Over the last decade energy security debates have shape-shifted. The debates have at times focused on issues such as price volatility, resource nationalism, supply chain vulnerability, resource abundance vs. resource constraints and more recently on the cyber vulnerabilities of energy information infrastructure networks. However energy security remains primarily about the availability, accessibility, acceptability and affordability of energy supplies primarily in the form of oil and natural gas (ONG), which accounts for nearly 60% of global primary energy consumption. Integral energy flow requires a functioning and secure energy infrastructure (EI) supply chain which not only includes physical infrastructure, such as pipelines and facilities, but also human capital (i.e. energy sector employees) and virtual networks (i.e. information infrastructure) that support the functions of energy systems and operations. However energy supply chains face myriad risks in today's complex environment one of which include those posed by violent non-state actors.

Over the years, threats against energy infrastructure from non-state actors have intensified and multiplied. These include maritime piracy and armed banditry attacks aimed at energy carriers and offshore platforms in key transit corridors, such as the Gulf of Aden and Indian Ocean or in producing regions such as the Gulf of Guinea, to the small yet frequent attacks on physical assets and energy sector personnel as characterized by flashpoints or energy attack clusters in Iraq, Nigeria, and Colombia to name a few. One can go as far to say that EI security is at heart of contemporary geostrategic challenges to the energy system. More recently, cyber attacks on energy systems have materialized in the form of intellectual property theft and espionage by those that aim to cause actual physical damage, as demonstrated by the Stuxnet virus, which targeted SCADA (supervisory control and data acquisition) systems which monitor and control infrastructure in the energy sector.

Going forward, given the significant changes in the threat picture, it is worth canvassing the phenomenon of targeting energy infrastructure by violent non-state actors (VNSA). Up until now threats to EI have largely focused on energy terrorism. Overall, when scanning resources for non-state threats to EI clearly a research gap in the literature exists in the different groups that make up VNSAs but also, more significantly, in a lack of structured information about the attacks they perpetrate. Comparatively, this research gap is similar to past issues when assessing the risk of severe technological accidents in the energy sector that then inspired the development of ENSAD (Energy-related Severe Accident Database) by the Paul Scherrer Institute (PSI). The creation of ENSAD allowed for comparative risk assessments using quantitative and objective information for better understanding these accidents. In analyzing the targeting of energy infrastructure, the project team has experienced a similar 'data issue'. Though numerous information sources exist, which include commercial and non-commercial databases, there is no open-source resource that deals explicitly with attacks specifically aimed at EI and/or dealt with VNSAs in general. Most existing research on the targeting of EI uses data available in large terrorism databases such as the Global Terrorism Database but limit coding to terrorist groups and their attacks. Though there has been some excellent analysis in this domain, many attacks and threats have not been included, as they naturally do not fit coding criteria for a terrorist attack. This research gap prompted the conceptualization of the Energy Infrastructure Attack Database (EIAD), a dataset currently being developed by the Center for Security Studies at ETH Zurich and the Paul Scherrer Institute (PSI).

Non-state threats to energy infrastructure

Given the energy import dependence of most countries, much of the world's critical ONG supplies must transit across increasingly uncertain terrain with varied security. As Michael L.

