command system ("ICS").
- **Collaboration and networks:** Broaden and deepen cooperation with relevant government agencies and organisations. Reinforce networks and institutional relationships. Establish standards for security management and engagement in joint ventures and partnerships.

The report makes clear that the main security failure was the ineffectiveness of the Algerian government, army, and gendarmes in protecting the outer security of the In Amenas facility. The army presence outside the facility was in fact a large one, responsible for security in the outer desert surrounding the facility. The gendarmes were responsible for securing the desert zone immediately around the facility. The army and gendarmes' assignments were to deter, detect, and stop attackers. The large army presence may

22 Ibid.

23 Statoil, "The In Amenas Attack," February 2013, http://www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf.

24 Ibid.

Saudi Arabia's Abqaiq is the main processing center for Arabian Extra Light and Arabian Light crude oils, with a capacity of more than seven million barrels per day. It has three main processing operations: oil, natural gas liquids, and utilities. *Photo credit:* Google Earth.

have contributed to a sense of complacency that its presence alone would be sufficient to deter an attack. While concern was rightly directed to the safety of employees after the attack, some key actions helped to limit damage to the facility and also probably saved lives. One crucial move was that the system automatically shut down power at the plant when a bullet hit a transformer early in the attack. Another was the quickness of the military attack against the terrorists, which took place on January 17. Numerous undetonated explosive devices were found in the facility after the military attack.

An important lesson from both the terrorist attack on In Amenas in January 16, 2013, and the attack on the Abqaiq processing facility and pump station in Saudi Arabia on February 24, 2006, is the critical need to carefully vet employees, contractors, and other personnel with access to critical facilities because of the added risk and damage potential posed by insider assistance or participation in an attack. In the case of the In Amenas attack, the attackers appeared to have knowledge from insiders about the entry points to the facilities and perhaps assistance in gaining entry to the main processing and residential areas. In the attack on Abqaiq, three vehicles were painted to appear to be state-owned Aramco vehicles. One car appeared to conduct reconnaissance while other militants breached the gates of the plant initially approaching a side gate to the outer perimeter rather than the main gate. The extent of damages might have been more severe if the attackers had insider knowledge about operational aspects of these facilities.[25]

The In Amenas attack further showed the importance of establishing good relations with the local population, including "buy in" from local residents

25 Ibid; Reuters, "Saudi Security Forces Kill 'Terrorist' in Abqaiq," September 4, 2015, http://www.reuters.com/article/saudi-security-idUSL5N11A15I20150904; CNN, "Saudi Shootout Kills '5 Militants'," February 26, 2006, http://edition.cnn.com/2006/WORLD/meast/02/27/saudi.shooting/.

on the economic and other benefits from having an industrial facility located nearby. Statoil and its partners engaged with the local community and contributed to its welfare directly as well as providing employment. Algerian workers at the plant generally showed exceptional loyalty during the terrorist attack, but the attack itself strongly suggested that attackers had the benefit of some local knowledge. In cases such as the Baku-Tbilisi-Ceyhan oil pipeline built by BP, gaining the buy in from the local population is especially important because of the length of pipeline that needs to be protected. BP invested heavily in the communities along the pipeline's path, which is probably one reason for the pipeline's success and the heavy ongoing investment in gas pipeline capacity in the same corridor.[26]

26 Statoil, "The In Amenas Attack"; Jonathan Elkind, "Economic Implications of the Baku-Tbilisi-Ceyhan Oil Pipeline," in S. Frederick Starr and Svante E. Cornell (eds), *The Baku-Tbilisi-Ceyhan Pipeline: Oil Window to the West*, Central Asia-Caucasus Institute, Silk Road Studies Program, 2005, http://www.silkroadstudies.orgresources/pdf/Monographs/2005_01_MONO_Starr-Cornell_BTC-Pipeline.pdf.

The war and subsequent civil strife in Iraq that began in March 2003 and ongoing problems in Nigeria underscore the importance of energy companies having a capable and responsible partner in the host government to help provide security for energy infrastructure. Without a government and military capability to control areas containing damaged facilities, those facilities often cannot be repaired. Even with such a capability, considerable cooperation and communications are required among all the parties to plan and execute those repairs.

Infrastructure damages from hurricanes and other weather-related events are also an important concern to companies, and predictions that climate change will lead to more volatility and a rise in sea levels raise further uncertainty about these risks.

Energy infrastructure security is a critical and enduring concern for global energy security as well as for investors and operators, as reflected in a CIA intelligence assessment on "The Iran-Iraq War: Some Oil Vulnerability Issues." Parts of this report were recently declassified (see text box below).

Extracts of CIA analysis of vulnerabilities of Middle East petroleum systems from a 1982 report declassified in April 2002.

The Iran-Iraq War: Some Vulnerability Issues

Iran-Iraq Facility Vulnerability

The petroleum production and export systems in both countries are vulnerable at a number of choke points. Many of these choke points—export terminals, storage facilities, pump stations, and crude processing facilities—have been subject to sporadic attacks since the war began in late September 1980. Iraq has suffered extensive damage, particularly to its Persian Gulf offshore export terminals. In contrast, damage to key choke points in Iran's petroleum system before the current offensive has been minimal.

Iraqi Facilities. The continued flow of Iraqi oil exports is entirely dependent on oil production from Iraq's northern oilfields. The only outlet for this crude is the pipeline through Turkey to Yumurtalik on the Mediterranean. Both the pipeline and production system are highly vulnerable to disruption. Iran, for example, could interdict this pipeline through sabotage in either Iraq or Turkey or by air attacks against the pump stations along the line. Sporadic sabotage has taken place during the war, but the flow through the Turkish pipeline has only been interrupted for short periods. Another key facility is the large crude processing complex at Kirkuk. Iran already has knocked out three of the 14 plants at this facility, which has caused the loss of 640,000 b/d in desorbing capacity.

From an oil market viewpoint, the oil system in southern Iraq is of little concern. No oil has been exported from the Persian Gulf since the beginning of the war. Moreover, the most important facilities—Iraq's two sea island export terminals in the Persian Gulf—have already been rendered inoperable. Damascus's closure in March 1982 of the Iraq-Syria pipeline to the Mediterranean effectively shut down all remaining export outlets for southern Iraqi crude. The major petroleum facilities in this area might still constitute lucrative targets for

Iran. While damage in these areas would not impair current Iraqi export capability, it would complicate postwar reconstruction.

