III. Research Notes

Research Note on the Energy Infrastructure Attack Database (EIAD)

by Jennifer Giroux, Peter Burgherr, Laura Melkunaite

Abstract

The January 2013 attack on the In Amenas natural gas facility drew international attention. However this attack is part of a portrait of energy infrastructure targeting by non-state actors that spans the globe. Data drawn from the Energy Infrastructure Attack Database (EIAD) shows that in the last decade there were, on average, nearly 400 annual attacks carried out by armed non-state actors on energy infrastructure worldwide, a figure that was well under 200 prior to 1999. This data reveals a global picture whereby violent non-state actors target energy infrastructures to air grievances, communicate to governments, impact state economic interests, or capture revenue in the form of hijacking, kidnapping ransoms, theft. And, for politically motivated groups, such as those engaged in insurgencies, attacking industry assets garners media coverage serving as a facilitator for international attention. This research note will introduce EIAD and position its utility within various research areas where the targeting of energy infrastructure, or more broadly energy infrastructure vulnerability, has been addressed, either directly or indirectly. We also provide a snapshot of the initial analysis of the data between 1980-2011, noting specific temporal and spatial trends, and then conclude with a brief discussion on the contribution of EIAD, highlighting future research trajectories.

Keywords: *energy infrastructure vulnerability, non-state violence, database, targeting*

Introduction

Attacks aimed at energy infrastructure have increased over the last decade, a trend that is correlated with the growing political and economic instability in oil and gas producing regions. Terrorism, insurgent tactics, maritime piracy, sabotage, targeted activism, etc., are part of the bouquet of violent phenomena where energy infrastructures have been targeted. Despite this, research on the targeting of energy infrastructure has remained in various research silos, particularly the study of terrorism or resource conflict studies, without branching out across other areas of research on violent phenomena in general, and the targeting behaviours of violent non-state actors (VNSA) more explicitly.[1] In one attempt to fill this gap the Center for Security Studies at ETH Zurich in collaboration with the Paul Scherrer Institute (PSI) developed the Energy Infrastructure Attack Database (EIAD): a compilation of data from 1980 through 2011 on reported (criminal and political) attacks/threats to energy infrastructures by non-state actors—which includes the range of actors from politically motivated groups (e.g. terrorists) to other criminal actors such as those committing acts of maritime piracy and armed banditry.

This fully searchable database (contained in an Excel datasheet) contains over 8,000 coded incidents, spanning the globe.[2] In addition to including attacks (both successful and unsuccessful) that aim to cause physical harm or damage, when possible other threats such as plots are also included so to capture the full breadth of (non-state) threats to energy assets. Furthermore, it is not just devoted to attacks aimed at the oil and gas sector (both onshore and offshore), but across all energy sectors (Biomass, Coal, Geothermal, Hydropower, Nuclear, Solar, and Wind) and electricity in general. Furthermore, within these sectors energy infrastructures (EI) include all human (energy sector personnel), physical (energy sector physical assets) and information (energy sector cyber systems supporting operations) infrastructures.[3]

This Research Note on EIAD aims to introduce this new dataset and our analysis on the targeting of energy infrastructure. We continue this discussion by first examining some key research themes where the targeting of energy infrastructure, or more broadly energy infrastructure vulnerability, has been addressed, either directly or indirectly. In this respect, we try to make the case that EIAD, and the ideas built emerging from its development, are interconnected with various research discussions and thus hope that its future utility will encourage cross-fertilization of research and analysis. Following this discussion we provide a snapshot of our initial analysis of the data between 1980-2011, noting specific trends and assessments. Finally, we conclude with a brief discussion on the contribution of EIAD and highlight future research trajectories.

Why EIAD?

When examining VNSA threats to Energy Infrastructures (EI), academic and policy discussions are often focused on terrorist threats to EI (part of which is connected to debates on energy security) or the relationship between conflict and natural resources, the latter of which is more about the conditions in which national resource abundance is related to conflict. There has also been a growing body of literature focusing on how businesses should operate in conflict-affected areas. In the process to develop the targeting energy infrastructure project the EIAD research team decided to look beyond 'terrorist targeting' in order to capture other types of non-state, violent phenomena. In doing so, we found these various research strands to be relevant for not only building up our understanding of this area but also positioning our analysis and where we see EIAD being particularly useful to further studies and analysis.

