Energy and conflict: Security outsourcing in the protection of critical energy infrastructures

Yuliya Zabyelina and Irina Kustova

Cooperation and Conflict published online 3 December 2014
DOI: 10.1177/0010836714558640

Article

Cooperation and Conflict
1–19

DOI: 10.1177/0010836714558640
cac.sagepub.com
SAGE

Energy and conflict: Security outsourcing in the protection of critical energy infrastructures

Yuliya Zabyelina
John Jay College of Criminal Justice, USA

Irina Kustova
University of Trento, Italy

Abstract

Attacks on oil and gas infrastructures by terrorists and criminals in places like Nigeria, Colombia, Iraq and Russia have amplified the vulnerability of critical energy infrastructures (CEIs) to deliberate physical attacks. Being unable or unwilling to protect CEIs, many national governments have made attempts to alleviate these vulnerabilities through outsourcing of security, i.e. contracting the responsibility to protect CEIs out to non-state actors. This article advocates the need to conceptualize security outsourcing in the domain of critical energy infrastructure protection (CEIP) in order to explain a variety of regulatory choices made by governments in this domain. Based on a qualitative analysis of four case studies, the article discusses various types of security outsourcing in the protection of CEIs, including the militarization of national oil companies, public–private partnerships and the involvement of international organizations and local social groups. The typology may serve as a tool of describing, classifying and evaluating various forms of security outsourcing. The findings of the article help to deconstruct the complexity of security outsourcing and capture some of the major contemporary trends in energy security.

Keywords

Critical energy infrastructure, oil theft, private military and security companies, public–private partnership, security outsourcing

Introduction

On the one hand, naturally vulnerable infrastructures have existed for a long time, and in that sense the need to protect critical energy infrastructures (CEIs)—facilities and

Corresponding author:
Yuliya Zabyelina, Department of Political Science, John Jay College of Criminal Justice, 524 West 59th Street, Room 9.65.36 New Building, New York, NY 10019, USA.
Email: yzabyelina@jjay.cuny.edu

services that are vital to the production, transmission and distribution of energy—is not a novel task for national governments. On the other hand, the increasing interest in CEIs in recent years reflects the changing conditions of states with regards to growing interdependencies, threat perceptions and the empowerment of violent non-state actors (VNSAs), all of which have profoundly challenged national security programs. While before the 1990s asymmetrical threats, e.g. terrorist and criminal attacks on CEIs, had a more occasional character, the post-Cold War era has witnessed repeated disruptions of CEIs by VNSAs in various parts of the world.

Large-scale illegal oil tapping and pipeline sabotage have become an increasingly salient issue over the last two decades. Terrorists, insurgents, opposing factions in civil wars and members of organized criminal groups have demonstrated the ability and willingness to attack CEIs. Although threats to CEIs have a truly global nature, they represent the biggest challenge for (post-)conflict regions and weak states (Koknar, 2009). Exploration and extraction of resources in these states have been a long and hard experience in coping with challenging security conditions and unstable political environments—the problems that have often been discussed in the 'resource course' literature (Rosser, 2006).

For example, it is estimated that oil production in Nigeria runs at only two-thirds of its capacity largely because of theft and disruption caused by the civil war (United Nations Office on Drugs and Crime (UNODC), 2009). According to the BBC report, oil theft costs Nigeria US$5bn every year (Walker, 2008). The problem related to oil theft has been aggravated by the involvement of politically-motivated militant groups in the illicit oil trade, the expansion of which goes back to the tensions between foreign oil corporations and local ethnic groups (Katsouris and Aaron, 2013). Members of the Niger Delta People's Volunteer Force (NDPVF) have been fighting for oil resources and seeking foreign oil companies' withdrawal from Nigerian oil fields. Under the conditions of constant attacks on their facilities, Eni and Royal Dutch Shell declared force majeure and shut down their activities in Nigeria in spring 2013 (Faucon, 2014).

Similar problems have been present in the MENA (the Middle East and North Africa) region and have emerged in connection to the Arab Spring (Salhani, 2013). Libya's output almost halted in the summer of 2011 as the civil war spread across the country. Syria and Egypt are two other important cases in point in relation to the impact of the Arab Spring on energy security. In Syria, for instance, oil and gas fields have been an important asset for various rebel factions and government forces to fight over since the beginning of the civil unrest (El-Katiri et al., 2014: 7).

The situation with asymmetrical threats in post-Soviet states has also been uneasy since the break-up of the Union of Soviet Socialist Republics (USSR). For example, Russia's oil pipeline monopoly Transneft has been struggling to combat oil theft in the North Caucasus since the times of the first military campaign in Chechnya. Oil theft and illicit oil trade have taken similar forms in Kazakhstan. Kazakhstan's religious extremists seem to be feeding on oil trafficking, having put pressure on the Kazakh government to take the issue of oil theft and oil contraband under serious consideration (Tashkinbayev, 2013).

Mexico, Colombia, Venezuela and Bolivia are among the most important oil producers in Latin America. All of these states have encountered critical levels of oil and gas theft, resulting in billions of dollars of losses. While oil theft has been Colombia's problem for several decades, one of the most recent trends is the use of stolen oil for drug

production (Walsh, 2012).[1] The situation is similar in Peru, where organized gangs siphon oil away from the Northern Peruvian Pipeline and process it into kerosene—one of the must-have substances of cocaine production.

These examples emphasize that CEIs are likely to become even more interdependent and will require much closer interaction between national governments and private sector stakeholders. Governments have an array of choices to select from when it comes down to critical energy infrastructure protection (CEIP). CEIP may range from state provision through collaborative arrangements between the public and the private sectors to market provision of CEIP (Assaf, 2008). Either being unable to effectively provide the security of CEIs, particularly as it relates to threats posed by VNSAs, or seeking cost-effective arrangements, many national governments, even those that have conventionally preferred state-run CEIP strategies, have made attempts to alleviate CEI vulnerabilities through security outsourcing (Dunn-Cavelty and Suter, 2009: 179–187). As the costs of implementing effective prevention strategies have escalated in the background of ongoing reductions in government spending on public sector security, public-private partnerships (PPPs) have been one of the prevalent solutions to CEIP. The importance of private military and security companies (PMSCs) as providers of CEIP has also risen in recent years. Finally, energy security has become a priority for various international organizations, some of which have been actively seeking to acquire some of the key roles in CEIP. Although research has been produced on PPPs and PMSCs, only a few studies have focused on how these new security actors participate in CEIP and what kind of relationship they build with national governments. Also, there seems to be little knowledge generated about the nature and the extent of the involvement of non-state actors in CEIP. Other questions are to be raised as well. What is security outsourcing? Which elements of CEIP are outsourced? To whom are these security functions outsourced? What are the potential consequences of security outsourcing?