Iranian Facilities. Iran's most vulnerable choke point is the Kharg Island oil export terminal. The terminal, designed to export more than 6 million b/d, consists of an oil-loading jetty on one side of the island, a sea island off the other side, and a conventional buoy-mooring system. Approximately 25 million barrels of storage capacity are also located on the island. Iraq has conducted sporadic airstrikes against Kharg Island during the past 22 months, but damage never posed much more than a short-term inconvenience to Iranian petroleum operations. Other important petroleum facilities in Iran include three mainland booster stations that pump crude from the oilfields to Kharg Island. Iraq attacked the Gurreh booster complex last September, but damage was not serious. Iran has more than sufficient capability to enable it to bypass damage to Gurreh and still maintain export levels.

Vulnerability Elsewhere

We are concerned about the damage that could be inflicted on oil facilities in Kuwait and Saudi Arabia. Their oil production and export systems are highly concentrated and extremely vulnerable to sabotage or direct military action. Iran already has demonstrated its capability to inflict damage to the facilities. In early October 1981, Iranian F-4 fighters attacked Kuwait's largest gas-oil separation plant (Umm al'Aysh) at the Raudhatain Oilfield.

Kuwait. By far the most critical and vulnerable Kuwaiti petroleum choke points are the offshore and onshore terminal loading facilities at Ahmadi, as well as the two tank farms and manifold stations located nearby. Major damage to these facilities would seriously impair Kuwait's ability to export crude because Ahmadi constitutes the only existing outlet. Damage to large numbers of the more than two dozen gas-oil separation plants (gathering centers) would also critically impair Kuwaiti productive capacity. Most facilities in Kuwait are easily accessible and are close to each other. Well-organized attacks could at worst halt all Kuwaiti exports for several months.

Targeting and Security

Saudi Arabia and Kuwait are aware of their vulnerability, and have taken countermeasures during the past year to provide early warning and to make it more difficult for Iranian commandos to reach their coastal petroleum facilities. These include an increase in air and naval patrols around potential target areas, the positioning of guards at some offshore oil facilities, and tighter controls on access to installations. Both countries also are reviewing engineering recommendations that would reduce the vulnerability to disruption. Despite these measures, Tehran could still seriously damage petroleum installations in various Persian Gulf countries.

Oil Facility Restoration

If key facilities are damaged, major work programs would be needed for restoration and repair. To evaluate this issue we have analyzed the leadtime required to restore major petroleum facilities in the Gulf region. A key problem is that many critical components of these facilities—for example, high pressure separation valves, storage tanks, loading arms, and crude stabilization columns—are custom-ordered equipment and not generally stocked. Replacement, delivery, and installation could require several months or more.

- Saudi Arabia suffered two industrial accidents during the past four years, seriously damaging most essential equipment at two gas-oil separation plants. In each case, 10 to 12 months were needed to bring these facilities back in operation. Similarly, Kuwait faces at least a one-year restoration effort at its gas-oil separation plant bomb damaged by Iran last October.

Based on a variety of information, it appears that Persian Gulf countries have initiated planning to reduce the required snapback time in an emergency. Among the measures under consideration are the construction of bypasses around critical choke points, contingency plans to cannibalize equipment from less essential facilities, and the development of a strategic inventory of critical equipment. Despite these efforts, we do not believe the Saudis or Kuwaitis can rebuild rapidly any key facility that has sustained major damage.

PERSONNEL SECURITY

Security of personnel trumps all other considerations. After the taking of hostages at In Amenas, Statoil made it clear to the Algerian government and its Algerian partner Sonatrach that saving lives was the priority and, by 0930 the first day, transferred authority to a hostage incident response team.[27]

One of the first priorities for personnel security is a rapid evacuation plan and the capability to remove personnel from danger. This is especially important for remote facilities, including offshore facilities. Because evacuations are rare, standby evacuation transport equipment might also be rare. Arrangements might be made in advance with local military forces or contracted with civilian companies, however, especially for offshore platforms. Because of the large number of personnel on many oil production platforms, marine vessels as well as helicopters may be needed. As with infrastructure security, preplanned communications and coordination that includes the host government, security personnel, and military is essential, as well as a response plan that enables each party to know its responsibilities. In addition, threat assessments, vulnerability studies, personnel screening, and multiple layers of protection for personnel are critical.

In the case of hostage-taking, fallback plans for emergency communications should be prepared. For example, when Iraq initially held about 2,000 Western workers inside the country for months after invading Kuwait in August 1990, workers with one US construction company laid out baseball diamonds so that their location could be recognized by aerial reconnaissance.[28] Separation of personnel quarters from oil and gas operations also is important to minimize exposure to damages inflicted on volatile equipment and processes. Following its investigation, Statoil recommended upgrades to the security of In Amenas that included facilities to accommodate a military response to an incident and some protective measures for workers, including measures to reduce vulnerability and provide protection against a vehicle bomb.[29]

A question that arose in Statoil's investigation of the In Amenas attack is whether security guards inside a processing facility should be armed. In the case of In Amenas, the guards were not armed, which was a decision made easier by Algeria's forbidding foreigners to serve formally as guards.[30] Not allowing guards inside processing facilities to bear arms is common practice.

Among the key lessons Statoil said it learned from its investigation was the need for a "holistic" approach to the management of security risks and to make security part of the company's core business, project planning, and investment decision process. In examining its approach to security, Statoil had found that security was not established as a core function separate from safety, and in most cases "was a small part of broader health, safety, and environmental positions."[31] The recognition of security as a separate discipline, expertise, and profession is vital to any major company's ability to manage risk.

27 Statoil, "The In Amenas Attack."

28 Patrick E. Tyler, "Standoff in the Gulf; Hostage Exodus Begins in Iraq," *New York Times*, December 10, 1990, http://www.nytimes.com/1990/12/10/world/standoff-gulf-hostage-exodus-begins-iraq-75-come-hiding-kuwait.html?pagewanted=all.