Ross has highlighted
"oil-producing states make up a growing fraction of the world's conflict-ridden countries". The upheavals throughout the Middle East & North Africa (MENA) key energy producing zones, as well as maritime attacks aimed at energy carriers in key energy transit zones, illustrate such developments. Yet, despite the changing context and the myriad threats posed to EI along the supply chain, a cursory overview of the literature on non-state threats to energy infrastructure reveals either an overwhelming focus on terrorist threats, discussions on the correlation of conflict and energy resources, or broader analysis on EI vulnerability and the need for comprehensive EI security plans and stronger partnerships. For example, a 2005 research report "Trends for Oil and Gas Terrorist Attacks" authored by Simonoff et al focused on terrorist threats to ONG infrastructure between 1990 and 2005. Using the now defunct National Memorial Institute for the Prevention of Terrorism (MIPT) database, the authors recorded 330 attacks; a small fraction of total terrorist attacks, and also noted the clustering of attacks in certain states/regions. A more recent 2010 study, "Terrorist Targeting and Energy Security, " while impressive and thorough had similar findings to the 2005 study; the authors found that the terrorist targeting of EI, while concentrated in certain countries, was comparatively few when examining other targets. In terms of analysis the report examines how environmental (terrain) factors and the presence of and access to EI are related to the strategic targeting decisions of today's violent non-state actors (VNSA), be they criminal and/or political actors. (Analysts may seek to examine one particularly helpful reference, "Brave New War" by Robb in 2007. While not a book specifically on EI targeting, in it Robb frames EI attacks within a broader phenomenon of systems disruption and refers to the violent actor as "global guerrillas." With he does not systematically evaluate all of the EI attack data he does note an interesting trend and need to look at this tactic with a broader lens. In particular he pointed to how today's violent non-state actors toggle between different motivational spaces, from criminality to different expressions of political violence such as terrorism, and how they are leveraging their terrain in new, dynamic ways.)

Going forward, the Center for Security Studies in partnership with the Paul Scherrer Institute conceived of the Energy Infrastructure Attack Database (EIAD), a dataset that would set out to gather and structure open source information on threats to EI (by non-state actors). In doing so the project team set out to answer some of the following fundamental questions: In what regions/states is EI targeted? In regions where EI is targeted, what tactics, techniques, and weapons are used and how are they composed? What are the impacts of attacks (local and global)? Needless to say, knowing the answers to such fundamental questions can help illuminate who is targeting EI, in what situations is EI targeted, in what situations is EI not targeted (and if so why not), who is supporting the perpetrators, what is the purpose of attacks (political platform and/or economic gain), and finally poses the question 'are there universal patterns that can be distinguished that would point to a common ecology of targeting behavior as it relates to EI attacks?'

Introducing the Energy Infrastructure Attack Database (EIAD)

The Energy Infrastructure Attack Database (EIAD),is a non-commercial dataset that structures information on reported (criminal and political) attacks to EI (worldwide) since 1980, by non-state actors. In building this resource, the objective was to develop a product that could be broadly accessible and also connect to existing available resources. There has been an effort to forge a community around this effort, engaging experts to review EIAD's coding methodology as well as presenting the approach to the following groups: a 2011 workshop of the Thematic

Network on Critical Energy Infrastructure Protection (CEIP) of the European Commission; the energy security division of NATO's Emerging Security Challenges Division at NATO HQ, and a NATO/EAPC conference on "Emerging Security Challenges" in Tbilisi, Georgia.

In terms of EIAD's approach and methodology, the following definition of energy infrastructure is employed: energy infrastructure (EI) refers to all human (energy sector personnel), physical (energy sector physical assets) and information (energy sector cyber systems supporting operations) infrastructures in the following core energy sectors: petroleum, natural gas, coal, hydropower, nuclear, new renewables and electric grids.

This is a standard definition that has been created and is particularly unique in that it classifies energy sector personnel as energy infrastructure. This may raise some debate as 'humans' do not traditionally fall under the heading of infrastructure. However, for this dataset, energy sector personnel are part of the energy system and its functioning. In fact, in many cases, threats to energy sector personnel have led to disruptions in operations and production activities. In addition, in certain cases, the targeting of energy personnel can represent certain shifts in a group's targeting behavior. For example, during fieldwork conducted in the Niger Delta in 2010 authorities noted that when pipeline security improved (or tightened) then they would notice that targeting would shift to sector personal (particularly for kidnapping/ransom).