This article has the objective of answering some of these questions by offering a qualitative analysis of security outsourcing in the domain of CEIP. We argue that although state protection measures remain essential, they are no longer the most preferable or exclusive parts of CEI security. Non-state actors seem to have been delegated some of the critical functions in CEIP. However, there is little homogeneity with regards to how CEIP is approached in various national contexts. The multiplicity of forms of security outsourcing are presented in a typology that reflects the complexity of security outsourcing as well as captures some of the major contemporary trends in energy security. The typology is supported by four case studies, all of which were chosen to illustrate how different types of security outsourcing manifest themselves empirically as well as how they come into play with political regimes.[2] Although security outsourcing strategies offered in our typology are not always mutually-exclusive, they shed light on the peculiarities of security outsourcing in the CEIP domain—the issue, which has too often been ignored in the mainstream literature on the topic.

The nature of threats to CEIs

Sources of vulnerability that make CEIs susceptible to destruction or incapacitation are manifold. Two types of threats are usually distinguished—accidental and deliberate (Koknar,

2009; Zabyelina, 2013). Accidental threats include excavation, insufficient system capacity, corrosion, mechanical failure (including IT vulnerability that is constituted by risks and failures in computers and/or in the communications system), harsh weather conditions and natural disasters, as well as the risks that come from operators' mistakes in planning, logistics and transfer system control mismanagement. Deliberate threats refer to destruction, disruption and exploitation of (segments of) energy infrastructures by intended attacks that vary from politically-motivated sabotage to profit-oriented theft.

Politically-motivated sabotage relates to any deliberate action aimed at weakening, or withdrawal of, a pipeline network (or any other CEI segment) by actions that include the use of explosives or machinery on a pipeline infrastructure, cyberattacks on pipeline control systems and employee kidnapping. Heightened global awareness of terrorism after the 9/11 terrorist attacks has led many governments and international organizations to tighten security around energy extraction facilities, transportation networks and other related installations as those have become considered as some of the likely targets for terrorist organizations. Moreover, attacking CEIs is relatively easy to arrange: a cheap self-made explosive device located at a critical section of a pipeline has the capacity to upset the operation of the entire CEI for extended periods of time.

Al Qaeda, which had not previously targeted oil facilities, announced a major shift in its strategy in late 2004 by calling on members to '[d]o everything you can to stop the biggest plundering operation in history—the plundering of the resources of the present and future generations in collusion with the agents and the aliens… Be active and prevent them from reaching the oil…' (BBC, 2004). Indeed, attacks on CEIs are an effective way to undermine the authority of the government (or international institutions), cause colossal losses to national (or global) economies, demonstrate strength and capabilities, as well as spread panic and chaos (Koknar, 2009: 19). Importantly, terrorist groups do not always have the primary objective of disrupting CEIs or inflicting casualties. They often pilfer oil from pipelines and sell it on the black market. Revenues generated from illicit trade in oil are often used to finance terrorist organizations. 'It is reasonable to believe that terrorists would target large-capacity infrastructures either for demonstrating their strength through blasts or via tapping that provides them with high-value resources which when sold generate substantial terrorist funding,' explained Lord Jopling at the NATO Parliamentary Assembly (NATO, 2007).

Profit-oriented perpetrators, thus, do not seek to disrupt CEIs. On the contrary, they have demonstrated unprecedented skills of tapping into oil pipelines through 'hot taps' that siphon oil away from the pipeline to illicit reservoirs—the process otherwise known as 'oil bunkering'. Theft of crude oil and its derivative products has led to significant losses that have contributed to poverty and degradation in many developing countries. The negative consequences of oil theft are not only those that incapacitate national economies dependant on contributions from the energy industry, but also those that relate to environmental degradation and damages to communities in the immediate proximity to pipelines. Hot taps often cause pipeline explosions that injure people and send flames and smoke long distances around the hotspot. Oil leaks also occur following both successful and failed attempts to steal oil with an illicit tap. Even if oil leaks do not explode, oil spills damage the environment, becoming an unwelcome

long-term part of the ecosystem. Harm to various species and their habitats, as well as human-cultivated agricultural zones, is one of the most far-reaching environmental effects brought by oil spills (Aroh et al., 2010).

Security outsourcing in CEIP

Exposure to non-traditional threats that are very difficult to respond to with traditional, national security measures, however, has been a powerful stimulus for many national governments to develop security outsourcing strategies. Reforms under the headings of privatization, deregulation and liberalization of security have been in place since the 1990s (Dunn-Cavelty and Suter, 2009). Although with some variance among states, national governments seem to have recognized that contemporary threats to energy security are not limited to geopolitical tensions, supply continuity and price fluctuations, but may also include deliberate attacks by VNSAs. Criminals and terrorists have indeed demonstrated that they are powerful enough to affect not only the states in the near proximity to hotspots but also more distanced regions. This has led to the merging of domestic and external problems, whereby 'no single country is either immune to effects or able to predict outcomes if neighbours suffered from serious infrastructure disruptions' (Pursiainen, 2009: 733). In this respect, several analysts have made observations on restructuring of public–private relations in the domain of security, whereby security is 'being transformed from a service for the public or common good into a privately provided service' and 'from vertical, centralized government to horizontal, fragmented security governance' (Tzifakis, 2012: 3).

What is referred to in this article as *security outsourcing* relates to the reallocation of state authority to non-state actors. Security outsourcing is a generic term that incorporates a variety of strategies, which are used by national governments to adjust to the new generation of risks in the energy security domain, mitigate shortages of skills and expand the pool of security resources available to them. There are several benefits to security outsourcing. First, security outsourcing reduces capital and operating expenses by eliminating the need to hire and train specialized staff and purchase dedicated equipment. When private security companies are hired, the provider is responsible for all administrative costs and the costs associated with ongoing training, licensing of its workers, tracking and renewing licenses, handling workers' compensation claims, providing supervisory oversight and, if necessary, handling disciplinary actions. Second, private security companies also provide customized security solutions, thus maximizing the efficacy of the overall security outsourcing program. They possess specialized knowledge and deploy proprietary security technology.

