Energy Security as a Subset of National Security

Chris Flaherty and Walter Leal Filho

Abstract Purpose The notion of energy security can be defined in one of two ways. It can be viewed as an economic concept or as a subset of national security. Viewed as a subset of national security, it allows for processes such as 3D vulnerability analysis to be used, which identifies areas of vulnerability in the physical infrastructure carrying energy from place to place. Some of these vulnerabilities can have national and international implications for a country's energy security.

Design/Methodology/Approach A conceptual framework for using 3D vulnerability analysis is presented as a methodology for collecting physical infrastructure vulnerability information. This can be used identifying areas of vulnerability—such as a particular section of transcontinental oil pipeline that if it was to fail would seriously weaken the energy security and ultimately national security of the country (or set of countries) reliant on it.

Findings The economic approach to energy security tends to be descriptive and frequently concerned with the price and supply measures of energy security. Approaches such as these, however, are not connected with the much broader national security and foreign relations policy realms. As well, the national security approach to energy security allows incorporation with Critical National Infrastructure Protection (CNIP) concepts, such as 3D vulnerability analysis. This method can be used to collect physical infrastructure vulnerability information, which can be used to identify potential threats to energy security (as a subset of national security).

C. Flaherty (✉)
Optimal Risk, London, UK

Soane Point, 6-8 Market Place, Reading, UK
e-mail: chris.flaherty@optimalrisk.com

W.L. Filho
Research and Transfer Centre, Applications of Life Sciences, Hamburg University of Applied Sciences, Lohbrügger Kirchstr. 65, Hamburg 21033, Germany

W. Leal Filho and V. Voudouris (eds.), *Global Energy Policy and Security*, Lecture Notes in Energy 16, DOI 10.1007/978-1-4471-5286-6_2,

Practical Implications The conclusions illustrate how concepts, such as 3D vulnerability analysis, can be used to achieve energy security. The 3D vulnerability analysis approach described collects physical infrastructure vulnerability information, which can be used to identify potential threats to energy security (as a subset of national security).
Originality/Value The paper provides a conceptual framework for looking at 3D vulnerability analysis and the relationship of this methodology to a wider understanding of energy security and ultimately national security.

Keywords Energy security • National security • Critical national infrastructure protection (CNIP) • 3D vulnerability analysis • Geographical information systems (GIS)

1 Introduction

The exact definition of national security, from a US perspective, and its relationship to concepts such as "energy security" is spread between two core US government documents. The US Department of Defense's Dictionary of Military and Associated Terms defines "national security" as a "collective term encompassing both national defense and foreign relations of the United States" (Director for Joint Force Development 2012). The US defense dictionary also lists concepts such as "national security interests," which includes in its listed definition the necessity "for fostering economic well-being" (Director for Joint Force Development 2012). Finally, there is the US President's statement on his National Security Strategy, which illustrates that energy security finds its way into the strategic approach to building the core foundations—economically and politically, as a component of national security (President of the United States 2010). From this perspective, energy security becomes a subset of national security concepts. An overview of this typology identifies three linked notions:

National security
Energy security
Vulnerability analysis

Looking at energy security from a purely economic view tends to focus on the association between national security and the availability of natural resources for energy consumption. As well, access to cheap energy is a given as being essential to the functioning of modern economies. It is also a given that the uneven distribution of energy supplies among countries can lead to significant vulnerabilities. However, there is also a much wider spectrum of energy security concepts. Various countries employ different strategies to achieve the same basic goal of energy security and ultimately national security.

Added to this typology is the concept of 3D vulnerability analysis (which will be discussed later). This is a "ground-level-and-view-up" approach, looking at the actual physical infrastructure which is carrying the energy. This process can be used to develop detailed information about the large-scale national and international vulnerabilities of the energy systems. This can be used as a road map to help achieve energy security. This is used to provide a security risk analysis of the built and fixed infrastructure environments as well as populate the analysis of potential threats to a country's (or group of countries) energy security.

The first part of this paper will look at energy security in an economic sense and then the broader national security approach to energy security. This examines how various countries have sought to achieve energy security. Finally, the concept of 3D vulnerability analysis is discussed.