Using this definition, reported EI incidents are included that fall within the defined criteria were they successful, failed and foiled attacks as well as plots and threats to EI that (roughly) date back to 1980 (with the exception of a few incidents to this starting point) carried out by non-state actors regardless of motivation. In fact, another unique aspect of EIAD is that we do not code for motivation, rather we code for attack type (bombing, assassination, etc.) and instrument used (i.e. vehicle bomb, dynamite, gun, etc.). The decision to not code for motivation was based on experiences in reviewing incident info and discovering that the motivation of the perpetrator (which is oftentimes unknown/not reported) is not always obvious. In fact, when relying on open-source media reports (or second hand material in general), one of three things can happen. First, in some cases motivation can be clearly defined. Second in other cases motivation is implied or assumed (i.e. based on the group carrying out the attack). Third, and finally, in most cases it is simply unknown because information (on perpetrator, details of attack, etc.) is lacking. As opposed to having huge variance in this area, as well as errors in reporting, the issue of motivation is omitted and left for assessment by those who use the EIAD, particularly regional experts, for future case studies and analyses.

In terms of gathering information and sources for EI incidents, as stated open-source information such as news stories, journal articles, government reports, non-commercial databases, books, and other available online resources are accessed. Once information is collected cases are coded using the following main categories and sub-categories:

- Incident Date (including extended incidents such as hijacking & kidnappings)
- Incident Location (location, including geo-coded information)
- Incident Information (summary, event type, and whether an 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 & fatalities, reported downtime, infrastructure impact, hostage info)
- Additional Information

- Source Information (media reports, social media, cross-ref to other databases, etc.)

As the EIAD is in the final stages of coding and refinement, only some very general feedback on the information quality of coded incidents can presently be provided. Given that open-source materials are used, on which many non-commercial datasets draw from, the detail of available information varies. On one extreme, some cases have very basic information such as location of incident, attack type (i.e. bombing, armed attack, etc.), and general target info. On the other extreme, other cases (particularly high profile cases) have more complete information. In general, the key questions that originally informed the EIAD project can be addressed – namely: where attacks are taking place (and when), what sectors are commonly targeted (i.e. oil, gas, etc.) and what are the most common tactics.

Once coding is complete the project will move on to an analytical phase. For this it is envisioned that a mixed-method approach (qualitative and quantitative) will be applied. One area of research that the project has been inspired by and hopes to contribute to concerns recent studies that have focused on collective human activities - including violence and terrorist attacks - and found that they exhibit universal patterns, i.e. follow approximate power-law distributions. (For a description on this dataset see, Lujala, P. et al. 2007. Fighting over Oil: Introducing a New Dataset. Conflict Management and Peace Science, 24:239–256.)

Therefore, the quantitative analysis of EIAD's data will start with an assessment of the risk, which can be expressed as the product of frequency of an event and the resulting consequences (e.g. fatalities, casualties, EI impact, hostage/ransom, etc.). Frequency and consequences will first be analyzed separately because the former generally show little statistical variation, whereas the latter can span from events with very limited consequences but high frequency to low probability but high impact events. In a second step, Bayesian modeling will be applied so to address a key problem in risk estimation involving the scarcity of data resulting in high uncertainties. A key output of the quantitative analyses combining data exploration and modeling techniques will be the estimation of a broad range of risk indicators that can then support stakeholders in decision-making processes. Finally, geo-referencing of individual attacks will allow the visualization of data by means of mapping tools and Geographic Information System (GIS) software, which can then be subjected to geo-statistical analysis to identify spatial patterns and hotspots.

In all, the public release of EIAD will be in Fall 2012 and will be presented in the following two areas: first, EIAD's data will be uploaded to ETH Zurich International Conflict Research (ICR) group's new online data portal GROWup which offers a user-friendly interface to view and download empirical data on ethnic groups and intrastate conflict compiled by ICR as well as by data provided by partners – which include CSS (i.e. EIAD), PRIO, University of Essex and Uppsala University. Second, given that EIAD's incidents are geocoded they will be visualized on Google Earth where it will then be overlapped with other data layers such as PETRODATA (i.e. ONG onshore and offshore infrastructure such as pipelines).