Given the multiplicity of forms of security outsourcing, this article offers a typology that has been developed based on the following criteria: (a) the *depth* of involvement of the state in security outsourcing; and (b) the *outreach* of security outsourcing. By 'depth' we mean the profundity of the state in rendering assistance via PPP schemes. The criterion of 'outreach' helps to identify whether the state delegates some of its security functions to domestic or external actors.

Based on these two criteria, four categories of security outsourcing can be identified:

1. *Security outsourcing to national oil companies* (NOCs) refers to situations, in which strategically important corporate actors that are totally or majority owned by the state are delegated advanced privileges, including military ones. In this case, the state mandates clear and precise security standards through legislation and rigidly monitors the activities of security companies. States allocate additional military powers to NOCs so that the jurisdiction and the powers of (selected) corporations that are usually strategically and economically critical to the state are expanded. In other words, this category refers to cases in which corporations are extensions of state authority by other means such as corporate armies. NOCs are thus granted exclusive discretionary powers and independence to develop their own security arrangements. This model is 'interventionist' because it refers to the formation of government-owned corporate armies, which, although constituting private sector entities, are in fact controlled by the state. The state delegates the responsibility to provide CEIP in de jure terms but preserves the dominant position in this domain. Examples include Russia's empowerment of state companies Gazprom and Transneft, Kazhakhstan's initiatives to create security forces for KazMunaigaz, and Saudi Arabia's decision to create industrial security forces that would protect oil pipelines independently from other state security units.
2. *Security outsourcing to PMSCs* refers to the employment of PMSCs[3] by multinational oil companies (MOCs) in situations when their host governments either fail or refuse to take responsibility for CEIP. Stimulated by the demand, PMSCs have emerged to fill in the (in)security 'gap'. Security has thus been transformed from a public good provided and distributed by the state into a privately provided service. From this perspective, security is a commodity that is bought and sold in the security market. The role of the government is transformed into the agency that encourages and induces such market transactions. This model represents a situation in which the state engages in consultation with PMSCs, whereby the role of the state shifts from coercive control towards more lenient approaches such as monitoring. Some examples of the 'hands off' type of security outsourcing include Nigeria, where activities of most foreign energy companies are protected by private security firms. Mexico can be considered as another example following the Mexican government's reforms in the energy sector that effectively gave the green light for private investors—both foreign and domestic—to enter the Mexican energy market in 2014.
3. *Security outsourcing to subnational actors* refers to the empowerment of local actors when the national army and security services have little access to remote areas and fail to establish control in some parts of the state. Attacks against CEIs can be a good indicator of the ability of the state to exercise the monopoly of force over its territory. In turbulent regions, in particular where political claims from non-state actors have persisted for a long time, the population may transfer allegiance to alternative centers of authority such as ethnic groups, clans and tribes. These informal groups have often substituted the state by taking over the administration of basic social, judicial and political matters, including the protection of CEIs and the redistribution of revenues these infrastructures generate. Forming

alliances with such non-state groups, especially in cultures with strong attachment to traditional forms of social organization may be one of the ways of enhancing CEIP. Seeking arrangements with local groups is likely to be an option for fragmented states, in which the government has not managed to establish authority throughout its territory. With little support in peripheral areas, the government has to negotiate various matters, including the protection of energy facilities, with local leaders. Some examples of this type of CEIP include Iraq, South Sudan and Libya. Local tribes and clans have control over extended territories and claim the ownership of energy resources located on those territories. Extracting energy resources without the consent of tribal leaders is difficult to imagine in these contexts. Thus, members of tribes are often hired by foreign companies in the capacity of security providers.

4. *Security outsourcing to supranational actors* refers to cooperation among states that goes beyond intergovernmental agreements. The 'supranational' feature may refer to an intra-governmental agreement on a regional or a global level, whereby member states transcend national boundaries to share in the decision-making on issues pertaining to common security concerns. In this model, there is an understanding of the benefits through an approach focused on cooperation, collaboration and mutual assistance. Different actors within and between states and across regions collaborate. This includes strengthening local government and building partnerships between the private sector and the civil society. There has been some emerging consensus that international organizations may play an important role in resolving some of the key issues affecting cross-border flows of energy ranging from measures to improve the efficiency of energy use to upgrading the security of CEIs. Achieving CEIP, particularly in light of post-9/11 security, seems to have become one of the objectives for supranational governance. The North Atlantic Treaty Organization (NATO) and the Organization for Security and Co-operation in Europe (OSCE), for instance, have reaffirmed the central role of energy security on their agendas, having actively engaged in energy dialogues and inter-regional and inter-institutional cooperation, as well as in joint activities and multilateral energy initiatives. They have also provided technical assistance, training and expertise to national governments. The European Union's (EU) role as a security provider has been reaffirmed more recently. It goes back to the European Council's statements in the late 2000s that raised the need for an integrated approach to security, for closer interaction between internal and external security actors and for combining civil and military capacities within the EU and beyond.

Towards an empirically grounded typology of CEIP

A typology is an organized system of categories that makes a contribution to 'concept formation and to the construction of categorical variables' (Collier et al., 2008: 152). A typology analysis thus requires careful review of the raw data before deciding in which cell of a typological matrix each data point should be classified. The categories used in a typology should be mutually exclusive to reduce ambiguity in classifying data (Collier