2 Energy Security in an Economic Sense

As outlined by Winzer (2011) there are several competing definitions of supply security. They all include the idea of avoiding sudden changes in the availability of energy relative to demand. A common feature of current definitions is that they all warn against the risks of discontinuity in energy supply, which characterizes a scenario where energy provision is insecure.

The notion of energy security, in a purely economic sense, can be defined in many ways. For instance, it can be the capacity of a country to meet all its energy needs with the energy it produces itself or energy which it can reliably obtain from partners. But regardless of the definition one is inclined to use, energy security tends to be assessed along price and supply measures. This can be detailed, examining a "multipolar axis of physical, price, and geopolitical security." Typically, the concept of energy security entails understanding the risks inherent in the use of fossil fuels, particularly oil for transport and gas for electricity generation and heating. Each of these elements entails specific risks and potentials.

Energy consumption worldwide has steadily increased over the past three decades and has presently reached substantial levels, as is illustrated in Table 1, which provides an overview of energy consumption from selected countries. This state of affairs means that energy issues not only are central to economic development but have also evolved to be matters of national security.

Table 1 shows that for countries such as the UK, Germany, Russian Federation, China, and the USA over the next 20 years, energy consumption will continue to increase. From an economic view the classical problems, which affect national security, will be the availability of natural resources for energy consumption and access to cheap energy. As well, it can be anticipated that the uneven distribution of energy supplies among countries will and can lead to significant vulnerabilities, such fuel shortages causing economic and political instability. For instance, in respect of energy, it is known that the EU meets about 50 % of its energy needs through imports. This is likely to increase to 70 % by 2030. Such dependence leads to various economic, social, ecological, and physical risks for the EU since a suspension of supply from one of the sources would have severe consequences to the economy of member countries.

Table 1 An overview of energy consumption in selected countries

Energy consumption in million tonnes of oil equivalent (MTOE)			
Region	Current (MTOE)	Projection (MTOE)	Difference (%)
UK	137.50 (2009)	148.065–167.037 (2030)	108–122
Germany	213.28 (2009)	199.255–194.976 (2030)	93–91
Russian Federation	991.0 (2008)	1,375.0–1,565.0 (2030)	139–158
	422.834 (2009)		325–370
China	1,432.986 (2009)	3,280.8 (2030)	224
	2,275.00 (2010)		144
US	2,380.02 (2009)	2,653.26–2,797.90 (2030)	111–118
	1,462.524 (2009)		181–191

International Energy Agency (2011)

In geopolitical terms, 45 % of oil imports come from the Middle East, and 40 % of natural gas imports come from Russia. The EU does not yet have all the necessary means to influence the international market and is at the mercy of suppliers. This weakness was highlighted by the sharp rise in oil prices at the end of 2000. As a means to steer against this trend, it prepared a Green Paper on the security of energy supplies (CEC 2000), which is still being implemented today. One solution recommended by the Green Paper is to draw up a strategy for security of energy supply aimed at reducing the risks in terms of supply, quantities, and price, linked to this external dependence. However, this is just one way of understanding “energy security” as a concept; in the next part, a much wider spectrum of energy security concepts is overviewed. Various countries employ different strategies to achieve the same basic goal of energy security, and these different approaches provide a much broader characterization of the concept of energy security, as a subset of national security.

3 How Various Countries Achieve Energy Security

As was introduced in the introduction, the concept of national security can be defined “to include, not only defence, but also state craft, foreign relations, and economic policy” (Kaufmann 1988; Flaherty 2003). National security is also “a central component of public policy” (Edwards and Walker 1988). The concept of national security changed significantly in the last decade of the twentieth century. The most notable change has been an extension beyond international relations concepts to incorporate domestic individual security as well as the earlier ideas of national defense. In short, many countries adopt strategies, policies, and military action under the mantel of energy security, which provides a much broader characterization of the concept, as a definition in its own right. The broad spectrum of coverage has significance especially when the various strategies used by countries that seek to achieve a notional concept of energy/national security are examined.