29 Statoil, "The In Amenas Attack."

30 Statoil, "The In Amenas Attack."

31 Statoil, "The In Amenas Attack."

POLITICAL CRITICISM AND REPUTATIONAL RISKS

Energy companies increasingly are critiqued by NGOs, the press, and other private groups, especially when operating in areas in which there is real or perceived abuse of the environment or human rights, corruption, inequitable distribution of wealth or other discrimination, lack of transparency, and transgressions that might mar a company's brand and diminish its credibility and competitiveness. The application of sanctions also exposes companies to still further potential for criticism.

One of the best illustrations of reputational risk challenges is the public controversy surrounding the decommissioning of Shell and Exxon's large offshore Brent Spar oil storage and tanker-loading facility in the North Sea. With the completion of a pipeline from the Brent field to an oil terminal in Scotland in 1991, Brent Spar had no further value. Disagreement over the best means of disposing of the facility raised questions about corporate social responsibility to the public and generated considerable unwanted publicity for Shell United Kingdom (UK), which managed the operation of Brent Spar.[32] Shell studied six options for the facility, including two onshore and two offshore disposal options and two options to either refurbish or continue to maintain the facility. These were narrowed to two options, horizontal onshore dismantling and deep-water disposal. Following consultations with the UK oil industry regulator, the Department of Trade and Industry, and with conservation and fishing groups, Shell decided to dispose of the facility in Atlantic waters 2.5 kilometers deep and 250 kilometers off the west coast of Scotland.[33] In 1995, the UK government approved the decision. Shell said that its scientific research and independent studies showed that this option would have negligible impact on the environment, would be less risky to workers, and cheaper than the onshore alterative.[34]

Greenpeace had long protested the disposal of any waste in the ocean and organized a widespread public campaign against Shell's decision. Greenpeace gained publicity by putting a team on Brent Spar in April 1995 and occupying it for several weeks. Greenpeace also released an estimate that there were 5,500 tons of crude oil left in the facility, far more than Shell's estimate of 50 tons. The campaign generated considerable public support in Germany, Denmark, and the Netherlands, diminishing Shell's stock value and reducing sales by 20 percent at Shell service stations in Germany.[35] About fifty stations were damaged. Facing growing damage to its reputation and brand, Shell reversed its decision in June 1995 despite already starting to tow the Brent Spar to deep water. After further, years-long study, Shell decided to dismantle the Brent Spar and use the largest parts to construct a ferry quay extension near Stavanger in Norway.[36]

The Brent Spar controversy raises lots of questions, ethical and otherwise. One clear lesson that Shell UK officials embraced is that the company initially made a decision without engaging and communicating with all of the appropriate stakeholders, which most importantly should have included environmental groups and public interests in northern continental Europe. Shell UK officials said that they initially treated the Brent Spar disposal decision as a Scottish and UK issue. The chairman of Shell UK said in 1998: "The days when companies are judged solely in terms of economic performance and wealth creation have disappeared. . . . Today, demands for openness and transparency in business reporting come from a wide range of stakeholders."[37] Following the dismantling of

32 See Shell UK, "Brent Spar Dossier," 2008, http://www.shell.co.uk/sustainability/decommissioning/brent-spar-dossier/_jcr_content/par/textimage.stream/1426853000847/6b0c52ecc4c60be5fa8e78ef26c4827ec4da3cd3cd73747473b4fc60f4d12986/brent-spar-dossier.pdf. The operation and disposal of the Brent Spar was the responsibility of Shell UK Exploration and Production ('Shell Expro'), the offshore oil and gas exploration and production division of Shell UK Limited, a large operating company that is part of the Royal Dutch Shell Group of companies. Shell UK Exploration and Production is operator of a co-venture in the UK North Sea with Esso Exploration and Production UK Limited. Both parties owned equal shares in the Brent Spar.

33 "Brent Spar Case," Ethics in Management Project, August 12, 2016, https://ethics-in-mgmt-project.wikispaces.com/Brent+Spar+Case; D. Nathan Meeham, "Society of Petroleum Evaluation Engineers Ethics Seminar," Baker Hughes, August 12, 2016, https://secure.spee.org/sites/spee.org/files/09%20Meehan%20SPEE%20Ethics.pdf.

34 Shell UK, "Brent Spar Dossier."

35 Brian Molloy, "The Environmental Conflict Surrounding the Decommissioning of Brent Spar," November 30, 2016, https://www.iaea.org/nuccomtoolbox/documents/Brent_Spar_Case_Study.pdf; Nathaniel C. Nash, "A Humbled Shell is Unsure on Disposal of Atlantic Rig," *New York Times*, June 23, 1995, http://www.nytimes.com/1995/06/23/business/international-business-a-humbled-shell-is-unsure-on-disposal-of-atlantic-rig.html.

36 Shell UK, "Brent Spar Dossier."

37 Ibid.

Disposal of the Brent Spar oil storage and tanker loading facility in the North Sea became a case study in reputational risk. *Photo credit:* Reuters.

the Brent Spar, a ban on future disposal of North Sea oil facilities at sea has gained widespread support.[38]

While the Shell UK experience with disposing of the Brent Spar facility provides a good case study of how to mitigate a reputational risk, one of the key questions raised by the Brent Spar controversy is how a company should balance commercial and social responsibilities. In particular, to what extent was Shell UK's decision commercial and to what extent did social responsibility enter their analysis? How do companies decide the appropriate set of stakeholders in a decision? Also, in this case Shell UK agreed that public opinion had a valid interest and input, but what if a company thinks that public opinion is wrong?[39] And how should the company react to allegations that it believes or knows are false?[40]

A more recent example of a major energy company engaging with a private advocacy group is BP's response to a paper released by Amnesty International in May 2004, which accused BP of failing to protect human rights in its Baku-Tbilisi-Ceyhan oil pipeline construction project. BP began a direct dialog with Amnesty International to inform the group about BP's plans to implement the Voluntary Principles on Security and Human Rights in all the security protection plans for the pipeline and to address BP's commitments to protect other wide-ranging human rights.[41] BP and its partners in Azerbaijan's largest oil

38 Ibid.

39 See Ethics in Management Project, "Brent Spar Case."

40 See Royal Dutch Shell, Brent Spar Dossier for the example of Royal Dutch Shell's claim that Greenpeace vastly exaggerated the amount of crude oil left on Brent Spar. Shell UK's Norwegian contractor measured the amount of oil at 150 tons when it was finally dismantled. Greenpeace admitted its inaccurate claim and apologized to Shell in September 1995, after Shell UK had reversed its decision to dispose of Brent Spar at sea. See Brandon Mitchener, "Environmentalists Apologize to Shell for Using Faulty Data: Greenpeace Admits Slip on Oil Rig Risk," *New York Times*, September 6, 1995, http://www.nytimes.com/1995/09/06/news/06iht-brent_.html.