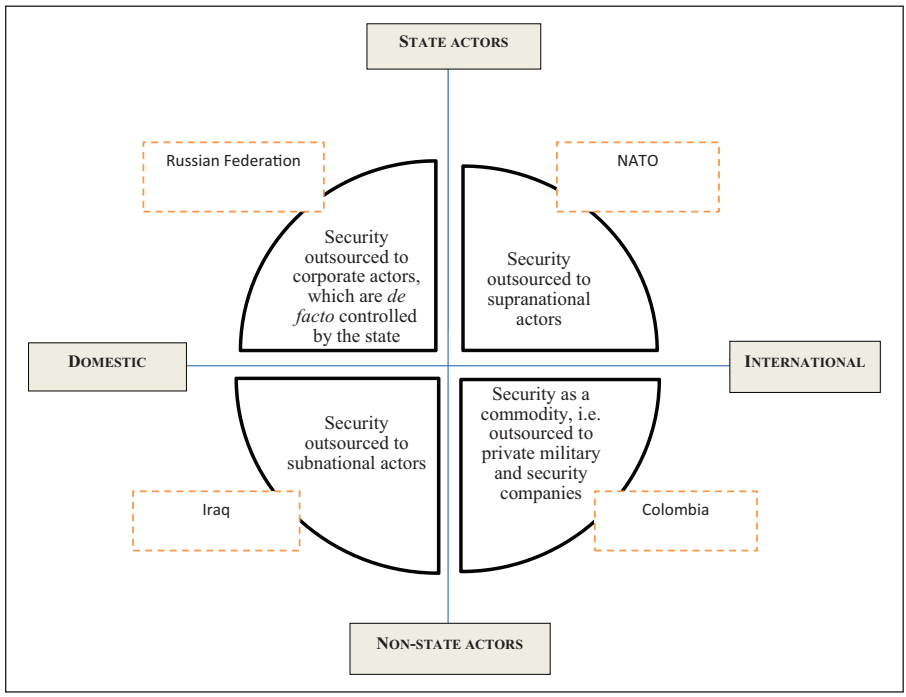

Figure 1. Security outsourcing in the protection of CEIs.
Source: authors' elaboration.

et al., 2008). A typology analysis serves several important functions: descriptive, classificatory and explanatory (Elman, 2005). First, typologies provide detail-rich descriptions of their categories. Second, they assign cases in the raw qualitative data, whereby the latter are classified under one of the categories in a typology. Finally, typologies allow researchers to make comparisons and assess whether the data are consistent with relevant theories (Collier et al., 2008).

Following on from the previous section, the typology of security outsourcing in CEIP incorporates four analytical categories [Figure 1]:

(a) Security outsourcing to national oil companies;
(b) Security outsourcing to private military and security companies;
(c) Security outsourcing to subnational actors;
(d) Security outsourcing to supranational actors.

In order to illustrate how each of these categories manifest themselves in empirical terms, this section offers four brief case studies. The aim of investigating these cases is to draw a detailed picture of each case's qualitative particularities as it relates to various types of security outsourcing in CEIP.

All cases have been selected purposefully. Because purposive selection 'has a logic and power… and provides rich information' Patton (1990: 169), we have selected the

most information-rich and interesting cases that fit our analytical framework. Purposeful sampling has its limitations, particularly in relation to the generalizability of findings, but it helps to achieve the purpose of this study, which is theoretical rather than empirical. The data gathering approach, which is not systematic and is primarily based on descriptive and inferential data, is also appropriate for the goals of this article. The four case studies offered below illustrate each of the types in their specific empirical context.

Militarization of Russia's Gazprom and Transneft

While statistics on the amount of revenues generated from oil theft and oil contraband are largely unavailable, Chechen warlords Shamil Basayev and al-Khattab allegedly collected oil from illicit refineries in Chechnya during the Second Russo-Chechen War (Zabyelina, 2013). After 2004, when pro-Moscow President Akhmad Kadyrov reinforced the positions of federal forces in the republic, the control over oil processing and transportation was split between Kadyrov's militia and Russian soldiers. According to some sources, there was a good level of cooperation between local groups, who extracted crude oil and processed it into petrol, and the Russian military responsible for transportation of illicit fuel outside of the republic (Zabyelina, 2013). Following pressure from Moscow, Ramzan Kadyrov, Akhmad Kadyrov's political successor and son, used harsh tactics to shut down illicit oil refineries in Chechnya. Whereas this move has been relatively successful in Chechnya, oil smuggling has become a serious problem in the neighboring republic of Dagestan (Zabyelina, 2013). In 2011, Transneft complained to Dagestan's then President Magomedislam Magomedov, expressing concerns over the security situation (Centre for the Study of Regional Problems, 2011).

Reaffirming the dangerousness of the situation with the security of pipelines in the Russian Federation, in 2006 the State Duma passed a bill that allowed energy companies Gazprom and Transneft to create corporate armies with expanded powers and privileges. According to the latest amendment of the Federal Law of 13 December 1994 'On Supplies for Federal Needs' adopted on 24 July 2007, Gazprom and Transneft are authorized to form specialized paramilitary units tasked to protect the pipelines. Without any reference to terrorist or criminal threats, Art. 4.1.1 of the Law states that strategic enterprises and joint-stock companies and their subsidiaries, and the owners of the Unified Gas Supply System, are strategic corporations, which, after obtaining the license in the Ministry of Internal Affairs, have the right to acquire weapons in line with the Federal Law of 13 November 1996 'On Armaments'. This law's Art. 12 (amended on 22 December 2008) authorizes these 'strategic corporations' to purchase and carry weapons for the purposes of the mission and for self-defense.

In 2011, the Ministry of Energy recommended that Gazprom and Transneft be given the right to create their own security police—*vedomstvennaya okhrana*—a special kind of armed unit employed by or for governmental agencies to provide security services to those agencies' properties. Given that the security management of Gazprom and Transneft is regulated not by the law on 'Private Security' of 14 March 1992 but by the law on 'Security Police' of 14 April 1999, the powers of corporate security units are much wider than those of private security agencies. Corporate security units are authorized to use force 'while in pursuit of individuals who have committed criminal or civil offenses at

the facilities under guard' (Hurst, 2010: 62). In this way, the law does not restrict weapons possession and use within the area they are tasked to protect. They conduct arrests, body and vehicle searches, both on and off their assigned premises. According to the data released by Rosbalt, 91% of Gazprom and its subsidiaries' objects are protected by its own corporate security units (Rosbalt, 2007). Approximately 5.5% are guarded by external private security companies, leaving only 3.5% to mixed, i.e. public–private security units (Rosbalt, 2007).

Going beyond the militarization of Russia's key state-owned oil and gas companies, the Duma has also supported tougher punishment of crimes against CEIs. In doing so, the list of criminal offences related to theft has been expanded to include theft of oil resources (Criminal Code of the Russian Federation (CCRF), Art. 158, par. 3). Theft of energy resources has become punishable by a fine of RUB 100,000 to 500,000 (ca. US$3000–14,000) or an amount calculated according to the salary of the offender, or by imprisonment for a period ranging between two and six years, in addition to the fine. Damages to oil or gas pipelines have been criminalized too (CCRF, Art. 215, par. 3). Depending on the severity of the damage, the fine ranges between RUB 400,000 to 500,000 (ca. US$12,000–14,000) or an amount calculated according to the salary of the offender through the period of seven months to one year, or by imprisonment for between two to five years.