Previous Work

One of the more notable, earlier studies in this field of research was carried out by Kjøk and Lia (2001) [4] and examined non-state threats against petroleum infrastructure. Using the ITERATE database of international terrorism, the authors found that 79 per cent of terrorist strikes against petroleum infrastructure (between 1922 to 1999) were made by domestic terrorist groups. In addition, the authors also noted a general increase, over time, in the number of attacks against petroleum infrastructures.[5] Another study, published in 2008, looked more specifically at the interest and capability of al-Qaeda attacking 'economic targets' (particularly EI),[6] an attempt not too dissimilar from other efforts in the post 9/11 era.[7] Mihalka and Anderson (2008) linked the analysis to global energy security concerns, found that despite verbal overtures global jihadists affiliated with al-Qaeda have not made EI, and economic targets more broadly, a serious priority. More recently, a 2010 study, "Terrorist Targeting and Energy Security," sought to uncover the general patterns and characteristics of contemporary terrorist targeting of EI.[8] Though Toft et al (2010) found a certain geographic concentration of attacks, similar to Simonoff et al (2005) [9], they did not find a correlation between energy rich countries and the number of EI attacks, nor did they observe a correlation between certain terrorist ideologies and EI targeting. Outside of these larger studies, there have also been some case studies that take into account dynamics or factors at the local level. Studies on specific countries,[10] regions,[11] or terrorist groups or Violent Non-State Actors (VNSAs) [12] have rendered some interesting insights; however, they continue to fall short of looking at the community interplay with other VNSA in regions where violence is prevalent and EI is vulnerable. Furthermore, all of these studies tend to focus on threats to the oil and gas sector, while EIAD is a dataset that captures threats to all energy sectors.

A second area of research - the resource conflict literature - is a useful resource for capturing some of the conditions in which energy infrastructure becomes vulnerable. In many cases, one can see a correlation between the increase in attacks aimed at petroleum infrastructure and the growing instability in oil producing/exporting states.[13] However, such studies have met some criticism. A subsequent study by Lujala et al (2007) found that it is not so much about the hydrocarbons per se, but rather the existence of conflict in areas where oil is located that may lead to, or exacerbate, conflict and thus, by extension, increase vulnerability.[14] Looking at the impact to oil and gas supplies during conflict, Luciani (2011) found that oil and gas installations are relatively resilient in armed conflict; but such conflicts tend to hinder investment and reduce revenues.[15] Of course, as demonstrated by numerous studies, such debates, correlations and linkages are certainly not new but nevertheless useful when assessing the spaces where EI vulnerability is directly or indirectly addressed.[16]

A third literature strand examines how businesses, particularly multinational corporations and those in extractive industries, are rather normative in the way debating how companies should operate in conflict-affected areas. The underlying theme in such debates is that business actors are significant players in the host environment, not only serving as partners with the host government but also with the host community where they require the social license to build and operate the infrastructure to carry out their activities. In this respect, through their operations they become intertwined with the different social and technical spaces, often meaning that they operate in or around conflict zones and may even contribute to conflict by the sheer expectations their activities create. This creates enormous challenges as not all state actors have the capacity or the will to provide security, giving way to the potential for business actors to incur "substantial war damages and rising security costs" and risk "being publicly associated with bloodshed and human rights violations".[17] Yet, even in this discussion there is little research that examines the challenges that arise from businesses having to engage (or inadvertently engaging) with VNSAs, particularly when their assets are threatened. Business actors bring the capacity to build large compounds, oftentimes well-equipped and developed, to house their staff, bring in large machinery to develop complex facilities and other infrastructures to conduct their business activities. They are responsible for extraction and production activities as well as bringing mineral products to the global market. All of this is supported by business operations, which include a capable staff and infrastructure. Meanwhile, community members continue to live without the same access to such services. The lack of electricity or access to decent roads, or any roads at all, creates a sense of tension that gives way to the formation of grievances which may in turn lead to violence aimed at the energy sector.

Brought together, when reviewing this literature not only did we find a gap in the types of violence and energy sectors considered within studies on the targeting of energy infrastructure (with an overwhelming focus on terrorist threats to oil and gas assets) but we also found that very few studies examined how violence emerges and evolves within a complex socio-technical space where infrastructural imbalances are both a large driver of conflict and influence the targeting behaviours of VNSAs. As a result, rather than using terrorism datasets to analyze trends, we decided that a new dataset needed to be developed to include other energy sectors as well as other types of violence carried out by non-state actors. Furthermore, given the growing extent and intensity of the non-state threats to EI, more comprehensive tools for risk assessment and management in the field of energy security are needed. Acknowledging the absence of an integral open-source that deals explicitly with attacks aimed at EI, the EIAD was developed to fill this research gap.

EIAD Structure, Data Collection, & Analysis

To be clear, EIAD is not a complete departure from existing open source datasets on non-state violence. If anything, we view EIAD as a contribution to research on the targeting behaviours of non-state actors and the vulnerability of energy infrastructure as well as a resource that serves as a connection point with other open source datasets. What sets EIAD apart is the inclusion of all forms of non-state violence aimed at energy infrastructure, which is defined as 'all human (energy sector personnel), physical (energy sector physical assets) and information (energy sector cyber systems supporting operations) infrastructures in fossil energy chains (oil, natural gas, coal), hydro and nuclear power, new renewable technologies (e.g. solar, wind, biomass, geothermal) as well as electricity infrastructures. However, given the broad utility of the Global Terrorism Database (GTD) [18] and the extraordinary efforts that have gone into developing and maintaining this dataset, the GTD was used as a basis for EIAD and thus we adopted a similar structure and methodology. With that, all of GTD's data on terrorist attacks aimed at energy infrastructure are included in EIAD and coded and sourced accordingly. Where EIAD departs from GTD is in its inclusion of other forms of non-state violence. This requires the use of various kinds of open source information (databases such as the International Maritime Bureau Piracy reports, news articles, etc.) to gather information on other (namely non-terrorist related) incidents where energy infrastructures have been targeted. In addition we have begun to receive incident information on the targeting of oil and gas infrastructures, in particular, from private sources such as companies and governments.