41 Jonathan Elkind, "Economic Implications of the Baku-Tbilisi-Ceyhan Oil Pipeline"; According to the US Department of State, The Voluntary Principles on Security and Human Rights "guide companies in conducting a comprehensive human rights risk assessment in their engagement with public and private security providers to ensure human rights are respected in the protection of company facilities and premises," US Department of State, "Voluntary Principles on Security and Human Rights," December 20, 2012, http://www.state.gov/j/drl/rls/fs/2012/202314.htm.

development project also introduced the Extractive Industries Transparency Initiative to the country.

Protests are likely to continue from private groups over human rights and also over the use of water and reservoir fracturing in shale oil and gas production. Eastern Europe, for example, has experienced a wave of protests in the past few years over the use of hydraulic fracturing to test the potential for shale oil production. Russian influence is associated with some of these protests.[42]

As these examples show, the importance of reputation to companies is likely to warrant efforts to protect it. Options that have proved useful are transparency and engagement with the public, along with concrete social, workplace, and community actions that demonstrate an appreciation of public interests and which, ideally, provide results that can benefit a wide array of stakeholders, including the company.

42 Keith Johnson, "Russia's Quiet War Against European Fracking," *Foreign Policy*, June 20, 2014. http://foreignpolicy.com/2014/06/20/russias-quiet-war-against-european-fracking/.

FINANCIAL RISKS

To a large extent, most of the risks covered in this report ultimately could be boiled down to financial risks, with the notable exception of personnel security risks. Financial risks have always been present, including market risks and the risk of expropriation, in particular, but some risks have grown in use and nature. Sanctions, for example, have been widened to include financial transactions and individuals as well as energy sales and purchases, imposing added burden, risk, and financial exposure for international companies. Local content requirements have grown, imposing additional burdens on companies, adding to expenses, and adding to the risk of greater losses due to inadequacies of some local labor, equipment, and services. Bureaucratic delays and visa and currency restrictions undermine efficiency and profit margins. Fines are being used as a source of government revenue and leverage, including by local government entities that previously had no role in policing company operations. Kidnap and ransom have grown as commercial risks as well as security threats. Changing tax codes are a risk in developed countries, such as the United States, as well as in developing countries.

Perhaps the greatest long-term financial risk facing oil and gas companies is the impact of climate change policies on the demand, supply, and future prices for high-carbon fuels. A recent study by Chatham House, which analyzed the possible implications of climate change for investment, points out that there is considerable uncertainty about how strong and effective policies to limit greenhouse gases will be, whether the policies will be supported by needed investments in renewable energies, efficiency improvements, and other low-carbon fuels. There is also still much uncertainty about the level of tax increases on fossil fuels that might be levied to mitigate demand and the subsidies that may be needed to boost low-carbon alternatives.[43]

The extent of the relationship between greenhouse gases and climate change is another uncertainty affecting the need to reduce high-carbon fuels. The International Energy Agency estimates that "strong" policies to limit global warming would reduce investment needed by 2050 by about 15 percent in the gas sector, 20 percent in the oil sector, and 33 percent in the coal sector. Moreover, international oil companies would be more vulnerable to oil price impacts than national oil companies because state-owned firms have a higher percentage of total oil reserves and resources as well as lower cost reserves and resources. The Chatham House study points to a 2014 cost curve study, Carbon Tracker, in which it is estimated that 84 percent of projects owned, or partly owned, by state firms would be economic at prices ranging up to $80 per barrel, but only 40 percent of projects available to private companies are in this price range.[44] Of course, the dynamics of costs, as well as all other factors, are subject to change.

In the United States, the challenge of anticipating climate change-related policies is magnified by a deep policy division.[45] This division is likely to slow policy

43 John Mitchell, Valerie Marcel, and Beth Mitchell, "Oil and Gas Mismatches: Finance, Investment and Climate Policy," Chatham House, July 2015. https://goo.gl/9j2ncx.

44 Ibid.

45 David Goldwyn, Robert McNally, and Elizabeth Rosenberg, "Increasing Prosperity, Resource Stewardship, and National Security," Papers for the Next President Series, Center for a New American Security, October 2016, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-PapersforthePresEnergy-finalb.pdf.

US differences on climate change science run deep. *Photo credit:* Reuters/Pauline Askin.

change, but adds uncertainty that could challenge aspects of energy operations and investment as well as impact the economics of long-term energy projects.

Despite divisions on climate change science, policy officials worldwide are increasingly addressing environmental concerns, taking account of local concerns about pollution and other impacts of oil and gas operations. The trend toward increasing concerns and responses to climate change considerations has also gained ground. The European Union is collectively pursuing goals related to climate change and several European countries have imposed taxes on carbon emissions.[46] Other countries, such as Japan and Canada, also tax carbon emissions or are moving to impose new taxes on carbon emissions.[47] Over time, these policies could change the relative values of energy assets, including petroleum resources.

Aside from generating financial risks, climate change-related concerns could also heighten companies' exposure to political attacks and reputational risks, and climate change itself poses potential hazards to existing and future energy infrastructure.

Amid this uncertainty over the impact of climate change policies, there are some options major international oil companies can consider that might help balance their risk, according to some consultants. These include divesting business units that are not profitable at lower oil prices, creating stand-alone business units for some riskier parts of the company, diversifying into renewable energy resources, and pursuing access to lower cost oil and gas resources, such as capitalizing on competitive advantages by buying holders of low-cost oil or entering joint ventures with state-owned companies.[48]

46 European Commission, "EU Climate Action," last updated December 8, 2016, http://ec.europa.eu/clima/citizens/eu/index_en.htm; World Bank, "Putting a Price on Carbon with a Tax," November 22, 2016, http://www.worldbank.org/content/dam/Worldbank/document/SDN/background-note_carbon-tax.pdf.