NATO and CEI security initiatives in the South Caucasus

The involvement of NATO in CEIP is a recent trend that goes back to the end of the Cold War. The first public reference to energy security, and CEIP in particular, as the NATO sphere of interests was introduced, was in the NATO New Strategic Concept in April 1999 (NATO, 1999). In 2008, there were even discussions at the ad hoc level about the possibility of expanding Chapter V of the 1949 North Atlantic Treaty to provide support to member states under threat of disruption to their energy supplies. Despite the fact that these discussions were largely rhetorical and did not lead to any legal change, they marked a significant shift closer towards NATO's involvement in CEIP. Information and intelligence sharing, advancing international and regional cooperation, and providing training and technological assistance have been identified as the key areas where NATO members were willing to provide added value to CEIP (Umbach and Nerlich, 2008: 275).

NATO's New Strategic Concept adopted during the Lisbon Summit in 2010 defined a wider role for energy security as one of the primary tasks of the Alliance. Accordingly, 'as a larger share of world consumption is transported across the globe, energy supplies are increasingly exposed to disruption,' (NATO, 2010: 12) therefore 'increasing energy needs will further shape the future security environment in areas of concern to NATO and have the potential to significantly affect NATO planning and operations' (NATO, 2010: 13). The development of a strong connection between operational and strategic planning of the Alliance and 'the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines' has been continuously discussed (NATO, 2010: 17).

Given the importance of the US–NATO geo-strategic interests in the South Caucasus and the geo-political turbulence caused by the 2006 Russia–Ukraine gas disputes and the

2008 Russia–Georgia conflict in South Ossetia, NATO's direct involvement in CEIP in the South Caucasus was repeatedly discussed as well. In a recent report to the US Senate's Committee on Foreign Relations (2012), the US strategic interests in linking the nations of the Caspian Sea region with European and global markets were clearly expressed, welcoming more active NATO involvement in the South Caucasus, where it could 'improve our ability to project power over long distances' (US Senate, 2012: 59) and 'address the energy insecurity of several NATO allies' (US Senate, 2012: 21).

While there were discussions about the possibility of creating specialized NATO troops for the protection of the Baku-Tbilisi-Ceyhan and the South Caucasus Pipeline, it was eventually recognized as unworkable. As Koranyi (2013) suggests, a direct NATO involvement in pipeline protection in the South Caucasus is difficult to imagine, since 'the regional repercussions, the possibility of tipping NATO forces against the The Collective Security Treaty Organization (CSTO) are simply too risky. Some sort of technical assistance and training provided by NATO allies might be more feasible.'

Regardless of the slow progress in NATO's involvement in CEIP in the South Caucasus, NATO forces have nevertheless provided training, operational support, and surveillance equipment. Several training programs on maritime security and the protection of energy facilities in the South Caucasus were held within NATO's Partnership for Peace Program. For example, seminars on energy security and protection of energy infrastructure and emerging security challenges were held in Georgia in 2010 and 2011 under the auspices of the Euro-Atlantic Partnership Council (MFA of Georgia, 2013).

Moreover, even if the involvement of NATO forces is rather limited, it is noticeably complemented by the involvement of the US government in the region. The US Global Critical Energy Infrastructure Protection (G-CEIP) strategy, launched in 2006, is a good example of external actors' involvement in CEIP in other states. Since any disruptions to CEIs in one state may lead to serious consequences in other parts of the world, the United States has also allocated training and equipment support for CEIP. The United States provides assistance to Azerbaijan in the protection of offshore platforms and in other aspects of maritime security training. In Georgia, the United States offered training to a local battalion tasked to protect the Baku -Tbilisi -Ceyhan (BTC) pipeline (Sloan, 2007).

The role of private security companies in Colombia

Long-lasting internal struggles between the central government and guerrilla groups have seriously impeded the proper functioning of the oil sector in Colombia. Leftist FARC and the ELN, as well as the rightist United Self-Defence Forces of Colombia (AUC) have attacked Colombia's CEIs. Despite the fact that the Colombian government has taken a number of CEIP initiatives in recent years, recurrent guerrilla attacks, however, continue to threaten the Colombian government and gravely challenge the activities of MOCs widely present in the country (EIA, 2013).

Colombia's model of CEIP is based on the division of responsibilities between facility operators and the host government, the so-called PPPs. In doing so, the Colombian government mandated that the facility operator takes responsibility for CEIP within the perimeter of its operations, while the host government would provide security outside the perimeter. In June 2013, Defence Minister Rodrigo Rivera admitted that 'the sharp

growth in Colombia's oil sector has made it impossible for the military and the police to adequately protect all oil installations, many of which are located in remote regions near guerrilla strongholds' (Alseema, 2011). He urged oil companies to invest in 'their own private security forces to help government troops combat a wave of attacks and kidnappings' (Alseema, 2011). Although foreign oil companies operating in Colombia were also heavily taxed in addition to paying regular taxes like companies in other sectors, they had little trust in the central government's ability to stick to its security obligations and accepted the costly necessity to employ PMSCs.

Since the 1990s, the Cusiana and Cupiaga oil fields and the Ocensa pipeline developed by British Petroleum (BP) were repeatedly attacked by rebel armed groups. Not limiting itself to cooperation with the Colombian army and local police, BP cooperated with paramilitary units and employed PMSCs to protect its facilities and employees. Since the 1990s, BP has contracted Defence Systems Colombia (DSC)[4] to provide training and equipment for Ocensa protection in Colombia.[5] In 1996, DSC trained the Colombian police that were deployed at Colombian branches of BP. Despite BP denying any ties with DSC, the collaboration between the two entities in the 1990s was reported by several journalistic investigations. One of them provided evidence about serious human rights abuses committed by the PMSCs in the line of duty. In 1997, *The Guardian* disclosed that BP's 'internal security department' was run by 'a secretive Anglo-American company, Defence Systems Limited,' which worked together with the 14th Brigade under secret agreement between BP and the Colombian Defence Ministry (Gillard et al., 1998). According to open sources, 'this brigade has one of the worst human rights records in Colombia's dirty war. Lawyers have proved the involvement of a brigade commander and officers in one of Colombia's massacres in Segovia in 1988 when more than 90 men, women and children were attacked and 43 of them killed' (Gillard et al., 1998). In another case in April 1996, former employees of DSC were accused by human rights organizations of involvement in killings, beatings and arrests while working for BP (Alamario, 1997). The accusation had not been recognized until 2006, when a group of Colombian farmers reached an agreement with BP in the High Court in London, according to which BP compensated the victims for harassment committed by the paramilitary troops employed by the company to protect the Ocensa pipeline (Verkaik, 2006).