The core concept of national and energy security has also of late been extended and somewhat redefined by the more encompassing notions of National Power and Homeland Security, which have all developed into partly interchangeable concepts; and these ideas over span the more conventional concepts such as that of the economy or national defense (President of the United States 2010). Under this approach, specific concepts such as “energy security” very much represent building blocks for the direct operation of supra-concepts such as Critical National Infrastructure Protection (CNIP—which most countries now use some variation[1]), which is largely concerned with the problem—as to how to best structure a methodology for developing a vulnerability—based on security risk assessment that can show how various threats can impact on the infrastructure systems that a country, or group of countries, relies vulnerability -based security risk assessment.

The passing of the US Homeland Security Act of 2002 represents a radical transition between an extraterritorial notion of national security and expansion of the concept into the civil domain (Flaherty 2003). The US Homeland Security Act merged a large number of US Government agencies into one entity. This entity was not only intended to deal with the traditional defense-related areas of national security but also nontraditional areas such as internal US security, its law enforcement, borders, as well as trade, investment, and energy security (however that may be defined, in the context of future US President’s policy initiatives).

The notion of energy security takes on many manifestations; it becomes linked to foreign policy, defense, or various trade and investment strategies. For instance, China since the period of economic reform in the 1980s in order to achieve energy security has developed overseas corporations engaged in foreign investment and reliant as well on nationalist Chinese overseas business networks to facilitate these trusted relationships (Flaherty 2002). This strategy was intended to ensure that China in the twenty-first century will have access to important energy stocks and the transport of these into China securely. The Chinese government in the 1990s, in response to the rise in energy consumption (Yang 2011), as well as the political perception that China’s domestic petroleum resources are far from sufficient to sustain its economic growth (Webber et al. 2002), decided to let its state-owned petroleum companies seek access to overseas supplies of oil and gas through investment. The focus of which has largely been a continental-based strategy. The most significant areas are Russia (Siberia gas fields) and the central Asian

[1] The US Presidential directive PDD-63 of May 1998 set up a national program for “Critical Infrastructure Protection.” In Europe the equivalent “European Programme for Critical Infrastructure Protection” (EPCIP) refers to the doctrine or specific programs created as a result of the European Commission’s directive EU COM (2006) 786 which designates European critical infrastructure that in case of fault, incident or attack could impact both the country where it is hosted and at least one other European member state. Member states are obliged to adopt the 2006 directive into their national statutes. In the UK, the same concept developed as CPNI, or the governmental authority—“Centre for the Protection of National Infrastructure”—that mandates critical infrastructure protection strategies for the UK.

republics especially of Kazakhstan (where China has two oil fields) and Turkmenistan (gas resources).

Maritime countries such as Australia have fundamentally focused on energy security as a justification for key foreign policy decisions, such as to ally with the USA, in regard to the war on terror in Iraq and Afghanistan (post-2001), seeing instability in these regions as a fundamental national threat to vital sea trade routes that carry their energy needs (Nelson 2007).

The Russian Federation, in particular, has long acknowledged the links between energy and security (Ministry of Energy of the Russian Federation 2010). As well, the Russian Federation has linked energy security to its military policies, adopting a continental strategy. The post-2000 revival of Russian Federation military capability has been aimed at ensuring capacity to project conventional forces efficiently within the Eurasian land mass and possibly beyond (House of Commons 2009). This seems to now be linked with energy security, as this has been recently identified as an area of common interest under the US reset policy agenda and the NATO-Russia Council Joint Review of Common Security Challenges, underpinning renewed US and NATO cooperation with Russia (Johnson 2011). In the case of Russian foreign policy, it has been suggested that energy security and military capability are used interchangeably in order to build capacity to dominate vital energy routes (carrying oil and natural gas) throughout Eastern Europe (Paillard 2010).

In the military context, there has been a focusing on the capability that can destroy or disable national energy systems as a means to compel a nation. Known as graphite bombs, these were first used against Iraq in the Gulf War (1990–1991) to knock out 85 % of the electrical supply. Similarly, later versions of these were used by NATO against Serbia (in May 1999), disabling 70 % of that country's power grid. In the later stage of Operation ALLIED FORCE, the NATO air force used conventional bombs and rockets to target power high lines and transformer stations (Lambeth 2001). Saudi Arabia and Iraq have similarly seen insurgency and terrorist constantly attack and destroy oil facilities, as a strategy to overwhelm the government (Al-Rodhan 2006; IAGS 2012). The Islamic Republic of Iran Navy (IRIN) and the Iranian Revolutionary Guard Corps Navy, which is now primarily tasked with securing Iran's interests in the Persian Gulf region, have both clearly developed capability intended to compromise shipping. The IRIN has developed a flotilla of domestically produced Ghadir-class midget submarines, while the Revolutionary Guard has some 1,500 boats and fast attack boats, armed with a variety of antiship missiles intended to harass shipping. These capabilities, combined with minelayers, allow for a repeat of the 1984–1987 phase of the Iraq–Iran war dubbed the "Tanker War."