47 Ibid; Associated Press, "Canada Will Tax Carbon Emissions to Meet Paris Climate Agreement Targets," *The Guardian,* October 3, 2016, https://goo.gl/w1zjPd.

48 As You Sow, "Unconventional Risks, The Growing Uncertainty of Oil Investments," August 17, 2016, http://www.asyousow.org/

CORRUPTION

From an international perspective, corruption means different things to different governments, but this just increases the risks to energy companies trying to navigate different cultures and laws. Oil is also a particularly corrupting commodity worldwide because of its high value. The widespread government perceptions beyond North America and a few other countries is that energy is a strategic and political good that requires government control. Some governments resemble investment schemes, in which officials gather investments from family, friends, and business partners to buy an important and lucrative position in the government. Those officials are then beholden to pay back their investors and might have a limited time in the government to do so. Oil extraction and related activities such as permits, taxes, customs collection, transport charges, and expenditures for security provide a quick and easy source of revenue for such purposes.

Oil is also frequently subsidized to curry political favor from local populations, especially as elections approach. Subsidized prices generate incentives to transfer sales to higher-priced markets. Stolen oil is even more lucrative to sell, and siphoning off tax revenues from oil-related industries creates another possible diversion of revenues.

The US Foreign Corrupt Practices Act has resulted in some large fines to energy companies for bribery and related offenses; other countries have similar versions. This further complicates operations for international companies. A compliance program tailored to a firm's particular situation that covers interactions with host government officials, partners, contractors, sub-contractors, and agents and includes detailed records of transactions will help mitigate risk. There are some basic red flags to observe according to a recent presentation by Dentons:

- Doing business in a country with historical corruption problems
- Refusal to promise in writing to abide by anti-corruption laws
- Lack of qualifications to do what the third party has been engaged to do
- Relationships with government officials
- Government officials serving as principals of the third party
- Reputation for unusual or unethical business practices
- Reliance on government contacts rather than knowledgeable staff and investment of time to promote company interests
- Inadequate or generic descriptions on invoices
- Missing or incomplete supporting documentation for invoices
- Requests for payments in cash or of unusual size or delivery method
- Requests for advance payments before service has been completed
- Desire to keep business relationships or location of bank accounts secret
- Mitigation includes a strong anti-corruption plan and training program.[49]

ays_report/unconventional-risks-the-growing-uncertainty-of-oil-investments/.

49 Dentons, "Compliance Trends Affecting Energy Companies Globally," June 10, 2014, https://www.acc.com/chapters/houst/upload/June-2014.pdf.

Table 2. Country Rankings for Absence of Corruption

Country	Score	Country	Score	Country	Score
Denmark	0.96	Croatia	0.54	Ivory Coast	0.4
Norway	0.93	Senegal	0.53	Zambia	0.4
Singapore	0.93	Jamaica	0.53	Bulgaria	0.39
Sweden	0.91	Macedonia, FYR	0.52	Nepal	0.39
Finland	0.9	Thailand	0.52	Burkina Faso	0.38
New Zealand	0.9	Romania	0.52	Indonesia	0.37
Netherlands	0.89	China	0.51	Nicaragua	0.37
Japan	0.86	South Africa	0.51	Lebanon	0.37
Australia	0.84	Belarus	0.5	Tanzania	0.37
Hong Kong, China	0.84	Tunisia	0.5	Albania	0.36
Austria	0.83	Hungary	0.5	Dominican Republic	0.36
Germany	0.83	Panama	0.49	Malawi	0.36
United Arab Emirates	0.82	Philippines	0.49	Uzbekistan	0.35
Republic of Korea	0.82	Morocco	0.49	Madagascar	0.35
United Kingdom	0.82	Turkey	0.49	Pakistan	0.35
Canada	0.81	Belize	0.48	Ukraine	0.34
Belgium	0.81	Argentina	0.48	Honduras	0.34
Uruguay	0.78	Egypt	0.47	Peru	0.34
Estonia	0.78	Ethiopia	0.47	Bolivia	0.34
United States	0.75	Sri Lanka	0.46	Mexico	0.33
France	0.75	Brazil	0.46	Guatemala	0.33
Georgia	0.73	Vietnam	0.46	Kyrgyzstan	0.3
Chile	0.72	Ecuador	0.45	Sierra Leone	0.3
Portugal	0.71	Kazakhstan	0.45	Zimbabwe	0.28
Spain	0.69	Ghana	0.44	Moldova	0.28
Costa Rica	0.68	Russia	0.44	Liberia	0.28
Czech Republic	0.66	Bosnia and Herzegovina	0.43	Venezuela	0.27
Poland	0.65	El Salvador	0.43	Kenya	0.27
Botswana	0.65	Colombia	0.43	Nigeria	0.27
Malaysia	0.63	Iran	0.42	Bangladesh	0.27
Slovenia	0.6	Myanmar	0.42	Cambodia	0.27
Jordan	0.59	Mongolia	0.42	Uganda	0.27
Italy	0.59	Serbia	0.41	Cameroon	0.25
Greece	0.54	India	0.4	Afghanistan	0.23

Source: World Justice Project, Absence of Corruption Index 2015, http://worldjusticeproject.org/sites/default/files/roli_2015_0.pdf.

CYBERATTACKS

Energy systems are highly vulnerable to cyberattacks due to the widespread use of electronic controls, including Supervisory Control and Data Acquisition (SCADA) systems used to control pipelines and other facilities.