The US Occidental Petroleum Corporation has been an active player in the Colombian energy sector since the early 1980s, when the Caño-Limón oil field was discovered. Faced with the need to cover the Colombian government's breach in providing security, Occidental Petroleum also contracted globally-operating PMSCs. AirScan, a US private security company that provides airborne surveillance and security operations for both governments and the private sector, was responsible for protecting Occidental Petroleum's facilities in close collaboration with the Colombian military. AirScan and Occidental Petroleum were also subject to suits for the incident in 1998 when the village of San Domingo was mistakenly identified by AirScan as a guerrilla target.[6]

Tribes and CEI protection in Iraq

In the 1990s in Iraq, organized criminal gangs with alleged connections to Saddam Hussein used to smuggle oil in breach of UN sanctions. Traditional trade routes

throughout the Persian Gulf and the Middle East were adapted for these operations. Trucks sent to Turkey, Jordan and Syria, and boats going through the Persian Gulf were used to bring in illicit revenues for the Ba'athist government. Following the US military operations in Iraq in 2003, these activities not only continued but also intensified (Pan, 2013). The disintegration of the Hussein regime was accompanied by intense fighting over oil production sites. Some of the machine-gun attacks in 2014, for instance, left parts of Iraq's main oil refineries in flames as militants, including hundreds of Islamic State in Iraq and the Levant (ISIL) fighters, battled against the Shiite Muslim-dominated government to seize more territory (Nabhan, 2014).

The involvement of tribes in CEIP initiatives in Iraq is a good example of hybrid alliances between central authorities, specialized oil protection units and tribes. Iraq gradually took control of its oil industry from international oil companies in a process which began in 1961 and ended in 1975 with the complete nationalization of assets and oil production in the country. Since the 1990s UN Security Council's embargo created the environment, in which colossal amounts of oil were stolen and sold as contraband, many of the parties involved in the illicit trade in oil benefited from UN sanctions. Power-sharing arrangements between the Saddam Hussein government and tribes enabled them to circumvent sanctions and continue to export oil, thus bringing a certain level of temporary peace (Taylor, 2005: 8).

Following the 2003 UN Security Council's Resolution that removed the sanctions and established control of the Coalition Provisional Authority (CPA) led by the US and the UK, the informal agreement between the Saddam government and local tribes was upset. Partially because the tribal leaders were scared of the US taking over Iraq's oil industry or because their autonomy and access to oil resources were restricted by the CPA, pipelines were regularly bombed from 2003 onwards. The CPA created specialized oil protection units. The effectiveness of these were, however, very limited because of the symbiosis between the guards and the smugglers, not least because of the fact that they were members of the same tribe. For example, Al-Juburi was employed by the Defence Minister to protect the Baiji-Kirkuk pipeline in 2004. Despite his mission, attacks intensified in 2005 because one of Al-Juburi's men allegedly put 'ghost soldiers' on his payroll and kept the money that was supposed to be used for their salaries and equipment (Williams, 2009).

At this point, it should be reiterated that Iraq's tribal system (similar to other states in the Arab world) is fundamental for the organization of social life. A tribe is a form of political identity based on common descent. Tribes are conventionally considered the central organizing principle of Iraqi society today. Although sheikhs are consumed by the daily struggle to survive and to preserve the authority and privileges from central government, rural areas largely remain under their exclusive control. As Williams points out, 'in such cultures, positions in government or law enforcement are seen not as opportunities for public service but as opportunities to meet family, tribal, or clan obligations' (Williams, 2009: 203).

Following privatization of the oil industry in 2007 and 2008, the Iraqi government held a series of open bidding rounds for oil field development contracts to foreign companies, including ExxonMobil, Royal Dutch Shell, Eni, Gazprom and Lukoil. With foreign companies' direct involvement, the Iraqi government seemed to have no choice but to seek an agreement with tribal leaders. Considerable efforts have been in place to

enhance cooperation between tribes, the central government and foreign companies. Since 2008, the forces fighting oil theft have been recruiting young men from tribes. The aim was to achieve security through creating job opportunities and stimulating local development in oil-producing areas (Phillips, 2008).

Conclusion

This article has studied various dimensions of security outsourcing in the protection of CEIs. The findings provide the grounds for a typology of security outsourcing strategies that charts the key players in the protection of CEIs, which are: (a) public authorities; (b) international organizations; (c) private security and military companies; and (d) local groups such as tribes or other social organizations. By studying various types of security outsourcing, the article contributes to an understudied area of research that is interesting from both the academic and policy points of view.

Each type of security outsourcing offered in the typology has been supported with an empirical case study. Among the four cases studied in the article, the Russian Federation is the case in which the state maintains robust oversight of CEIs and their operators. Despite on-going debates about the state being subject to various changes in the era of globalization, the monopoly of force remains an indispensable part of the national agenda that the Russian government is reluctant to delegate to any other authority. Having faced limited ability of intelligence agencies and police to prevent or at least reduce oil thefts through the whole country, the Russian government has supported the militarization of its key energy corporations, Gazprom and Transneft, having nevertheless opted for the public authority and the military to play a greater role in the protection of CEIs.

The wider consequences of the militarization of Gazprom and Transneft are difficult to predict. On the one hand, the two companies could considerably help to reduce the number of attacks on Russia's CEIs. They could also help to boost the quality of Russia's security agencies, thus contributing to the state's domestic stability far beyond their roles as energy corporations. On the other hand, the amendments of Russia's federal laws discussed in this article lack important details such as those that relate to restrictions on the size of corporate troops and the types of weapons they are authorized to carry. Moreover, it should be acknowledged that before militarizing energy companies, one should try to deal with corruption in the public and private sectors. Stealing oil under pressure requires professional knowledge that is rarely available to outsiders. Most oil thieves depend on collaboration with (ex)-employees of energy companies as providers of management information and technical expertise for a share of illicit profits.

Although working with tribes in the case of Iraq may help to stabilize the post-conflict situation in this country, forming alliances with informal groups may bring some risks as well. One is that the alliance with local groups may lead to tipping local tribal influence in favor of one clan over another. Growth in power and influence of several tribes, especially those that control the areas in proximity to pipelines, can affect the domestic balance of power by triggering armed clashes between tribes. Another risk is that tribes as established social organizations supporting the interests of their members may downplay the role of the national government and lead to the rise in power of sheikhs.