At present, EIAD contains reported threats (plots, hoax, etc.) and attacks (successful, failed and foiled) on EI throughout the world between 1980 and 2011. Each coded incident in the database has its geo-reference, which will allow the visualisation of data by means of mapping tools and Geographic Information System (GIS) software, allowing the geo-statistical analysis to identify spatial patterns and hotspots. Another unique aspect of the EIAD is that we do not code for motivation but rather for attack type (e.g., assassination, assault, bombing, etc.) and instrument used (e.g., firearms, explosive-dynamite, arson/firebombing, etc.). The aspect of motivation was omitted due to errors in reporting as well as the fact that the motivation of the perpetrator is not always obvious and in many cases not known/reported. Nevertheless, EIAD includes a category for 'Perpetrator Group/Actor', which can help with identifying motivation/intent.

Data Collection & Verification

The data collection for the EIAD follows standard coding procedures: human coders collected information through open-source (non-commercial) databases, books, and other available online resources. In order to ensure the accuracy of the data, researchers used standardised data entry formats. The standardised data categories include *Incident Date* (including extended incidents such as hijacking and kidnappings); *Incident Location* (location, including geo-coded information; *Incident Information* (summary, event type, and whether event was part of a multiple attack); *Attack Information* (attack type, instruments used, combination attack, second attack type); *Target Information* (specific target, energy sector, energy infrastructure, second target); *Perpetrator Information* (individual/group, group type); *Incident Consequences* (casualties and fatalities, reported downtime, infrastructure impact, hostage information); *Additional Information*; and *Source Information* (media reports, social media, cross-reference to other databases, etc.). Except for incident date, summary, additional information and sources, all of the categories have standardized data entry lists to select from. Furthermore, in the development of our categories we kept close to the format used by GTD to maintain synchronicity and compatibility where possible. In terms of energy sectors and subsectors we drew from other resources to create a comprehensive list for data entry.

Given that we used data drawn from the GTD as well as other databases and resources, the first step of the database development process involved gathering, structuring and aggregating data from various sources. This allowed us to merge duplicate data as well as address redundancies. This step involved combing through the coded data to address duplications and also fill gaps in information where possible. During this step we also addressed any incidents that contained multiple attacks, disaggregating them when and where necessary. By disaggregation we are referring to our decision to have single incidents which involve multiple type or locations of an attack to be disaggregated such that each attack within the incident is recognized as both connected to another incident (by being marked as a 'multiple attack') as well as having its own incident ID. After consultation with various experts during the development of EIAD's coding methodology we determined that the tendency for VNSA to carry out small, oftentimes multiple attacks in confined periods of time best reflected the nature of the threat and the capability of the threat actor. Single incidents that involve large damage are represented in EIAD; however, they are less frequent than the smaller types of attacks, most of which are targeting numerous points across a pipeline, or various connecting electrical pylons, for example.

Once we had our master dataset, another reviewer examined the data to address incorrect data entry or irregularities as well as another person that carried out the quantitative analysis. Overall, while such a massive data collection, aggregation, and structuring will render some overlaps or errors we have attempted to mitigate such lapses through these steps of verification and review. It is also our intention to continually maintain EIAD as a living database, one that through feedback from users can continuously be improved.

Most of our incidents contain one source, though we have aimed for two sources in the interest of verification. For all incidents where verified data sources have been cited, such as GTD or the International Maritime Bureau, typically one source has been referenced. In addition we have also received some data from companies and governments, which provide data that is often not found in media sources. In such cases, we list the source as "private", if there is an agreement of confidentiality, or list the actual name of a source provider if permitted. However, this issue of sourcing brings up two limitations of the data. For one, we need more primary data in order to increase the robustness and accuracy of the incident information. In many cases we only list 'explosives' (for example) as the attack type or instrument used as opposed to having access to more detailed information on the type of explosive. First of all, this type of specific information, which is difficult to access as it commonly remains in the confidential knowledge bank of governments and companies, is important for research as it enables analysis on the behaviour and tactics of violent actors over time. Secondly, this type of more detailed information would provide more exact information on the location of attacks. Most of our geo-coded information on the location of attacks refers to a city or in some cases a region. This is due to the lack of specific, geo-coded reporting from open sources. In comparison, the information that we have received from primary data sources has offered more specific geo-coded information, which in turn can be helpful for not only visualising hotspots at the micro level and tracking the movement patterns of violence but also for improving qualitative analysis on the area where violence emerges.

