Little is known and even less is understood about the role of the Organization for Security and Cooperation in Europe (OSCE) in the field of energy security. Probably best known for its election monitoring activities, the OSCE has a mandate to promote dialogue on energy security, including at the expert level, involving producing, transit and consuming countries. This mandate is both instructive and important. Among the organization's 56 member states, the OSCE is the only European multinational organization that includes both European and North American net energy producers and exporters such as Canada, Kazakhstan, Norway, the Russian Federation, and Turkmenistan along with some of the world's largest energy consuming states such as the United States, Russia, and Germany. It also includes among its members key transit states for European energy supply including Belarus, Ukraine, Poland, Azerbaijan, Georgia, and Turkey. The OSCE is therefore unique in that it provides a platform for dialogue specifically within a European context between energy producers, consumers and transit states that are counted as full members of the organization.

Over recent months there has been accelerating activity on energy security within the OSCE. In July 2009 the Slovak government sponsored an OSCE conference entitled, "Strengthening Energy Security in the OSCE Area." During deliberations, the Slovak Minister of Foreign Affairs H.E Miroslav Lajcak pointed out that:

"The issue of energy security encompasses a broad array of technical, technological, economic and security aspects, which are covered by a political umbrella. The role of the OSCE is not to duplicate, but rather to complement the activities of international energy organizations. It takes a declaration of political will and a quest for consensus for the necessary changes in the area of external energy security to materialize. The OSCE can become a forum which spells out such political support to the steps taken by other initiatives and organizations. By the same token, the outcome of discussions within the OSCE can serve as an example of the existing common approaches and joint interests of OSCE members."

The challenge is for the OSCE to identify where it can add value to the activities of other organizations within the energy sphere, and in doing so support the political dialogue within other organizations that leads to better coordination between producers, consumers, and transit states on issues critical to energy supply security and the security of the infrastructure that delivers it.

Where Can the OSCE Add Value?

One key area where the OSCE can add net value where other institutional initiatives have been

lacking is in the area of tracking and detailing disruptions to critical energy infrastructure (CEI) in the OSCE's area of responsibility (AOR). The OSCE was mandated to engage on the issue of terrorist attacks against CEI at an OSCE Ministerial Conference in Madrid in November 2007.

To have lasting and enduring value, however, the tracking of incidents which disrupt, debilitate or destruct critical energy infrastructure should cover, inter alia, the following types of incidents:

- attacks of a deliberate nature (terrorist attacks such as those carried out in Turkey, North Iraq or Columbia)
- breakdowns of a technical nature or those caused by accidental human activity (Greece, Germany)
- debilitation or destruction of critical infrastructure from natural causes (Italy, Switzerland)
- disruptions of a commercial or political nature (Ukraine, Belarus)

Recent History

Critical infrastructure protection is key to energy-supply security and to global price stability. Energy prices in a time of scarcity—current lower energy prices due to the effects of the global recession are but a deviation from a future upturn in energy prices—are particularly vulnerable to even small attacks on global energy supply vis-a-vis the infrastructure that transits it. According to researchers at the Center for Security Studies in Zurich:

"The main factors driving high crude oil prices from the 2004 to mid-2008 period can largely be attributed to record demand from a global economic boom, price inelasticity, and tightened supply. However, political instability in producer regions further compounded this challenging environment. Such turbulence resulted in what analysts defined as a security or 'risk premium' - ranging from as low as US $4 to as high as $25 dollars per barrel - being placed on crude oil prices within this timeframe. In fact, during this period one can find a direct correlation between EI attacks and increasing global energy prices driven by traders and speculators who viewed EI targeting as a threat to supply and, perhaps, an exploitable opportunity to inflate prices."

In short, the select targeting of CEI by terrorists, criminal gangs or groups vying to exercise leverage over national governments to achieve political, economic or social objectives through the targeting of energy infrastructure significantly contributed not only to pre-recessionary high energy prices (2004-2008) but also price volatility (for both consumers as well as producers) in recent years.

OSCE Energy Security Policy Framework

OSCE involvement in energy security is based on the 2003 Maastricht Strategy Document agreed in December 2003 at the Maastricht Ministerial Council. This document states that a high level of energy security requires a predictable, reliable, economically acceptable, commercially sound and environmentally friendly energy supply. It also underlines the need to ensure the safety of energy routes.

In 2006, the Ministerial Council adopted in Brussels a more focused approach to the issue, highlighting the importance of an energy dialogue it could facilitate with partner organizations such as the Energy Charter and the IEA. The Council pointed out that the OSCE concept of energy security goes beyond security of supply to include security of demand and security of transit, as well as energy efficiency. Under the 2006 Belgian Chairmanship, the Chairman-in-Office (CiO) also requested the OSCE Secretariat to conduct a technical fact-finding mission to gather and analyze information on energy security within the OSCE area, and to make suggestions on renewed international dialogue.