These later examples of the various military campaigns and weapon systems aimed at energy transport are more than just threats; these form part of a well-defined military strategy, aimed at the destruction of a country's national capacity. Examples such as these show a multitude of ways that countries employ to achieve the same basic goal of energy security, and these different approaches provide a much broader characterization of the concept of energy security. The notion of energy security takes on many manifestations linked to foreign policy, defense, or various trade and investment strategies. The question becomes how can we identify national security threats relating to the supply of energy staples oil and gas. This could, for instance, be the risks associated with critical transport nodes, such as the Straits of Hormuz, Malacca Straits, and the Suez Canal. However, in order to identify those risks, one approach is a "ground-level-and-view-up" one, looking from a physical vulnerabilities perspective, which helps identify security risks, threats as well as mitigation strategies. However, in order to have truly national security implications, this process for vulnerability analysis has to be conducted on a sufficient national/international scale.

4 Vulnerability Analysis

Identifying some of the key physical built-environment risks involved along various paths for transporting energy such as oil and gas can be problematic. For instance, "on the path" of energy in transit from the supplier to the consumer country:

> "An ideal way of capturing this kind of risk would be to account for the exact path of each energy import flow into each consuming country, e.g., whether the energy is exported through vulnerable areas, whether alternative transport routes are available, and so on. However, to our knowledge such data are not available." (Le Coq and Paltseva 2009)

However, supra-concepts such as CNIP were specifically created to deal with this exact problem. This is where 3D vulnerability analysis comes into play—as it is supposed to be creating the data needed to do this. The problem is how to overcome the complexity such as that found across Europe and globally as there are multiple regulatory and technologically disparate subsystems—all involved in the transport of energy. The failure of the weaker ones can threaten any country's national and international "horizontal" linkages that work across its energy supply system. In many cases over which, it may exert little or no control.

5 The European Union Concept of "Horizontal Convergence" for Infrastructure Protection

The EU concept of "horizontal convergence" (CEC 2006) for infrastructure protection justifies the use of 3D vulnerability analysis. The original 2006 Commission of the European Communities "proposed council directive" outlined the need for:

- The "identification and designation of European critical infrastructure"
- The assessment of the need to improve their protection
- Further identified that these needed a "horizontal framework," for this identification (CEC 2006)

The phrase "horizontal convergence" is a borrowing from economic geography, identifying in addition to the vertical integration of European supply systems; there was also a need to understand the "horizontal" linkages which reside within individual member countries and which crisscross these. This is intended as a means to identify multiple regulatory and technologically disparate EU member states and the aspiration to collect uniformly and ultimately share similar levels of critical infrastructure protection, via the technology convergence currently being experienced.

The same "horizontal convergence" analogy provides a starting point for developing a 3D vulnerability analysis for energy security focused on identifying the weaknesses and threat points embedded within national and extraterritorial linked infrastructure. The argument is there can be uneven development of various lengths of infrastructure identified across Europe. These contribute to vulnerabilities that can substantial raise the security risk index for other member countries relying on the successful transportation of energy staples via these less reliable paths. Adaptation of methodologies, such as the "3D analysis box" (Flaherty 2010), for use in the analysis of these vulnerabilities, can contribute to solving this very problem.

6 3D Vulnerability Analysis: Micro- Versus Macroanalysis

A macrolevel economic view of energy security argues:

> "The composition of energy imports also matters for security. If energy imports are well diversified, the consuming country faces a smaller risk of supply disruption than if all its energy imports come from a single supplier, other things equal. Therefore, one needs to account not only for the overall contribution of imported energy into the consuming country's energy portfolio, but also for the diversity of the energy suppliers that contribute to these imports."