Analysis

The present analysis of EIAD includes 8.602 data records encompassing the years 1980-2011.[19] In the 1980s and 1990s a total of 1808 and 1508 events were recorded, whereas in the 2000s with 4,223 events it more than doubled. The two years available for the 2010s already amount to 1,063 EI attacks, indicating that a further increase could be expected if no drastic changes in the overall situation and/or boundary conditions will occur in the next few years.

Figure 1 shows the annual numbers of attacks for this period as well as the respective decade averages. The apparent overall upward trend in EI attacks is also statistically confirmed by a non-parametric Man-Kendall test (n = 32, Z = 3.16, p = 0.01). It is worthwhile to note that the year 1993 appears to be a substantial outlier to this trend with only 14 attacks; however it does not affect the prevailing pattern. This can be illustrated by replacing the 1993 value by the average of 1992 and 1994, which increases the decade average by a modest 10%.

The low 1993 value can be explained by the fact that EIAD uses the Global Terrorism Database (GTD) as one of its key primary information sources for terrorism related incidents. The data for 1993 were lost prior to the compilation of GTD and despite several efforts could not be recollected (GTD Codebook).[20] Cumulated country level statistics in the Appendix of the above cited GTD document suggest that GTD should contain almost 5,000 incidents for 1993. Within our ongoing EIAD coding efforts we were also not able to obtain a better coverage of individual EI attacks for 1993, which is why EIAD currently has the same data gap for 1993 like GTD.

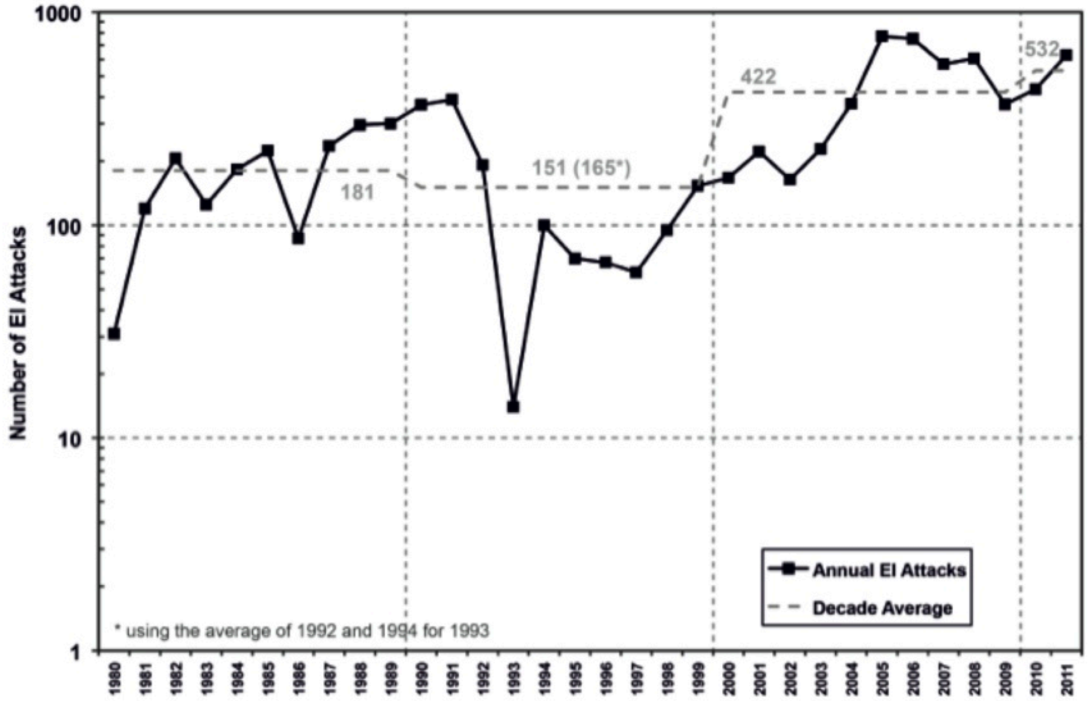

Figure 1: Annual number of EI attacks and decadal averages over the period 1980 – 2011.

The vast majority of EI attacks in the period 1980-2011 were classified as successful (8.211), distantly followed by foiled (175) and failed (203) attacks. The remaining 0.15% was categorized as threat (8), plot (3) and unknown (2). Though we code for hoaxes, we do not have any incidents coded as such in the database. This high share of successful attacks can be explained by several factors. Certain energy infrastructures such as pipelines and transmission lines are due to their "linear" nature relatively easy targets, and are therefore exposed to a high attack pressure. Furthermore, production and transit of energy carriers takes place in or passes through less developed countries that do not have the financial means to harden such infrastructures and provide high protection levels. Finally, we can safely assume that we are not capturing a completely comprehensive picture, given that many attacks go unreported and thus do not surface in the media. This may be more important for foiled and failed attacks, and particularly threats, plots and hoaxes, which are also not the main focus of EIAD. In fact, most companies would prefer to keep threats to their assets as quiet as possible. Of course, this is one of the consequences, and indeed drawbacks, of relying on public or open sources for information, particularly as it concerns threats to energy infrastructures that are often owned/operated by private actors.