The involvement of private security actors in CEIP has been the mainstream trend in many countries. Although private companies have demonstrated relative success in coping with the task of protecting energy facilities and long-distance pipeline networks, several areas of public–private interaction have proved problematic in practice. Security outsourcing to PSMCs in such a sensitive area raises concerns about corresponding to the principles of accountability and legitimacy. Providing CEIP as a commercial good has led to a number of serious human rights violations. Although many private energy corporations seek the 'hands off' approach in their operations and are often very reluctant to share any internal information (particularly the one on their vulnerabilities), it is necessary that national governments conduct a more in-depth assessment of potential inroads into how PSMCs can be professionalized. It is also necessary to identify the ways national law enforcement agencies can better oversee the activities of PSMCs hired by foreign companies.

Despite energy security and the protection of critical infrastructures being novel areas of NATO competence, the Alliance has been forging its involvement in this domain in recent years. Although NATO's cooperation with national governments in the South Caucasus has been relatively successful and all parties have developed regulation and resilience programs for the protection of CEIs, the case of NATO's involvement in this region reveals several challenges that may also appear in other regions of NATO presence as well. One of them is the need to promote inter-regional dialogues at all levels among representatives of Georgia, Armenia, Azerbaijan and Russia. Until regional disagreements at the ad hoc level, especially those between Russia and Georgia in the aftermath of the 2008 South Ossetia War over the status of South Ossetia and Abkhazia and the one over Georgia's aspirations to join NATO, are resolved, inter-institutional dialogue is not likely to happen. Finding an appropriate balance of interest for different actors along the entire cross-border energy chain is fundamental in this context.

In terms of future research, it is recommended that scholars pay attention to studying the relationship between the choice of a model of security outsourcing and domestic institutional arrangements. For example, states with powerful national energy companies and the nationalized (or quasi-nationalized) energy industry, such as the Russian Federation and Kazakhstan, are likely to adopt the 'interventionist' model of security outsourcing. With reference to the 'hands off' model of security outsourcing, the extensive reliance of national governments on PMSCs is likely to be adopted in developed states with a well-established and well-developed private sector such as the USA and the UK. PMSCs are also expected to be key players in countries with a long history of presence of MOCs. Despite high costs and few incentives on behalf of the host government to do so, MOCs hire PMSCs because host states are either incapable or unwilling to provide sufficient guarantees and security so that MOCs could operate without any impediments and/or losses. This model of security outsourcing is characteristic of conflict-ridden and poorly-governed states with energy resources such as Colombia, Nigeria and Mexico. Finally, the involvement of social organizations, for instance tribes and kinship groups, in protecting CEIs is a likely outcome of much more deep-seated socio-cultural processes and state-formation patterns. These research areas have been largely neglected in mainstream academic and policy

literature despite their importance for understanding the complexity of energy security and the role of security outsourcing in it.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes

1. A kilogram of cocaine requires between 280 and 325 liters of gasoline to process.
2. All of the case studies in the typology refer to the protection of critical oil and gas infrastructures. Thus, we have excluded nuclear energy and electricity networks because of the limited scope of the article. The analysis of cyberattacks on CEIs has also been omitted for the reason that this topic requires a detailed analysis of its own and could not be adequately covered in this article.
3. The discussion on various types of PMSCs goes beyond the scope of this article. For more information about typologies of PMSCs see: Kinsey (2006); Alexandra et al. (2008); Tzifakis (2012).
4. DSC is one of the subsidiary firms of Defence Systems Limited (DSL)—one of the leading private providers of security services internationally.
5. Although many reports indicated to the contrary, BP has never recognized having any connections with DSC.
6. Neither Occidental Petroleum nor AirScan were found to be responsible for this incident.

References

Alamario J (1997) British run private armies in Colombia. *Executive Intelligence Review*, 22 August, pp. 67–71.

Alexandra A, Caparini M and Baker D-P (eds) (2008) *Private Military and Security Companies: Ethics Policies and Civil-Military Relations*. London: Routledge.

Alseema A (2011) *Oil companies in Colombia say security is government's job*. Colombia reports, 10 August. Available at: http://colombiareports.co/oil-companies-in-colombia-say-security-is-governments-job/ (accessed 8 August 2013).

Aroh KN, Ubong IU, Eze CL, et al. (2010) Oil spill incidents and pipeline vandalization in Nigeria: impact on public health and negation to attainment of Millennium development goal. The Ishiagu example. *Disaster Prevention and Management* 19(1): 70–87.

Assaf D (2008) Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection* 1: 6–14.

BBC (2004) Excerpts of Bin Laden message. *BBC*, 16 December. Available at: http://news.bbc.co.uk/2/hi/2751019.stm

Centre for the Study of Regional Problems (2011) Vorovstvo nefti v Dagestane prevratilos v biznes gosudarstvennogo masshtaba [Oil thievery in Dagestan has become a business of national importance], 23 August. Available at: http://www.rf-region.ru/articles/360.htm (accessed 5 September 2013).

Collier D, Laporte J and Seawright J (2008) Chapter 7. Typologies: forming concepts and creating categorical varieties. In: Box-Steffensmeier JM, Brady HE and Collier D (eds) *The Oxford Handbook of Political Methodology*. Oxford: Oxford University Press, pp. 153–173.

Dunn-Cavelty M and Suter M (2009) Public-private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection* 2: 179–187.

EIA (2013) U.S. Energy Information Administration. Colombia, Background. Available at: http://www.eia.gov/countries/cab.cfm?fips=CO (accessed 10 September 2013).

El-Katiri L, Fattouh B and Mallinson R (2014) *The Arab uprisings and MENA political stability: implications for oil & gas markets*. OIES Paper: MEP 8. Oxford: The Oxford Institute for Energy Studies (OIES).

Elman C (2005) Explanatory typologies in qualitative studies of international politics. *International Organization* 59(2): 293–326.

Faucon B (2014) Italy's Eni shuts Nigeria pipeline after sabotage: unrest and theft rattle oil industry in West African nation. *The Wall Street Journal*, 10 January. Available at: http://online.wsj.com/news/articles/SB10001424052702304347904579312630260095784 (accessed 10 May 2014).