Typically it is argued that "other things equal, suppliers that constitute a larger share of country's energy imports potentially may cause more problems for energy security." Another way of looking at this argument is that a further level of inquiry could be added overlaying the macrolevel economic view, with a microlevel vulnerability survey of the system that is actually being used. In some cases, it may well be found that the potential vulnerabilities actually reverse the proposition—"suppliers that constitute a larger share of a country's energy imports potentially may cause more problems for energy security"—as it could be found that this particular supplier is functioning and that other potentials (the diversified pool of suppliers) actually represent a source of higher security risk, as their actual transportation of the energy is highly compromised; thus, there is a higher than acceptable level of energy/national security vulnerability.

Notionally, three-dimensional or "3D" vulnerability analysis seeks to look at the full volume of space, understanding complex simultaneous factors as well as incorporating time and location factors (Flaherty 2007). The 3D vulnerability analysis techniques are intended to sit under the mandate of CNIP and enable security risk scenarios to be developed. The core aim of which is to "produce" the information (identifying the vulnerabilities) necessary to begin the security risk management cycle, and this applies equally to the question of energy security, either at macro- or microlevels (Flaherty 2007).

The application of the “3D analysis box” (Flaherty 2010) has been designed as a practical aid to achieving the monumental task of assessing vast infrastructure systems, particularly the transportation paths taken such as pipelines and tankers as well as developing an “index” of security risk for energy transport which could feed into the “energy policy topic” in terms of resilience and security of energy imports (for consumers) and exports (for exporters). This can be developed as a security risk or threat model based on the Commission of the European Communities identification of “horizontal convergence.”

The 3D vulnerability approach is simple; it is a question-based audit seeking to identify individual vulnerabilities or “fail characteristics” (as these can be known). These are identified in a question-based survey—seeking to identify weak systems linkages or weaknesses in the building frames, fabric, or structures. Once identified, these can all be measured in order to illustrate the possible range of consequences, if these vulnerabilities were to be enlivened, either through an act of nature, or deliberately (terrorism, war, etc.), or accidental human intervention. Applied to the problem of energy security, the 3D vulnerability analysis approach looks at the various stages of a path for the transportation of a particular energy staple. This is built into a multistage and multi-segmented 3D vulnerability analysis of the whole system. The purpose is to illustrate multiple clustering of vulnerabilities which indicate key areas, as well as key hubs along transportation paths for energy transport, connecting a country’s energy supply system transnationally. This would identify vulnerability, as it arises from:

1. Clustering
2. When (time-wise) these are stable or unstable
3. Likely points of attack or places where accidents could make this happen
4. How at various times vulnerabilities can appear or disappear

One criticism is that the analysis is specifically microlevel in focus. However, some identified vulnerabilities will be significant from a national security view (at a macrolevel) and others not—as some infrastructure vulnerabilities only ever have local effects that cannot impair energy transport nationally, or internationally, and therefore are not national/energy security issues.

In the case of 3D vulnerability analysis, the object is to illustrate the “how” and the “why” when multiple consequences manifest from failings in systems, buildings, or places. This could be a single failing, or it could involve complex multiple failings simultaneously that are below the visible surface, such as embedded within the infrastructure itself—where a clustering of possible fails could compromise each other. This involves a dynamic approach to modelling, involving factors such as time and phase.

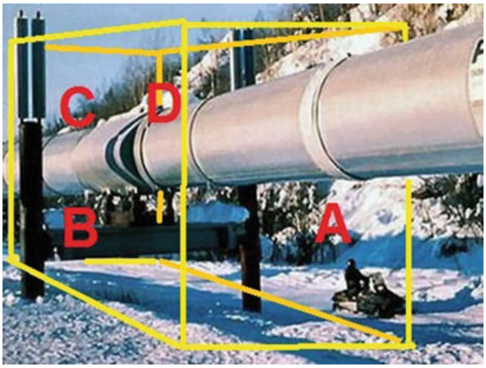

Fig. 1 Illustration of the 3D box technique in regard to a section of the Odessa–Brody oil pipeline

7 Illustrating the 3D Vulnerability Approach: A Simple Model

The "3D analysis box" (Flaherty 2010) is a classical technique illustrated in Fig. 1. This technique also incorporates "cluster modelling" and "linear modelling" (Flaherty 2007). The following is a simplified example of how the 3D vulnerability analysis could be undertaken, in relation to a desktop analysis of a photograph taken of some section of the current Odessa–Brody oil pipeline (using the 3D analysis box).