The most damaging cyberattack on energy infrastructure to date occurred in December 2015, when an attack brought down the power grid in western Ukraine for six hours. The attack reveals some of the extensive damage that such a cyber raid can inflict, including physical damage to critical equipment and facilities. It targeted SCADA systems in Ukraine, which include controls linked to the Internet, and it highlights the vulnerability of such control systems, which according to cyber security experts are susceptible to breach by a determined hacker. The risk increases if the attack is state-sponsored.[50]

The attack caused widespread electrical outages in Western Ukraine according to an assessment by Dentons, leaving over 700,000 residents without power. One electricity distribution company said that twenty-seven of its substations were knocked offline, 103 cities completely lost power, and 186 cities suffered partial blackouts. Another electricity distribution company said that thirty of its substations went offline. Communications with call centers were also blocked, preventing many customers from reporting the outages. Field operators manning substations had to manually reclose breakers to restore power and switch operations to manual mode.[51]

Multiple attack elements were combined to bring down the power grid and complicate restoration of power and the investigation of the attack. The attack employed malware to gain entry and infect the operating system by "spear phishing" with a Microsoft Word attachment and inducing a recipient to open it despite built-in Microsoft Office security warnings. The email was designed to appear to be from the Ukrainian Parliament. The malware spread from the workstation into the SCADA system, allowing the attackers to remotely operate control systems and blinding system operators to the damage. The blocking of customers' calls to report damage further disguised the attack, delaying the response and allowing the attackers more time to destroy files.[52]

The US government recently announced a scale to rate the severity of cyberattacks, ranging from Level Zero for an "inconsequential" attack to a Level Five for an "emergency" or an attack that poses an "imminent threat" to critical systems such as the electric grid, the stability of the federal government, or people's lives, according to the Washington Post. A US official said that the suspected Russian cyberattack on Ukraine's power grid would have been rated a Level Four had it occurred in the United States. A Level Four event is a "severe" event likely to cause "significant" harm to public safety or national security, according to the US government scale.[53]

Other significant cyberattacks on critical infrastructure include a massive cyberattack against Saudi Aramco in August 2012 and a series of cyberattacks against Estonia beginning in April 2007 amid a dispute with Russia. The malware attack on Saudi Aramco lasted just a few hours but totally or partially destroyed 35,000 hard drives on Aramco computers. Initial entry into Aramco's network was obtained when an Aramco employee clicked on a spear phishing email. A group called The Cutting Sword of Justice claimed responsibility, citing Aramco's support for the Saudi royal family. Aramco immediately disconnected all of its computers from its systems and data center as well as the Internet. Oil production continued because Aramco had invested heavily in cyber security for industrial operations, but all business transactions had to be handled on paper. Aramco needed five months to recover, during which it purchased 50,000 replacement hard drives, driving up the cost of hard drives for everyone from September 2012 to January 2013, and had to build a new security operations center.[54]

In Estonia, a three-week barrage of cyber warfare triggered by the relocation of a soviet war memorial

50 Dentons, "Global Energy Game Changers," Spring 2016, http://www.dentons.com/en/insights/guides-reports-and-whitepapers/2016/april/12/global-energy-game-changers. Dentons' experts note that this account of the cyberattack against Ukraine is based on information deemed to be true and reliable; however, Dentons makes no representations to the same.

51 Ibid.

52 Ibid.; Gabrielle Desarnaud, "Cyber Attacks: A New Threat to the Energy Industry," Institut français des relations internationales, July 7, 2016, https://www.ifri.org/sites/default/files/atoms/files/edito-desarnaud_cyber_attacks_energy_industry_eng2.pdf.

53 Ellen Nakashima, "United States Reveals Game Plan for when Cyberattackers Strike," *Washington Post*, July 27, 2016.

54 Fahmida Y. Rashid, "Inside the Aftermath of the Saudi Aramco Breach," *Dark Reading*, August 8, 2015, http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676.

and war graves in Tallinn targeted public and private institutions including government ministries, political parties, universities, banks, telephones, and newspapers. A major effort by the Estonian government to address shortcomings in information technology and telecommunications after the breakup of the Soviet Union had created heavy reliance on the Internet as well as vulnerabilities that hackers were able to exploit by orchestrating massive attacks using a variety of techniques, including denial of service and flooding attacks. The hackers sent out instructions to other websites on how to attack Estonian cyber targets and enlisted or commandeered computers in over fifty countries, including the United States, in the attack.[55] The widespread denial of services raised tensions between Estonia and Russia, created instability and riots in Estonia, and led Tallinn to ask for assistance from NATO and other allies. Estonia needed an emergency government-led response team and help from Finland, Germany, Israel, and Slovenia to first isolate its system from international networks and then restore its own networks.[56] The seriousness of the attack awakened other countries to difficulties in dealing with cyber warfare and potential vulnerabilities of critical infrastructure and operating systems, including energy networks.

The culture, history, and structure of energy companies make them particularly vulnerable to cyberattacks. Culturally, industrial operations conducted by energy firms are generally designed by engineers primarily for efficiency, safety, and physical security rather than for cyber security. Historically, operational control systems procured and used to automate and optimize industrial functions were probably first introduced as proprietary systems with specific purposes. This would make them more difficult to hack than later, off-the-shelf software adopted for current business, communications, and industrial operations. Structurally, different business units and equipment in a company can be used by hackers to gain access to networks linked to operating controls and systems for key operations, heightening overall vulnerability.[57]

According to Dentons' analysis, which is based on widespread reporting, many industrial control systems that run critical infrastructure in the United States probably have been infected by malware similar to that used in previous attacks. Major targets probably include military systems, energy installations and networks, airport controls, and telecommunications. Smaller targets include metering facilities that allow oil theft by remotely tampering with meters measuring oil and gas volumes, or for insiders to redirect oil to different accounts. Other sectors such as health care, manufacturing, and transportation also are probably at risk. As the Internet and cyber capabilities evolve, these systems could become even more vulnerable because many components may have been designed and installed without taking into account modern Internet threats.[58]

Use of mobile phones and other personal devices to share sensitive information can magnify all other risks that companies face by increasing opportunities for other parties to use the information for financial gain or other malicious purposes. Even if one's own devices are secure, interacting with another mobile phone or device that is not secure can provide access to such information. Mobile phones and other devices also make it easy to track personnel for malicious purposes.