This mandate was reaffirmed in Athens on 2 December 2009 when it called for intensified dialogue and cooperation on energy security. However, it failed to spell out any specific provision(s) on where pragmatic mechanisms should be developed that move the dialogue process beyond the talking phase. The development of a database to detail and track events which impact on critical energy infrastructure, within the OSCE's AOR and beyond, would ground OSCE aspirations in the form of a tangible deliverable

Russia

To avoid the political fallout from energy supply disruptions, the European Union and Russia —Europe's most important supplier of its fuel of choice, natural gas—decided in October 2009 to develop an 'early warning system' to help avoid problems in the supply of Russian energy deliveries. According to EU reports, "The early warning system would include a hotline for emergency situations and obliges Brussels and Moscow to inform each other of potential problems through designated contacts." Russia's Gazprom purportedly lost billions in revenue due to its 2009 gas disruption to the Ukraine and to downstream energy consumers.

Earlier in 2007 Russia proposed to APEC states a regionally based initiative to develop a rapid response network for critical energy infrastructure protection.

Clearly, as Russia is not only Europe's largest provider of natural gas but also an important provider of oil and coal, the Russian Federation has a clear national interest in the integrity of cross-border transit of its energy supply to downstream customers. Tracking and detailing

disruptions to European energy supply networks is therefore key to promoting these interests. The development of a discrete and well defined analytical tool (under the auspices of the OSCE for the benefit of all OSCE members) to help better understand, measure and prevent future events with a negative impact on CEI will help Russia in particular to achieve its following national objectives:

- demonstrate its commitment as a reliable energy partner
- engage with partner states along its entire energy supply chain on the protection of the critical infrastructure on which supply deliveries depend
- ensure the uninterrupted flow of export revenue back to Russia's national government that depends on such revenue
- strengthen its counter-terrorism strategy in the field of energy and energy supply system security in cooperation with other OSCE members
- demonstrate tangible leadership in the field of supply security through the realization of and contribution to the construction of a critical energy infrastructure incident database (CEIID)
- base future actions and protective measures on decidedly scientific data derived from the construction and functioning of the CEIID

Why the OSCE?

There is a qualitative difference between the OSCE and the North Atlantic Treaty Organization which has also been mandated to protect critical infrastructure in its AOR. That difference is Russia. Russia's disdain for NATO is well known. This deters it from positively engaging on critical energy infrastructure protection within the organization's framework. Second, Russia lacks NATO member-state status. Third, Russia views NATO, rightly or wrongly, as an unnecessary vestige of the Cold War and as an organization with a strategic concept which when expressed does not always reflect Russian foreign policy objectives. Conspicuously, Russia has chosen not to engage NATO on the issue of critical infrastructure protection within the framework of the NATO-Russia Council.

The OSCE as noted is an organization that includes both Russia and the United States as members. Whereas the US and some other NATO member states may view the development and utility of such a database as primarily the responsibility of international oil companies (IOCs) this is not an issue for Russia. Both Russia's oil and gas majors are state-owned and operated. This also reflects incidentally the ownership pattern of the vast majority of oil and gas assets and their reserves around the world (i.e. publicly owned versus privately owned and managed) and quid pro quo holds true for the ownership structure of the majority of oil and gas assets in the OSCE's AOR.

Also, Russia wields considerable influence within the OSCE and is active on many fronts. The

United States contrarily views NATO as Europe's principal collective security organization, based on its capacity and capabilities to project force abroad as it has done from Kosovo to Afghanistan. Having said this, the United States actively engages within the OSCE, but on issues different than NATO's mission. Therefore the choice of the OSCE as a place to park the development of a CEIID bodes well for Russia and does not require any shift in focus on the part of the United States away from NATO's grounded political and military activities.

Finally, Russia indicates within its own national security strategy the important contribution of Central Asia to its own national security and the role that secure access to these and other energy resources play in its own national agenda. Unlike the United Nations Economic Commission for Europe, which also facilitates energy dialogue, the OSCE has a security mandate and as such can embrace more robust acts, such as the development of an actual mechanism, in this case in the form of a CEIID, to prevent, mitigate or help respond to challenges faced by energy producers, transit states, and end users where infrastructure is concerned. Russia's neighbors like Kazakhstan and Turkmenistan are OSCE members and as such may welcome a concrete and collective step forward to ensure their own endogenous energy resources and the infrastructure that transits them.