Illustrated in Fig. 1 is a picture of a segment of Odessa–Brody oil pipeline. This particular example demonstrates some key vulnerabilities and the zone of potential threat, as the greatest concentration or clustering of key assets that can be damaged, during an event (such as an explosion). The 3D analysis box has been overlaid as a technique to assist focusing and identifying key physical vulnerabilities during a simple survey. For instance, the types of vulnerabilities, which could be identified within the oil pipeline's physical structure (which may be seen in this particular example) are the pipeline itself, as well as individual joinery/banding sections (Fig. 1: A); the aboveground piers and pipe's supporting connector beam (Fig. 1: B, C); and clamping system (Fig. 1: D). An attack on this cluster renders the greatest damage and cost, as opposed to attacking the pipe on its own.

8 A Horizontal Convergence Approach: GIS Applications

A horizontal convergence approach to the simple model illustrated in Fig. 1 would entail the upscaling into multistage and multi-segmented 3D vulnerability analysis illustrating multiple clustering, as well as key cluster hubs along transcontinental infrastructure. *The main requirement is for an evidence-based approach to* *understanding multiple vulnerabilities that can link consequently to create a hazard impacting on the operation of a site or the safety of people located there. However, attempting to map these consequences, especially those that occur simultaneously across a site, presents a fundamental problem for undertaking vulnerability and counterterrorist assessments.*

The 3D vulnerability analysis approach is a look "ground-level-and-view-up" from a physical vulnerabilities perspective, which helps identify security risks, threats as well as mitigation strategies. In order to have truly national security implications, this process for vulnerability analysis has to be conducted on a sufficient scale to actually have national and international implications. The core aim of vulnerability analysis is to "produce" the information or data necessary to begin the security risk management process, as outlined in various international standards, as this ultimately leads back to the supra-concepts of CNIP, and national security considerations. In addition to which, the following can be added:

- The consequence analysis is merged with an effective tactical analysis, which may include identifying a likely terrorist operational plan (where the analysis is focused on counterterrorist assessments).
- The assessment is intended to be developed as a Geographical Information Systems (GIS) approach, visualizing the vulnerability-risk-threat-security profile, from a CNIP/national security perspective.

The versatility of these types of GIS-based approaches is that these can easily accommodate any volume of data, drawn from a wide variety of sources—such as on-the-ground inspection of actual lengths of infrastructure identifying the vulnerabilities—which then gets swept up into the information, or data matrix, which produces an "index," such as the rating of areas of higher levels of vulnerability. In practice, data about consequences is sourced from a wide examination of the building, system, or space, closely following the question methodology typically derived from the international or US governmental standards such as the FEMA 426 Reference Manual: Chapter 1.6 "Building Vulnerability Assessment Checklist (US FEMA 2002)" or that used by the UK Government National Counter Terrorism Security Office (NaCTSO)'s Vulnerability Self Assessment Tool (VSAT) (NaCTSO 2012).

9 The Concept of Vulnerability: Some Final Comments

Some physical vulnerabilities are not fixed, as these may only occur during particular times and in conjunction with other events (Flaherty 2004). For example, key vulnerabilities may only arise in the segment of Odessa–Brody oil pipeline, illustrated in Fig. 1, in times of peak usage of the pipeline or in circumstances where there is accessibility to the line, as represented by presence of the snow ski driver. Environmental issues may also come into play that coincide with peak usage. For instance, severe cold could weaken the structure, through weathering and fatigue.

The vulnerability information or data collected in a survey can reveal significant clusters of related vulnerabilities (which are the individual "fail characteristics" identified in a question survey). These can be used to illustrate a range of potential security risks or impacting consequences. In the case of 3D vulnerability analysis, the object is to illustrate the "how" and the "why" of multiple consequences and failures occurring simultaneously when many clustered structural and systems vulnerabilities mutually compromise each other, during some even such as an explosion. Essentially, this is a dynamic modelling approach, as factors such as time and phase are important considerations.

