# Terrorists versus the Sun: Desertec in North Africa as a case study for assessing risks to energy infrastructure

**Karen Smith Stegen (a), Patrick Gilmartin (b) and Janetta Carlucci (c)**
a. Jacobs University Bremen, Campus Ring 1, Bremen 28759, Germany.
b. The Fletcher School of Law and Diplomacy, Tufts University, Medford, Massachusetts, USA.
c. Hertie School of Governance, Berlin, Germany.

*This is an Accepted Manuscript of an article published by Macmillan in the journal Risk Management in 2012, available online:* http://www.palgrave-journals.com/rm/journal/v14/n1/abs/rm201115a.html.

*To cite this article: Karen Smith Stegen, Patrick Gilmartin, and Janetta Carlucci (2012): Terrorists versus the Sun: Desertec in North Africa as a case study for assessing risks to energy infrastructure. Risk Management, 14, 3-26.*

**Abstract** As renewable energies gain both in importance and in share of the global energy mix, questions arise as to whether they will face the same energy security challenges – such as terrorist attacks – that have confronted the oil and gas industry. This article addresses the risk of terrorism to the infrastructure associated with renewable energies and electrical power systems and transmission lines. It reviews the capacities of various risk assessment tools and analyzes the potential terrorist threat to the Desertec concept, which envisions meeting 15 per cent of Europe's electricity demand by 2050 with renewable energy sourced from the Middle East North Africa region. Some industry observers have already voiced grave concerns about potential European dependence on this region, specifically because of the presence of terrorist groups, including Al Qaeda, which was responsible for the 2001 attacks in the United States. The data for the Desertec case study analysis are partly informed by a series of interviews conducted with correspondents located in Europe and in North Africa.

**Keywords:** terrorism; critical infrastructure; Desertec; energy; power transmission; North Africa

[page 3]

**Introduction**

Dwindling reserves of fossil fuels and the prospect of massive global warming have helped drive the push for sustainable sources of energy. In 2010, global solar capacity grew by 73 per cent and

[page 4]

wind capacity by nearly 25 per cent. Overall, global consumption of renewable energies increased by 15.5 per cent (BP, 2011). As renewable energies gain both in importance and in share of the global energy mix, questions arise as to whether they will face the same energy security challenges confronting fossil fuels (Criekemans, 2011). The oil and gas industry, for example, has often been the target of terrorist attacks. Indeed, an analysis of the Global Terrorism Database, which systematically tracks terrorist attacks, reveals that the per- centage of terrorist attacks targeting the energy sector has risen in recent years, from 25 per cent of all attacks in 2003 to 35 per cent in 2007 (Giroux, 2009).

Several scholars have discussed the risks to renewable energy, and a few have zeroed in on security risks (Komendantova *et al*, 2009; Toft *et al*, 2010). This article seeks to launch a discussion of how to analyze terrorist threat to energy infrastructure – specifically renewables and electric power – by assessing the capacities of various risk tools and subsequently applying these tools to a case study: the Desertec concept as deployed in the Middle East North Africa (MENA) region. The Desertec vision comprises powering the world's energy demand with renewable energy sourced via transmission lines – which in many cases would be both long and across international borders – from the world's deserts (this concept will be hereafter denoted as 'Desertec'). Desertec made international news in 2009 when the Desertec Foundation and 12 companies founded the Dii (originally the Desertec Industrial Initiative), which asserts that by 2050 the European Union (EU) would be able to import 15 per cent of its electricity from MENA countries.

The Dii's initial focus has been on North Africa, where the terrorist group Al Qaeda is known to have a presence (Lipton, 2007; BBC, 2009; Hansen and Vriens, 2009). Critics have already vociferously expressed their fears about European dependence on North Africa. As the CEO of *Bloomberg New Energy Finance* declared, 'I am not sure we want to be dependent on North Africa for our electricity supply when anyone with a shoulder-launched missile can take out the electricity supply for Europe' (Beckman, 2010). As it is planned to replicate the Desertec EU-MENA concept around the world, these concerns over dependence on foreign countries for electricity may rise again and again. A general framework is needed that can contrast the security risks of differ- ent types of projects, such as the risks of importing electricity from Morocco versus Egypt, or the risks of importing electricity from MENA versus natural gas from Russia. The foreign policy and security concerns that accompany energy dependence on foreign

countries means that policymakers and industry executives will inevitably face tough decisions about risks for specific projects. Thus, a framework must also allow for the comparison of different categories of risks so that scarce resources can be appropriately allocated for mitigation and adaptation. With this article, we contribute to the literature by approach- ing terrorism risk analysis for critical energy infrastructure with an analytic

[page 5]

structure that both covers the specific risks involved in large energy projects and offers sufficient flexibility to be applied in a wide variety of energy project scenarios around the world.

**Desertec Overview**

The Dii's goal is to enable and facilitate the development of renewable energy sourced from the world's deserts, starting with the MENA region. The plan is to lay the groundwork (for example, regulatory, political, commercial) and to encourage governments and industry to install power plants utilizing a portfolio of renewable energy technologies, particularly concentrated solar power (CSP). The hope is that, eventually, the MENA region would be able to export excess power to Europe, primarily through High Voltage Direct Current (HVDC) transmission lines (for more detail on the Dii's plans and on the technologies, see Figure 1, as well as www.dii-eumena.com and www.desertec.org). The MENA region would benefit from a boundless energy supply and a heat source for the desalination of water, both of which would support its projected eco- nomic and population growth, whereas Europe would benefit from emissions-free electricity and a diversification of its power supply.