What is an Infrastructure Database and Why is it Important?

A critical energy infrastructure database is essentially a knowledge-based intellectual tool. It contains information culled from non-proprietary information resources that track, detailing as much as possible, global attacks carried out against critical energy assets, be they up-, mid- or downstream. This database will result in the ability to run time-series analyses on attacks against CEI on a global scale. In short, while one cannot predict a specific attack against a specific installation, one can assess the probability of the type of attack based on analytical tools that are empirically based.

In culling and importing data into a database, non-proprietary data is sufficient, as it covers approximately 95% of all incidents carried out against this infrastructure. Some may argue that it is the remaining 5% of incidents that is most important. These incidents are typically detailed by national intelligence and defense organizations, but the database's objective is trend analysis, not specific incident analysis in the first instance. There is a good precedent for this.

While a critical energy incident infrastructure database could be newly constructed, it could also be adapted from an existent software platform. The SIPRI (Stockholm International Peace Research Institute's) Arms Transfer Model database could be applied to tracking and detailing energy infrastructure incidents (CEI). SIPRI's database is well respected by military establishments around the world and its inputs are from non-proprietary sources as well.

Second, OSCE member states may object to culling and inputting data on incidents involving energy infrastructure on a global basis versus focusing exclusively on incidents which occur in the OSCE's AOR. This would be a mistake. Where terrorist activities occur against individuals or infrastructure, the migratory nature of the modalities used to carry out attacks is well documented. For example, the use of IEDs in Iraq are now the overwhelming weapon of choice in Afghanistan. So too do the modalities of attacks against energy assets and infrastructure migrate from theatre to theatre, or even within specific theatres. For states and energy companies it is as important to know what to protect against (tactically) as much it is to pinpoint what will be attacked (target fields). A CEIID would assist in satisfying both of these objectives by detailing them on an empirical basis.

Third, the contentious issue of 'disruption' cannot be avoided. Downstream consuming states have an interest in availing themselves of as much data as possible when a disruption of a commercial nature cascades into a significant energy supply failure. Commercial disruptions can have the same supply magnitude of impact as do technical failures, accidents or terrorist attacks. The database, as an empirically-based mechanism, does not foresee as a deliverable the identification of political determinants that lead to fault determination in the case of a commercial dispute. Individual users can derive their own conclusions. The CEIID will simply record the energy supply failure impact on producing, transit, and consuming states in empirical terms.

Fourth, the issue of cyber-war and attacks carried out against IT infrastructures that control energy and power networks must be addressed and included in the incident database. Frank Umbach and his colleagues at the Center for European Security Strategies in Munich have extensively researched the cyber side of the energy security challenge. Frank writes, "In both Western governments and industries, security concerns about increasing cyber warfare attacks by individuals, crime organizations and governments regarding espionage or malicious software programs that damage and disrupt processes of critical infrastructure assets and processes have grown considerably in the last several last years. These cyber attacks have risen to an unprecedented level of sophistication. As a result, the vulnerabilities of digital systems and networks have grown exponentially. However, public awareness has not kept up with these new threats, and vulnerabilities in cyberspace, which have the potential to affect all sectors of private and public life, national and international businesses, and even the defense policies of states, multinational organizations like the EU...," and, by implication, the OSCE. One can only conclude that a CEIID without the inclusion of cyber-related attack data would be an anathema to a full analysis of risks which challenge CEI within the framework of the current threat environment.

If energy security is a topic salient to the security concerns of states, commercial enterprise, and policy makers charged with assessing the cascading effects of critical energy and power

failures on civil society, then both enhanced dialogue and informed actions need to occur to address identified threats. Dialogue alone will not do the trick. Better data can inform all stakeholders on their individual role and contribution to enhancing this security environment for the collective benefit of all concerned. The OSCE Secretariat as mandated may want to take this recommendation under consideration. Finally, the OSCE's focus on energy security comes at an opportune time in the organization's history. In January 2010, for the first time in the history of the organization, the Chairman-in-Office of the organization will be Kazakhstan lead by the Kazakh Foreign Minister Marat Tazhin. The Kazakh Minister has already pledged that under Kazakhstan's leadership, "Kazakhstan will strengthen OSCE support for development of effective Eurasia transit and transport corridors." It should be an interesting year to come.

Kevin Rosner is a Senior Fellow with the Institute for the Analysis of Global Security in Washington D.C. and is the Managing Editor of the on-line Journal of Energy Security. This article was adapted from comments he made to an OSCE Energy Security conference organized by the Belarus Ministry of Foreign Affairs in Minsk in December 2009.