Analyzing EIAD: current observations

A full analysis of EIAD will not be conducted until its launch; however, what can be highlighted are some observations based on data thus far assembled. As it currently stands there are 7,998 incidents in EIAD, though this number will likely change once the database is complete. 2012 data has not yet been coded and there is still some duplication in data from previous years as well as new cases which will be added during refinement. In general, of these 7,998 incidents, 3,597 have occurred between 2000 and 2011. While this would be an average of 327 per year,

the data shows that prior to 2004, less than 200 attacks occurred. Since then attacks have more than doubled reaching over 500 attacks at certain periods. In 2011 nearly 500 EI attacks, with a concentration of indents occurring in Colombia, India, and along the Afghan-Pakistan border were recorded.

An increase in EI attacks

What can account for such an increase? One assumption is that reporting of EI attacks has improved. Another assumption is that the targeting of EI is increasing in general due to instabilities in energy producing and transit zones. Within these zones tactics are introduced and, if successful, adopted by other actors creating a viral type effect. Of these attacks a majority of incidents are aimed at oil and gas infrastructure – primarily pipelines and mobile energy targets such as tankers and personnel, all of which are difficult to protect in a challenging host environment. Electricity infrastructure is also frequently targeted and there have been some attacks aimed at hydropower facilities. Full statistics on the targeting of energy sectors will be released upon EIAD's launch later this year.

Furthermore, within the last decade, another interesting observation that merits further analysis is the wave-like and contagion tendencies of EI attacks. For example, when we look at EIAD's data from 2000 to 2010 we see 4 prominent clusters of attacks.

- Cluster/Wave 1 late 1990s to 2002: Colombia
- Cluster/Wave 2 2003-07: Iraq
- Cluster/Wave 3 2006-09: Nigeria
- Cluster/Wave 4 2008-2011: Afghan-Pakistan (with smaller clusters in India and Colombia)

Each cluster demonstrates contagion of EI attacks within the specific period noted. This is not to say that during these periods EI attacks did not occur in other countries or regions but simply that they did not occur with the same intensity (frequency). Going back earlier in the dataset there are clusters of attacks but not with the same frequency or overlap.

To show the distribution of attacks, 70% have been geo-coded; using National Geospatial-Intelligence Agency Geonet Names Server (NGA-GNS) coordinates and integrated into the ICR Growup platform (see Image 1). The remaining 30% of the incidents that were not geo-coded include those that occurred in the United States (as these have not yet been geo-coded as of this writing) and/or where location information was incomplete. While these issues will be addressed in the coming months during refinement, the current picture provides an interesting snapshot of where EI attacks have taken place. Attacks are broadly dispersed across the globe, yet there are regions that have a higher density or clustering of attacks. As it concerns oil and gas infrastructure there is a correlation of incidents occurring in economically and politically unstable countries (such as Colombia, Nigeria, Iraq, Sudan, to name a few) that are concurrently oil and gas producers. The more recent addition to this list is Mexico where since 2007 there has been a general increase of EI attacks largely carried out by drug cartels.

This is not a remarkable finding as the relationship between conflict (or conflict-prone countries) and oil and gas production/export has been well documented, particularly by resource conflict scholars. However, when looking at the actual targeting of energy infrastructure in such contexts the correlation is not necessarily straightforward. For example, Nigeria has a history of conflict in the oil-producing region of the Niger Delta where VNSA – with political and criminal motivations - have increasingly turned to the energy sector as a primary target. This has manifested in attacks that speak to both areas: pipelines are attacked by criminal rings to steal

oil and sell it on the black market and these same pipelines are also attacked by political actors who seek to disrupt production and communicate grievances. On the other hand, in a country like Algeria, which is also a major energy producer/exporter, has as history of conflict, and large socioeconomic inequalities but it has not experienced major disruptions to its energy sector. In fact, when the Salafist Group for Preaching and Combat (GSPC) merged with al Qaeda and became the al Qaeda Organization in the Islamic Maghreb (AQIM) in 2006 an increase in threats to Algeria's energy assets given that al Qaeda had called for such attacks was expected. What the data in fact tells us is that its affiliates act differently. Granted, Algeria has made some significant investments in securing its energy assets and benefits from EI being located in less populated areas, but this does not fully explain AQIM's behavior. It is such comparative studies (between those with similar contexts but with different outcomes) that will provide some interesting insights into this area. It worth noting that no correlation between specific groups and attacks that involve electricity infrastructure seem to exist. Here a broad range of attacks being carried out in countries like France, Spain and the US (periods vary), where electricity infrastructure is targeted but these attacks are carried out by multiple and varied actors.