10 Conclusion

The aim has been to present a conceptual approach to energy security, linking it to an alternative definition as a subset of national security concepts. The notion of energy security can be defined in one of two ways. It can be viewed as an economic concept or as a subset of national security. Viewed as a subset of national security, it allows for processes such as 3D vulnerability analysis to be used. 3D vulnerability analysis can identify areas of vulnerability in the physical infrastructure carrying energy from place to place, and some of these vulnerabilities can have national and international implications for a country's energy security.

3D vulnerability analysis itself is derived from supra-concepts such as CNIP. The paper provides a conceptual framework for looking at 3D vulnerability analysis, as a methodology for collecting information or data that allows a security risk analysis to take place at a microlevel, and this information informs the macrolevel relationship between various aspects of critical infrastructure—such as a particular section of transcontinental oil pipeline that if it was to fail would seriously weaken the energy security and ultimately national security of the country (or set of countries) reliant on it. One of the key aims of 3D vulnerability analysis is to provide "a set of definitions and observations" (Flaherty 2010). The approach is intended to build up a picture "from the ground-up" of the vulnerabilities and major clustering of these for built or physical infrastructure or systems. This then enables analysis of multiple consequences and multipolar risks using GIS-based methodologies, such as cluster modelling and linear modelling.

The core aim of vulnerability analysis is to "produce" the information or data necessary to begin the security risk management process, as outlined in various international standards, as this ultimately leads back to the supra-concepts of CNIP and national security considerations. The versatility of these types of GIS-based approaches is that these can easily accommodate any volume of information or data, drawn from a wide variety of sources—such as on-the-ground inspection of actual lengths of infrastructure identifying the vulnerabilities—which then gets swept up into the data matrix, which produces an "index" of the critical areas of vulnerability in the physical infrastructure that carries energy from one place to the next.

Developing a horizontal approach (in line with the EU policy concepts underpinning CNIP) to energy supply paths, given the scale of these, entailing transcontinental and global linkages requires the upscaling of the basic 3D vulnerability analysis, with the use of the "3D analysis box" into multistage and multi-segmented 3D vulnerability analysis. These would illustrate issues: multiple clustering as well as key cluster hubs along transcontinental infrastructure. The aim would be to help identify vulnerability phenomena, as they arise from clusters, when these are stable/ unstable, as well identifying the point of an attack designed to make this happen (and various relevant timescales).

The "3D analysis box" provides a reproducible methodology, focused on cutting complex infrastructure paths into components that can be analyzed individually or in groups in order to illicit security risk information or data (within a GIS-based framework). This is actually (or should be) the "breadmeal" of core national CNIP programs in terms of identifying the risks in the system. Namely elements such as (1) autonomous and heterogeneous agents, (2) organizational relationships, (3) nonlinear dynamics, (4) knowledge levels, (5) local interactions, and (6) the explicit space these occupy geographically, along the lengths of transcontinental infrastructure that not only has energy security but the national security needs of a country firmly in sight.

References

Al-Rodhan KR (2006) The impact of the Abqaiq attack on Saudi energy security. Center for Strategic and International Studies Arleigh A. Burke Chair in Strategy, Washington, DC. Revised 27 Feb 2006. http://www.csis.org/files/media/csis/pubs/060227_abqaiqattack.pdf

Commission of the European Communities (CEC) (2000) Commission Green Paper of 29 November 2000 towards a European strategy for the security of energy supply, COM(2000) 769. CEC, Brussels

Commission of the European Communities (CEC) (2006) Proposal for a directive of the council on the identification of European critical infrastructure and the assessment for the need to improve their protection (12 Dec 2006, COM-2006-787-Final), 7. CEC, Brussels

Director for Joint Force Development (J-7) (2012) Joint Publication 1–02: Department of Defense Dictionary of Military and Associated Terms (8 Nov 2010; as amended through 15 Apr 2012), p 220

Edwards GC, Walker WE (1988) Introduction. In: Edwards GC III, Walker WE (eds) National security and the U.S. constitution: the impact of the political system. Johns Hopkins University Press, Baltimore, MD, p 1

Flaherty CJ (2002) Australian-Chinese business networks: a case study of the role of networks used to organise trade between firms in Melbourne (Adelaide) and Shanghai. Ph.D. Thesis, University of Melbourne, School of Anthropology, Geography, and Environmental Studies, 2002. UniM Bail T. Call No. FLAHERT