The Cano Limon pipeline in Colombia provides an example of how guerrilla attacks by Revolutionary Armed Forces of Colombia (FARC) and National Liberation Army of Colombia (ELN) could be significantly reduced from 2002 to 2004 due to a strong militarisation of the area as well as the demobilisation and reintegration of paramilitaries in Colombia [21]. However, this improvement in security was at the expense that exploration of new reserves came practically to a standstill. More recently, approaches involving engagement of local communities have been adopted by industry and affected countries to increase local support through participation processes, socio-economic benefits, and protection of the environment. In contrast, "point sources" such as refineries or power plants are thus easier to protect against physical and cyber-attacks. EIAD data clearly supports this notion with close to 50% of attacks attributable to electricity transmission lines and sub-stations, followed by oil pipelines (ca. 15%), oil transports by road tanker and natural gas pipelines (each in the order of 7%). Finally, a rather large amount of almost 40% or 3413 of EI attacks were considered multiple attacks. The multiplicity of attacks within a specific country points to the power of 'tactical contagion' within certain contexts and which contribute to the crests of the wave. For example, to identify the motivational complexity of such cases, fieldwork carried out by Giroux in 2012 in Nigeria and Colombia, two prominent locations in EIAD where EI has been frequently targeted (tactical contagion), revealed that though many of the attacks were carried out by political motivated groups, such as the FARC in Colombia, the motivation for attacks were various. Some attacks were carried out as a way to send political messages while others were motivated by pure economic reasons (e.g. threats to EI as a form of extortion).

Among the EI attacks in the observed period of time, 80.4% were carried out with some type of bombing device, followed by several other attack types with more than 100 events that cumulatively amount to 15.0% (Figure 2). Siege and hostage events contribute a low 0.4%, whereas armed attacks, cyber-attacks and vandalism with a share of 0.1% are practically negligible.

The low levels of cyber incidents capture the coding challenges within this area. Due to lack of information, particularly on the actor (state or non-state), including incidents, such as the infamous Stuxnet worm that targeted supervisory control and data acquisition (SCADA) systems in the energy sector,[22] is a hurdle. For one, the actor of this event, like many cyber attacks, is unknown and may very well be a state actor, which would mean that it does not meet EIAD's coding criteria. Other incidents, such as hijacking typically refer to vessels carrying energy (e.g. oil or gas products), offshore whereas assassination attacks involve the targeting of specific energy personnel. Lastly, it should be noted that 4.1% of all events could not be assigned to a specific category because of incomplete information in the available incident summary, and thus are classified as unknown.

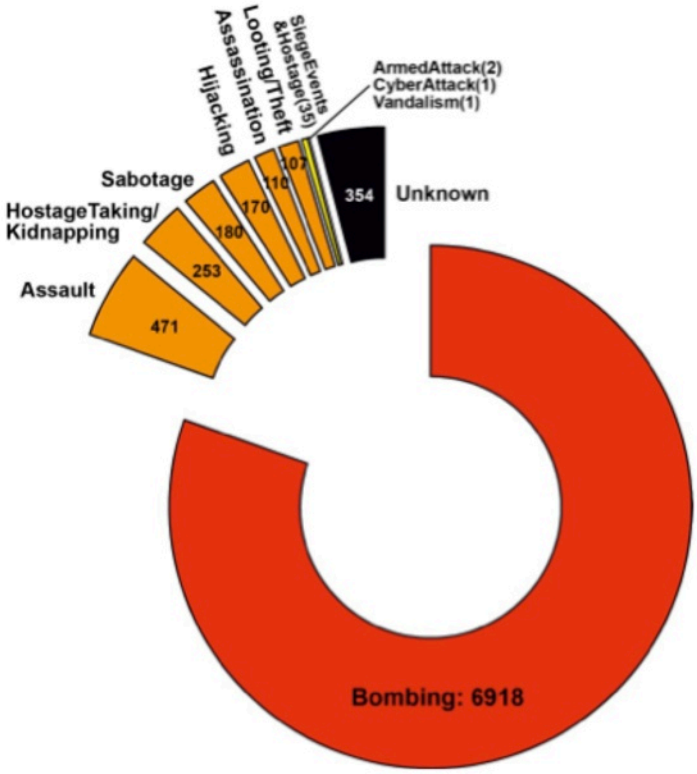

Figure 2: Classification of EI attacks by attack type (1980-2011; n=8602)

Figure 3 shows the spatial distribution of EI attacks by country for the years 1980-2011(Only events that could be accurately geo-referenced were considered, which is why only 6990 out of all 8602 EI attacks are shown in the figure). It is in the visualisation of EIAD incidents and the breakdown of attacks by country that the role of tactical contagion comes to life, illuminating the specific areas (or hotspots) where EI attacks have been particularly common.