Gillard M, Gomez I and Jones M (1998) BP hands 'tarred in pipeline dirty war'. *The Guardian*, 17 October. Available at: http://www.theguardian.com/world/1998/oct/17/1

Hurst C (2010) The militarization of Gazprom. *Military Review*, September–October. Available at: http://fmso.leavenworth.army.mil/documents/Militarization-of-Gazprom.pdf

Katsouris C and Aaron S (2013) *Nigeria's Criminal Crude: International Options to Combat the Export of Stolen Oil*. London: Chatham House.

Kinsey C (2006) *Corporate Soldiers and International Security: The Rise of Private Military Companies*. London: Routledge.

Koknar A (2009) The epidemic of energy terrorism. In: Luft G and Korin A (eds) *Energy Security Challenges for the 21st Century: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO, LLC, pp. 18–31.

Koranyi D (2013) I can hardly imagine a direct NATO involvement in protecting BTC and BTE. *News.Az*, 31 January. Available at: http://news.az/articles/economy/75900

MFA of Georgia (2013) *NATO-Georgia Relations*. Ministry of Foreign Affairs of Georgia. Available at: http://www.mfa.gov.ge/index.php?sec_id=453&;lang_id=ENG (accessed 11 September 2013).

Nabhan AA (2014) Main Iraq oil refinery in flames after rebel attack. *The Wall Street Journal*, 18 June. Available at: http://online.wsj.com/articles/main-iraq-oil-refinery-in-flames-after-rebel-attack-1403080397

NATO (1999) The Alliance's strategic concept, 24 April. Available at: http://www.nato.int/cps/en/natolive/official_texts_27433.htm (accessed 14 August 2013).

NATO (2007) *The protection of critical infrastructures*. 162 CDS 07 E REV 1, NATO Parliamentary Assembly Special Rapport by Lord Jopling. Available at: http://www.nato-pa.int/default.asp?SHORTCUT=1165 (accessed 11 August 2013).

NATO (2010) *Strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation adopted by heads of State and Government*. The NATO summit in Lisbon, 19–20 November.

Pan I (2013) Why unrest in Libya has persistently disrupted oil production. *The Market Realist*, 18 September. Available at: http://marketrealist.com/2013/09/unrest-libya-caused-persistent-disruptions-oil-production/

Patton MQ (1990) *Qualitative Evaluation and Research Methods*. 2nd ed. Newbury Park, CA: Sage.

Phillips K (2008) Iraq recruits tribes to combat oil smugglers. *CNN*, 5 March.

Pursiainen C (2009) The challenges for European critical infrastructure protection. *Journal of European Integration* 31(6): 721–739.

Rosbalt (2007) Korporativnyi soldat [The corporate soldier]. *Rosbalt*, 5 July.
Rosser A (2006) *The political economy of the resource curse: a literature survey*. IDS Working Paper 268. Brighton: Institute for Development Studies (IDS).
Salhani C (2013) Oil well, oil facilities and pipelines: new targets in a new war. *The OilPrice.Com*, 20 August.
Sloan E (2007) *NATO Approaches to Energy Security: Future Options, Challenges and Directions* (Critical Energy Infrastructure Protection Policy Research Series). Canadian Centre of Intelligence and Security. Available at: http://www3.carleton.ca/cciss/res_docs/ceip/sloan.pdf (accessed 13 August 2013).
Tashkinbayev T (2013) Oil trafficking funds Kazakhstan's religious extremists. *Tengri News*, 1 June.
Taylor R (2005) *Tribal Alliances: Ways Means, and Ends to Successful Strategy*. Strategic Studies Institute (SSI). Available at: http://www.au.af.mil/au/awc/awcgate/ssi/tribal.pdf
Tzifakis N (2012) *Contracting Out to Private Military and Security Companies*. Brussels: Centre for European Studies.
Umbach F and Nerlich U (2008) Asset criticality in European gas pipeline systems—increasing challenges for NATO, its member states and industrial protection of critical energy infrastructure. In: Gheorghe A and Muresan L (eds) *Energy Security: International and Local Issues, Theoretical Perspectives, and Critical Energy Infrastructure*. Dordrecht: Springer, pp. 273–304.
United Nations Office on Drugs and Crime (UNODC) (2009) *Oil Theft Lubricates Corruption in West Africa*. Vienna: UNODC.
US Senate (2012) *Energy and security from the Caspian to Europe*. Minority staff report prepared for the Committee on Foreign Relations, 112th Congress, 2nd Session, 12 December. Available at: http://www.foreign.senate.gov/imo/media/doc/Energy%20and%20Security%20from%20the%20Caspian%20to%20Europe.pdf
Verkaik R (2006) BP pays out millions to Colombian farmers. *The Independent*, 22 July. Available at: http://www.independent.co.uk/news/world/americas/bp-pays-out-millions-to-colombian-farmers-408816.html
Walker A (2008) 'Blood oil' dripping from Nigeria. *BBC*, 27 July. Available at: http://news.bbc.co.uk/2/hi/africa/7519302.stm
Walsh H (2012) Colombia combats Martians robbing crude for cocaine labs. *Bloomberg*, 5 October. Available at: http://www.bloomberg.com/news/2012-10-05/colombia-combats-martians-robbing-crude-oil-for-cocaine-labs.html
Williams P (2009) *Criminals, Militias, and Insurgents: Organized Crime in Iraq*. Strategic Studies Institute (SSI). Available at: http://www.strategicstudiesinstitute.army.mil/pdffiles/pub930.pdf
Zabyelina Y (2013) Assessing the vulnerability of cross-border energy infrastructures: pipeline sabotage and contraband of energy resources. *International Journal of Energy Security and Environmental Research* 1(1): 81–97.

Author biographies

Yuliya Zabyelina is an Assistant Professor at the Department of Political Science at John Jay College of Criminal Justice, CUNY, New York. Her research interests include security governance and various aspects of the study of transnational organized crime and corruption from global and local perspectives. Before moving to the United States, she was a Newton Research Fellow at the University of Edinburgh in Scotland and has completed several visiting fellowships in North America and Europe.

Irina Kustova is a PhD candidate at the School of International Studies, University of Trento, Italy and holds an MA in European Studies from Maastricht University. She has been a trainee at the Agency for Cooperation of Energy Regulators (ACER), and has been a visiting researcher at the King's College London and the Energy Research Institute of the Russian Academy of Sciences. Her expertise lies in the area of the European gas market, energy governance, EU integration and Russian domestic oil and gas sectors.