Dealing with the risk of cyberattacks requires preparation and planning similar to that required for physical attacks. The first goal should be prevention, and firms should consider this a risk management issue. Four steps can be taken to reduce vulnerability to cyber breaches.[59]

The first step is to protect digital devices and communications with anti-virus software, secure connections, firewalls, and passwords for all mobile and desktop devices. Mobile phones are especially vulnerable to interception. Access to sensitive data or equipment should be strictly limited to vetted personnel and not shared with contractors or outside partners, including national oil company officials unless they are also vetted. A cyber protection program also should include an advance determination of what constitutes a breach in security that will require a response. Personnel should know beforehand if a breach is any unsanctioned access of a system or only incidents in which something has been damaged or taken.[60]

55 Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for US National Security," *International Affairs Review*, Summer 2015, http://www.iar-gwu.org/node/65.

56 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security,* Summer 2011, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.

57 Gabrielle Desarnaud, "Cyber Attacks: A New Threat to the Energy Industry."

58 Dentons, "Global Energy Game Changers."

59 Dentons, "Cybersecurity, Part 2: Firms Should Avoid These Common Mistakes," May 11, 2016, http://www.dentons.com/en/insights/newsletters/2016/may/11/daily-report-in-practice/cyber-security-part-2-firms-should-avoid-these-common-mistakes.

60 Ibid.

Second is to prepare a detailed response plan, which should designate the person to be in charge of a response, a reporting chain of command and process for coordination, information on the physical location of data to help the internal investigation, a plan for conducting interviews and preserving evidence, a plan to notify employees or affected parties, and plans for dealing with the authorities and press.[61]

Third is to test systems regularly, both to determine normal levels of activity and to detect breaches. Evidence of a cyberattack can be subtle, and a firm might only detect a breach if it can determine a certain level of activity is abnormal. Another option is to hire someone to test the system by trying to hack into it. This can help identify vulnerabilities in the company's system as well as help alert the firm to suspicious activity.[62]

Fourth is to train personnel to recognize and avoid risks, how to practice the firm's security policies, and how to report a possible breach. Such training needs to include managers, contractors, and partnering companies.[63]

As in infrastructure and personnel security, vetting of employees, contractors, and other persons with access to information and control systems is very important. Insider assistance, knowledge, and participation can have similar consequences as devastating in cyberattacks as in attacks on infrastructure and personnel.

Additional options include professional liability insurance policies that specifically cover liability for information and other cyber breaches. Lawyers with experience in cyber security protection can help design a cyber protection plan, investigate and respond to incidents, and advise on what protections are most useful.[64]

61 Ibid.
62 Ibid.
63 Ibid.
64 Ibid.

POPULISM

Populism is an additional risk that cuts across many of the identified categories of risk that companies face in petroleum investment and development activities. It takes a variety of forms that interact with and magnify financial and political risks as well as expose investors and operators to political criticism and reputational risk.

Populism can arise quickly when associated with a change in government and frequently accentuates other risks to a wide range of market activities. Populist policies can undermine the rule of law and efficiencies of free market forces, especially in the hands of authoritative governments without checks and balances. Populism in petroleum-producing countries accompanied by large subsidies for energy and other commodities historically tends to be unfavorable to investment as the government becomes more dependent on energy revenues and sovereign wealth funds, leading to devaluation in the local currency, which causes capital flight and raises uncertainty. Venezuela under Hugo Chavez and Nicola Maduro is a blatant example of the negative impact populist energy policies can have, in this case magnified by an extraordinarily authoritarian brand of populism. Other countries in Latin America, including Argentina and Brazil, have also suffered from populist policies since the turn of the century, but the geographical dispersion of examples is widespread. Russia, Iran, Egypt, Thailand, and Indonesia are among those that have struggled with populism, as well as a number of African countries.

Populism is generally defined by national policies that seek short-term goals, which are popular with the public, strong central government control of revenues, cronyism, corruption, suppression of opposition parties and media, direct appeal to the populace for political support, marginalizing of democratic institutions, weak legislatures, a lack of transparency in government operations, subsidies of energy and other basic goods, overspending, and currency volatility and devaluation leading to capital flight. The particular risk to energy companies in such an environment is the potential for them to be targeted as sources of additional revenue and low-cost energy, or accused of greed and conspiratorial, corrupt behavior in order to boost the popular appeal of public officials.

Mitigating the risk of exposure to populism is difficult. Diversifying investments geographically and conducting appropriate due diligence in political risk assessments are fairly obvious measures, as

Former President Hugo Chavez rode the bounty of high oil prices to popular support in Venezuela. He was succeeded by Nicolas Maduro following his death from cancer in March 2013. *Photo credit*: Reuters/Marco Bello.

well as carrying sufficient political risk insurance and negotiating contracts that provide the host government a strong interest in the financial success of projects. Early identification of the characteristics and potential for populism can be key to avoiding losses in assets in some circumstances. Even in cases such as Venezuela, however, some companies have been able to continue operating.

CONCLUSIONS AND IMPLICATIONS

The risks on the playing field for international companies investing in and operating petroleum projects have grown with the rise of terrorist threats, armed conflicts, failing and failed states, cyberattacks, and reputational risks. At the same time, financial risks linked to market volatility, sanctions, taxes, emissions restrictions, corruption, rule of law, and contract sanctity still abound, adding to uncertainty and the need for integrated risk management and planning. "The rise in cyber capabilities alone is a game changer that magnifies all other risks as well as introducing new and dangerous risks to the industry. The spread of conflict coupled with weakened states that cannot enforce or refuse to enforce rule of law and regulatory requirements poses additional challenges."[65]

Risks posed by climate change and populism cut across other categories of risk and generate an increased level of concern because the stakes can be particularly high for companies with large investments in long-term projects. Early recognition and diverse investment strategies can help ease possible negative financial, reputational, and other consequences of change that adversely impact companies' assets and outlook.

Looking ahead, cyber security may generate the biggest changes in the operation of energy firms. The need to encrypt operational controls and communications, including email, may be on the horizon. Other investment and operational risks are likely to remain high priorities, especially personnel security and reputational challenges.

Statoil's recommendation that the security discipline and profession be separated from safety following its investigation of the In Amenas attack represents a major step forward for managing security risks. The company further recognized the need to integrate the management of physical, personnel, and cyber risks in its reassessment of security capabilities and procedures.