The information in this figure can be summarized as follows:

The top 3 countries were Colombia (1.381 EI attacks), Iraq (1.085) and Pakistan (1.009) accounting for 49.7% of all EI attacks in the years 1980 - 2011.

- Another 25.7% were attributable to El Salvador, Peru, Afghanistan, Nigeria and Chile (200+ attacks each)
- India, Angola, Philippines, Thailand and Russia (100+ attacks each) contributed another 11.8%.
- Spain, Turkey, Yemen and Guatemala (50+ attacks each) sum up to 3.8%.
- The remaining 69 countries for which data were available accounted for the remaining 8.9%, and roughly two thirds of them contributed 0.1% or less.

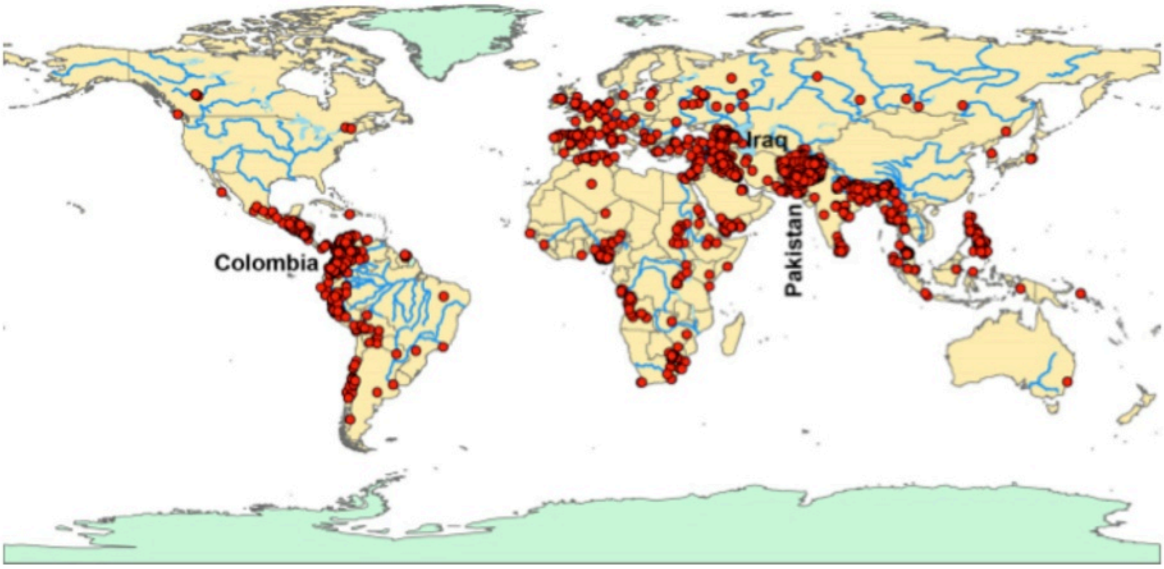

Figure 3: Spatial distribution of EI attacks in the period 1980-2011 (n = 6990).

Figure 4 illustrates the top three country clusters (Colombia, Iraq and Pakistan), and provides additional information on the temporal dynamics as well as involved energy sectors and infrastructure types in each cluster. The combined representation of these two factors with the temporal aspects allow for a more subtle differentiation of country hotspots.

In the case of Colombia, three distinct peaks of EI attacks can be observed from 1988-1992, 1999-2002 and 2005-2007. It is worthwhile noticing that the first peak is less pronounced than the two others, and that after the second peak the annual numbers of attacks do not decrease again to similar low levels as before. The peak from 1988-92 is clearly attributable to the petroleum sector and attacks on the Cano Limon pipeline. The second peak comprises a combination of attacks on oil pipelines and transmission lines, with attacks on the former dominating in 2001, and on the latter in the years 1999, 2000 and 2002. The strong decrease in attacks on oil pipelines between 2002 and 2004 is then due to the previously mentioned militarisation of the Cano Limon pipeline region.

Iraq exhibited a clear peak from 2004 to 2007, with 2005 and 2006 having more than 300 and 250 attacks, respectively. Overall, oil pipelines and transmission lines were most often attacked, followed by attacks directed at energy and government personnel. Across the years included in this analysis, there were some shifts in patterns of infrastructures predominantly affected, i.e. oil pipelines in 2004, oil pipelines and transmission lines in 2005, personnel in 2006, and all categories about equally in 2007.

In Pakistan, between about 70 and 140 attacks per year occurred from 2005 to 2010, and then the number of attacks nearly doubled to 270 in 2011. The actual impacts on Pakistan's energy sectors and infrastructures can be divided as follows. The lower peak period concerned mostly transmission lines (2005-2009) and natural gas pipelines, whereas the high peak in 2011 is a combination of transmission lines, oil transport by road tanker and natural gas pipelines. As illustrated by these top three cluster countries, it is important not only to look at spatial clustering (hotspots), but also to analyze the temporal patterns and underlying mechanisms creating these clusters through time.