Flaherty CJ (2003) Australian national security thinking. Def Force J (May/June, 160):3–10

Flaherty CJ (2004) Decisive strike, criticality and homeland security. Def Force J (164):43–50

Flaherty C (2007) 3D tactics: an advanced warfare concept in critical infrastructure protection. Int J Emerg Manage 4(1):33–44

Flaherty C (2010) Command, influence and information in 3D tactics. J Inf Warf 9(1):18–31

House of Commons (UK) (2009) Russia's Military Posture, Research Paper 09/35. House of Commons Library, London, Apr 2009, p 68. http://www.publications.parliament.uk/pa/cm200809/cmselect/cmdfence/276/27605.htm#n48

Institute for the Analysis of Global Security (IAGS) (2012) Iraq pipeline watch. http://www.iags.org/iraqpipelinewatch.htm

International Energy Agency (2011) 2011 Key world energy statistics. IEA, Paris

Johnson JD (2011) Developing better relations. Armed Forces J 148(8):14–17, http://www.armedforcesjournal.com/2011/04/5786296

Kaufmann WW (1988) Forward. In: Edwards GC III, Walker WE (eds) National security and the U.S. constitution: the impact of the political system. Johns Hopkins University Press, Baltimore, MD, VIII

Lambeth BS (2001) NATO's Air war for Kosovo: a strategic and operational assessment. RAND Research (MR-1365-AF)

Le Coq C, Paltseva E (2009) Measuring the security of external energy supply in the European Union. Energy Policy 37(11):4474–4481

Ministry of Energy of the Russian Federation (2010) Energy strategy of Russia for the period up to 2030. Ministry of Energy of the Russian Federation, Moscow

Nelson B (2007) Australia 'Has Iraq Oil Interest'. News BBC (Thursday, 5 July 2007). http://www.news.bbc.co.uk/1/hi/world/asia-pacific/6272168.stm

Paillard CA (2010) Rethinking Russia: Russia and Europe's mutual energy dependence. J Int Aff 63(2):65–84

U.K. Government, National Counter Terrorism Security Office (NaCTSO) (2012) Vulnerability self assessment tool (VSAT). http://www.nactso.gov.uk/OurServices/VSAT.aspx

U.S. Federal Emergency Management Agency (2002) FEMA 426 reference manual: a how-to guide to mitigate potential terrorist attacks against buildings (Dec 2002), Chap 1–45. U. S. Federal Emergency Management Agency, Washington, DC

U.S. Homeland Security Act of 2002. US Government, Washington, DC

U.S. President of the United States (2010) National Security Strategy. The White House (May 2010). http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

U.S. Presidential Directive PDD-63 of May 1998

Webber M, Wang M, Ying Z (eds) (2002) China's transition to a global economy. Palgrave Macmillan, New York, NY, p 53

Winzer C (2011) Conceptualizing energy security (EPRG working paper 1123, Cambridge working paper in economics 1151). Cambridge University, Cambridge

Yang J (2011) China's energy consumption rises. Wall Street J. http://www.online.wsj.com/article/SB10001424052748704615504576171922168262078.html

Chris Flaherty is a PhD graduate from the University of Melbourne in 2002. Based in London since 2008, he is an active contributor on security, terrorism early warning, and related international intelligence issues. He is currently involved in developing a "Scripted Agent Based Microsimulation Project" (University of Wollongong NSW, Australia). He currently specializes in the area of Mass Gathering Vulnerability analysis in the UK and the USA. He advises on risk analysis projects for building facilities. His work covers a broad spectrum of risk-related endeavors including resilience, counterterrorism, critical infrastructure protection, 3D tactics, fragmentation, and vulnerability analysis.

Walter Leal Filho Prof. Dr. (mult.) Dr. h.c. (mult.) is Senior Professor and Head of the Research and Transfer Centre Applications of Life Sciences, Hamburg University of Applied Sciences in Germany.

http://www.springer.com/978-1-4471-5285-9

Global Energy Policy and Security
Leal Filho, W.; Voudouris, V. (Eds.)
2013, VIII, 330 p. 72 illus., Hardcover
ISBN: 978-1-4471-5285-9