Dealing with the uncertainty of the impact of climate change policies on hydrocarbon markets may present petroleum companies with a new and expensive financial risk. The question of how strongly policies to reduce greenhouse gas will be pursued is currently open to a wide variety of scenarios, making it difficult, at this stage, to plan. The amount of information available to companies on this issue is increasing, however, and the direction of the policy in some countries is gaining clarity.

The issue of reputational risk has also become a bigger concern, and demands more attention from companies to public interests such as protecting the environment and human rights, among other considerations. As has been shown, reputational interests cannot be divorced from commercial interests. Transparency, communications with the public along with social, workplace, and community actions are useful options to deal with challenges to companies' reputations. Use of the Voluntary Principles on Security and Human Rights and the Extractive Industries Transparency Initiative are also helpful ways to serve a variety of interests.

Finally, high risk locations are not always bad places to invest. Despite the volatility, favorable terms and shared interests among all shareholders can help lead to profitable projects.

65 Karl Hopkins, Atlantic Council Global Energy Center conference with Dentons' security experts on November 28, 2016.

ABOUT THE AUTHORS

Bud Coote is a senior fellow with the Atlantic Council Global Energy Center. He recently retired from the Central Intelligence Agency (CIA) as the Agency's leading international energy analyst and a key adviser to senior US officials on a wide array of global energy issues. He helped to establish and build the CIA's energy program dating back to the early 1970s, producing actionable intelligence that directly supported and helped shape decisions made by US policy officials, foreign officials, and private companies. His most recent publication is an Atlantic Council report on S*urging Liquefied Natural Gas Trade: How US Exports Will Benefit European and Global Gas Supply Diversity, Competition, and Security*.

Karl V. Hopkins is a Dentons' partner and global chief security officer. He counsels the firm on international strategy, business and political intelligence, and security and threat analysis. In addition, he provides strategic advice to the firm's clients on global operations, including the performance of due diligence and compliance investigations, physical and cyber security assessments, country and political risk assessments, and threat analyses. This includes risk management and organizational resiliency advice. Karl also provides clients with strategic and legal advice regarding crisis and incident response. He has managed various types of crises, including physical security breaches and cyber incidents, insider threats, and reputational impacts. He also assists clients with the formulation and implementation of communication and crisis management policies and protocols. In addition, Karl has represented a number of multinational clients before various arbitration tribunals and in global asset identification and recovery matters, and has extensive experience advising clients, including a number of oil and gas producers and oilfield service and supply companies around the globe in connection with energy infrastructure projects.

ACKNOWLEDGMENTS

The authors wish to thank the following for their support and valuable contributions to this report: Gregory Gause, Kevin Hulbert, Arkadiusz Krasnodębski, Melissa Mahle, Lori Taylor, and Clinton A. Vince. The Global Energy Center would also like to recognize the tireless efforts of our publications team in making this report a success.

Atlantic Council Board of Directors

CHAIRMAN
*Jon M. Huntsman, Jr.

CHAIRMAN EMERITUS, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*George Lund
*Virginia A. Mulberger
*W. DeVier Pierson
*John J. Studzinski

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
*Peter Ackerman
Timothy D. Adams
Bertrand-Marc Allen
John R. Allen
Michael Andersson
Michael S. Ansari
Richard L. Armitage
David D. Aufhauser
Elizabeth F. Bagley
Peter Bass
*Rafic A. Bizri
Dennis C. Blair
*Thomas L. Blair
Philip M. Breedlove
Reuben E. Brigety II
Myron Brilliant
Esther Brimmer
*R. Nicholas Burns
William J. Burns
*Richard R. Burt
Michael Calvey
John E. Chapoton
Ahmed Charai
Sandra Charles
Melanie Chen
George Chopivsky
Wesley K. Clark
David W. Craig
*Ralph D. Crosby, Jr.
Nelson W. Cunningham
Ivo H. Daalder
Ankit N. Desai
*Paula J. Dobriansky
Christopher J. Dodd
Conrado Dornier
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
Julie Finley
Lawrence P. Fisher, II
*Alan H. Fleischmann
*Ronald M. Freeman
Laurie S. Fulton
Courtney Geduldig
*Robert S. Gelbard
Thomas H. Glocer
*Sherri W. Goodman
Mikael Hagström
Ian Hague
Amir A. Handjani
John D. Harris, II
Frank Haun
Michael V. Hayden
Annette Heuser
Ed Holland
*Karl V. Hopkins
Robert D. Hormats
Miroslav Hornak
*Mary L. Howell
Wolfgang F. Ischinger
Reuben Jeffery, III
Joia M. Johnson
*James L. Jones, Jr.
Lawrence S. Kanarek
Stephen R. Kappes
Maria Pica Karp
Sean Kevelighan
*Zalmay M. Khalilzad
Robert M. Kimmitt
Henry A. Kissinger
Franklin D. Kramer
*Richard L. Lawson
*Jan M. Lodal
Jane Holl Lute
William J. Lynn
Izzat Majeed
Wendy W. Makins
Zaza Mamulaishvili
Mian M. Mansha
Gerardo Mato
William E. Mayer
T. Allan McArtor
John M. McHugh
Eric D.K. Melby
Franklin C. Miller
James N. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Susan Molinari
Michael J. Morell
Georgette Mosbacher
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Sean C. O'Keefe
Ahmet M. Oren
*Ana I. Palacio
Carlos Pascual
Alan Pellegrini
David H. Petraeus
Thomas R. Pickering
Daniel B. Poneman
Daniel M. Price
Arnold L. Punaro
Robert Rangel
Thomas J. Ridge
Charles O. Rossotti
Robert O. Rowland
Harry Sachinis
Brent Scowcroft
Rajiv Shah
James G. Stavridis
Richard J.A. Steele
*Paula Stern
Robert J. Stevens
John S. Tanner
*Ellen O. Tauscher
Nathan D. Tibbits
Frances M. Townsend
Clyde C. Tuggle
Paul Twomey
Melanne Verveer
Enzo Viscusi
Charles F. Wald
Michael F. Walsh
Mark R. Warner
Maciej Witucki
Neal S. Wolin
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
George P. Shultz
John W. Warner
William H. Webster

*Executive Committee Members
List as of December 1, 2016

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org