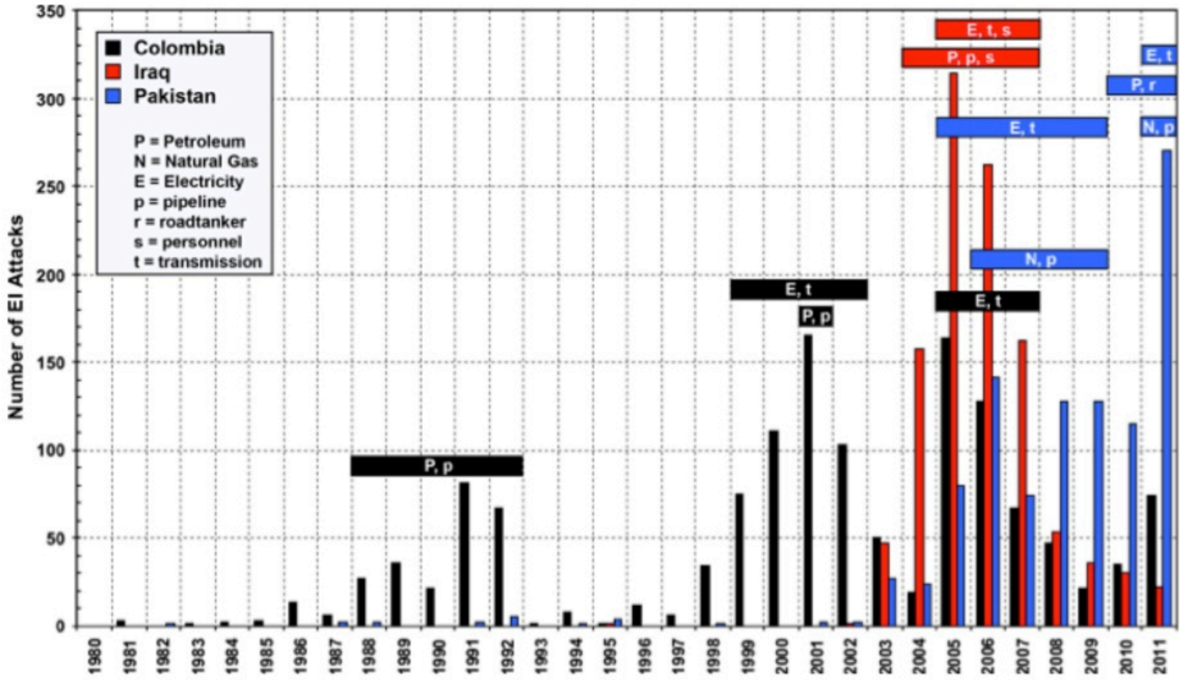

Figure 4: Annual numbers of EI attacks for top three countries, including identification of temporal attack peaks in the period 1980-2011.

Contribution & Future Research Trajectories

In all, EIAD provides a comprehensive foundation for the analysis of energy infrastructure attacks by VNSAs. In our analysis we evaluated the spatial and temporal patterns and conceptualized the patterns of clustering as type of 'tactical contagion' within specific areas or locales as well as across regions. In other words, we denote a common pattern whereby attacks on energy infrastructures are often multiple events and concentrated both in time and space, resulting in distinct hotspots. We also found that attacks predominantly take place on "linear" energy infrastructures (e.g. pipelines and transmission lines) that are difficult to protect and often pass through remote areas. Therefore, consequences in terms of fatalities and casualties are mostly minor, although when attacks occur frequently (in terms of multiple and connected events), they can result in substantial business and supply disruptions. For example, in Iraq, between January and August 2013 there were over 30 bombings aimed at the Kirkuk-Ceyhan pipeline, which led to repeated downtime for repairs.

Looking ahead, there are multiple avenues for future research that can adopt and develop other conceptual approaches to understand trends as well as continue to improve EIAD's utility. For one, EIAD has room for further development, particularly in the area of fostering avenues for a community of interest – made up of public and private partners – to provide and help improve the quality of information. This can help address some of the information shortcomings discussed earlier. In addition, given that we have identified discernible patterns in the data (i.e. 'tactical contagion' or hotspots) there is the potential to use EIAD to forecast likely future clusters. This will require further analysis on the correlating factors across regions that lead to clusters, and would be a worthwhile endeavor. At a micro-level more cases studies are needed to add depth and breadth to EIAD – simply analysing the data at a macro level has already revealed some interesting insights and illuminates some of the context-specific factors and nuances that can, in turn, inform policy prescriptions and recommendations.