In terms of offshore attacks, that EIAD draws on data from the International Maritime Bureau (IMB) piracy report as well as the project team's own supplementary research (using news aggregators). This area has experienced an increase in attacks aimed at energy (specifically ONG) infrastructure. While offshore attacks also have a broad distribution, there appear to be 3 prominent clusters within the last decade:

- Cluster/Wave 1 early 2000s to 2005: Malacca Straits (Indonesian based)
- Cluster/Wave 2 2007 - Present: Gulf of Aden, Indian Ocean, Arabian Sea (contagions shift) (Somali based)
- Cluster/Wave 3 2009-Present: Gulf of Guinea (Nigerian based)

Lastly, the issue of coding cyber incidents has been a challenge. Cyber-attacks aimed at energy systems is a growing concern yet such incidents are clouded in a world of anonymity. There is an actor identification problem (i.e. unknown perpetrator - i.e. is it a state or non-state actor?) and an information problem. As cyber-security expert Myriam Dunn Cavelty recently noted in the German Times , "Sophisticated cyber attacks cannot be attributed to the perpetrator due to the architecture of cyberspace. This attribution problem refers to the difficulty of clearly determining who is initially responsible for a cyber attack. Attacks and exploits that seemingly benefit states might well be the work of third-party actors operating under a variety of motives. At the same time, the challenges of clearly identifying perpetrators also allow state actors to officially distance themselves from attacks."

The question then becomes, "How does a dataset like EIAD treat cyber incidents when the actor is typically unknown and, when information is lacking, nebulous, or contradictory? This is one of the major hurdles facing EIAD's development. As it currently stands, information is being collected on relevant cyber incidents and the project team is continuing to consult with experts with the hope that a solution can be found.

Finally, returning to the discussion on the viral tendencies of EI attacks theory from epidemiology may prove useful in helping to understand this better. In other words, one could

first look at which group/actor introduces the tactic (or, as referred to in public health, a virus) into a community/region and then analyze how it becomes a kind of epidemic can inform a methodology for dealing such viral characteristics of VNSA in sociological terms. Just like a disease, tactics do not emerge or spread in a vacuum rather they demonstrate a complex, interactive process between people and their environment. By understanding the factors that influence the targeting of energy infrastructure and by beginning to weigh them within specific contexts one might better understand how to better "contain" and "mitigate" EI attacks in resource rich, conflict-prone zones. Conversely, when looking at contagion/clusters, those communities or neighborhoods that express a particular resilience to violence (i.e. EI attacks are not adopted) might also provide instructive. This could be down by comparing the characteristics of different communities, such as socio-economic factors, political participation, social organization and capital, etc.

Snapshot of 70% of EI incidents coded in EIAD, using ICR Growup platform

Concluding thoughts

This article has sought to canvas the phenomenon of EI targeting and in doing so has identified research gaps that have led to the conceptualization and development of an EIAD. Preliminary insights bring to light the importance of EIAD's development and the type of research that this dataset can inspire. Once EIAD is launched, further research in this area will fully unpack and understand similarities and distinctions of energy infrastructure targeting. This can be in the development of a predictive tool that can be used to predict flashpoints and attack clusters (or hotspots) as well as more in-depth analyses of specific cases. For example, future studies may evaluate and weigh the different factors that influence targeting behaviors such as the location of EI (i.e. is it embedded in a populated area?), the security of EI (have the public and private stakeholders invested in securing/hardening the energy assets?), in the motivation and group characteristics of non-state actor/violent groups, and factors related to the political economy of EI attack location areas.

Contributor Jennifer Giroux is a Senior Researcher with the Center for Security Studies/ETH,

Zurich and contributor Peter Burgherr is a Team Leader with the Paul Scherrer Institute