About the Authors:

Jennifer Giroux *is a Senior Researcher for the Risk & Resilience Team at the Center for Security Studies (CSS) at ETH Zurich. She also heads the targeting energy infrastructure research project through which the Energy Infrastructure Attack Database (EIAD) was developed.* **Peter Burgherr** *is Head of the Technology Assessment group, Laboratory for Energy Systems Analysis, at Switzerland's Paul Scherrer Institute. He is also the primary person responsible for PSI's database ENSAD (Energy-Related Severe Accident Database), which is the world's largest database on severe accidents in the energy sector.* **Laura Melkunaite** *is a Project Assistant at the CSS; she has worked on the development of EIAD*

Notes

[1] Acts of war against energy infrastructures by states are not covered in EIAD

[2] For access to EIAD see: http://www.css.ethz.ch/research/research_projects/index_EN/EIAD

[3] Overall the EIAD consists of 10 main categories and sub-categories to be discussed in the section 'EIAD Structure, Data Collection, & Analysis'.

[4] Ashild Kjøk & Brynjar Lia. *Terrorism and Oil – An Explosive Mixture? A Survey of Terrorist and Rebel Attacks on Petroleum Infrastructure 1968-1999*. FFI/RAPPORT 2001/04031, Norwegian Defence Research Establishment, 2001. Online at: http://www.ffi.no/no/Rapporter/01-04031.pdf

[5] Ibid, p. 22.

[6] Michael Mihalka & David Anderson. *Is the Sky Falling? Energy Security and Transnational Terrorism*. Strategic Insights, Center for Contemporary Conflict at the Naval Postgraduate School in Monterey, California, July 2008.

[7] For example see: John C. K. Daly. *Saudi Oil Facilities: Al-Qaeda's Next Target?* Terrorism Monitor 4, Issue 4, 2006; Gal Luft. *Pipeline sabotage is terrorist's weapon of choice*. Energy Security, March 28, 2005.

[8] Peter Toft, Arash Duero & Arunas Bieliauskas. *Terrorist targeting and energy security*. Energy Policy, 38, 2010.

[9] S.J. Simonoff, C. Restrepo, R. Zimmerman & E.W. Remington. *Trends for Oil and Gas Terrorist Attacks. I3P Report No. 2, Hanover, NH: The I3P, November 2005.*

[10] Babatunde Anifowose, Damian M. Lawler, Dan van der Horst & Lee Chapman. *Attacks on oil transport pipelines in Nigeria: A quantitative exploration and possible explanation of observed patterns.* Applied Geography, 32, 2011; Jennifer Giroux. *Turmoil in Delta: Trends and Implications. Perspectives on Terrorism,* 2: 8, 2008.

[11] See: Pavel K. Baev. *Reevaluating the Risks of Terrorist Attacks Against Energy Infrastructure in Eurasia*. China and Eurasia Forum Quarterly, Vol. 4, No. 2, 2006; Jennifer Giroux. *Targeting Energy Infrastructure Examining the Terrorist Threat in North Africa and its Broader Implications*. Circunstancia 7: 18, 2009.

[12] John Robb. *Brave New War: The Next Stage of Terrorism and the End of Globalization*. John Wiley & Sons Inc., Hoboken, New Jersey, 2007; Toft et al. 2010.

[13] Halvard Buhaug. *Relative Capability and Rebel Objective in Civil War*. Journal of Peace Research, Vol. 43, No. 6, 2006; Michael L. Ross. *Blood Barrels: Why Oil Wealth Fuels Conflict.* Foreign Affairs, May/June 2008.

[14] Päivi Lujala, Jan Ketil Rod & Nadja Thieme. *Fighting over Oil: Introducing a New Dataset*. Conflict Management and Peace Science, 24, pp. 239-256, 2007.

[15] Giacomo Luciani. *Armed Conflicts and Security of Oil and Gas Supplies*. CEPS Working Document, No. 352, 2011. http://www.princeton.edu/~gluciani/pdfs/WD%20352%20_SECURE_%20Luciani%20on%20Armed%20Conflicts.pdf.

[16] E.g.: Paul Collier & A. Hoeffler. *On economic causes of civil war*. Oxford Economic Papers, 50: 4, P. 563-573, 1998; Michael Ross. *What do we know about natural resources and civil war?* Journal of Peace Research, 41: 3, pp. 337-56, 2004.

[17] Nicole Deitelhoff & Klaus Dieter Wolf. *Corporate Security Responsibility? Corporate Governance Contributions to Peace and Security in Zones of Conflict*. Pelgrave Macmillan, p. 3, 2010.

[18] Gary LaFree & Laura Dugan. *Introducing the Global Terrorism Database*. Terrorism and Political Violence, 19: 1, pp. 81-204, 2007.

[19] This is a snapshot of a larger data analysis and study that was supported by the United States Institute for Peace in partnership with our host institutions. The full data analysis with case studies will be featured in another publication.

[20] See the GTD Codebook, p.3: www.start.umd.edu/gtd/downloads/Codebook.pdf

[21] Markus Koth. *Demobilization and Reintegration of Paramilitaries in Colombia*. Bonn International Center for Conversion (BICC) Papers, July 2005.

[22] J.P. Farwell and Rafal Rohozinski. *Stuxnet and the Future of Cyber War*. Survival: Global Politics and Strategy 53: 1, pp. 23–40, 2011.