To supply 15 per cent of Europe's forecasted load in 2050, about 700 terawatts/year of solar electricity would have to be transmitted via HVDC

**Figure 1**: Potential Configuration of HVDC lines connecting EU demand centers with CSP sites in MENA.
*Source*: Trieb *et al* (2009, p. 124), German Aerospace Center

[page 6]

lines (Trieb and Müller-Steinhagen, 2009). As higher irradiation levels increase efficiency and cost effectiveness, site selection is of utmost importance. Using Geographic Information System techniques and a variety of filters (including direct normal irradiance and existing access to power transmission infrastruc- ture), Ummel and Wheeler (2008) arrived at a list of five preferred sites in Morocco, Libya, Egypt, Saudi Arabia and Jordan.
Renewable energy activities in North Africa have already begun to move forward, particularly since the announcement of the Dii's founding. In the past few years, a number of projects have been developed or proposed in the region, including several integrated solar combined cycle plants (Wiese *et al*, 2010) and a 500-megawatt solar power plant in Morocco, the first of several planned (Alternative Energy Africa, 2010; Norton Rose Group, 2010). The Dii has further selected Morocco as the location for its first reference project: In June 2011, the Moroccan Agency for Solar Energy (MASEN) and the Dii signed a cooperation agreement to develop a project, which will 'demonstrate the feasibility of the export of solar generated electricity to Europe'. MASEN will operate as project developer and the Dii as 'enabler' (Dii, 2011).
Transmission planning is also progressing. For realization of the full Desertec vision, the HVDC lines will be a necessary and significant investment. Although there are several projects in various stages of development, only one interconnection currently exists between Europe and North Africa: the Morocco–Spain alternating current (AC) submarine cable, commissioned in 1997 with commercial operation commenced in 1998 (a second line was added in 2006). Until 2013, this link is expected to be *the* export corridor for any North African electricity exports (Granadino and Mansouri, 2007). According to Trieb and Müller-Steinhagen's (2009) model, capacity will have to be upgraded to 2 gigawatts ( = 2000 megawatts) by 2016 and Lilliestam and Ellenbeck (2011) assume 19 gigawatts by 2050. Other major projects have been proposed between Algeria–Italy and between Tunisia–Italy (Guarniere, 2008; ESTELA, 2009; Economist Intelligence Unit, 2011); these projects, however, are further from implementation.

**EU Worries Concerning the Terrorist Threat to Energy Infrastructure**

The threat of terrorism is often brought up in press coverage of the Desertec project: 'The creation of centralized solar energy plants in Africa also raises its vulnerability for terrorist attacks. If someone attacks the transmission lines, much of Europe could be without electricity' (Rzhevskiy, 2009). Potential investors and project stakeholders have also expressed fears about *force majeure* risks (such as terrorism) associated with building renewable energy projects in North Africa (Komendantova *et al*, 2009). For

example, Lars Josefsson, the CEO of Vattenfall, specifically mentions terrorism risk as one of the problems associated with Desertec (Lubbadeh, 2009).

[page 7]

Underlying these worries is the fear that rather than enhancing European energy security, realization of the Desertec vision will undermine it. Two factors conspire to create these concerns: a history of terrorist attacks against energy infrastructure (see, for example, Fedorowicz, 2007; Jopling, 2008; Giroux, 2009), and the fact that renewable energy plants will be built in coun- tries where Al Qaeda or other Islamic terrorists are known to be active, such as Morocco, Algeria and Tunisia (Atwan, 2006). The argument is that terrorist groups see energy infrastructure as an attractive target because of the impor- tance of energy to developed economies. The leaders of Al Qaeda have long called for economic jihad involving attacks on oil platforms, tankers and refineries (Rudner, 2006; Rudner, 2008a, b). Why would *electricity* infrastruc- ture not be the next logical step?

**Assessing the Terrorist Threat to Desertec**

The proposed Desertec power plants will be located in a region with a history of political instability and local terrorist activity: therefore, an assessment of the terrorist threat is warranted. This section examines various methodologies used for risk assessment, focusing on those applicable to infrastructure and to terrorism. It then assesses the risk posed to the Desertec project under several scenarios.

**Methodology**

This article strives to provide a framework for policymakers and industry executives to evaluate risks and mitigation strategies. Numerous general risk methodologies are obtained, and several could be applied to infrastructure. As delineated by Aven (2008), these include *coarse risk analysis* (or *preliminary risk analysis*), which breaks the subject of analysis into sub-elements and then determines the risk associated with each sub-element, and *SWIFT* (*Structured What-If Technique*) *analysis*, which poses a series of 'what if … ' questions about the security aspects of a project or installation in order to elucidate the threats facing it (and thus, appropriate responses). Other techniques include *exceedance probability curves*, which specify the likelihood of losses surpassing some threshold, and *vulnerability analyses*, which 'characterize the forms of physical, social, political, economic, cultural and psychological harms to which individuals and modern societies are susceptible' (Kunreuther, 2002, p. 661).
Some methodologies have been developed or adapted to specifically assess the risk posed by terrorism (but not necessarily linked to infrastructure). Ezell *et al* (2010) review *probabilistic risk analysis* (PRA) and *event tree analysis*, often used together, as well as some of the controversies that have accompanied their use in terrorism applications (see, for example, Martz and Johnson, 1987;

[page 8]

Gleason, 1988). Aven and Renn (2009) stress the difficulties in establishing reasonable probability estimates for events occurring. Elsewhere, critics have said that the adaptive nature of terrorism limits PRA's usefulness (and can even make it dangerous): if terrorists know a given target is defended, they will attack elsewhere (Brown and Louis Anthony Cox, 2011a, b). Cupp and Spight (2007) focus on US domestic threats and settle on the relatively simplistic formula Threat = Intent + Capability.

Falling slightly outside the realm of risk analysis, but still relevant to the topic at hand, a growing literature explores issues of crisis response management and proactive intelligence-based approaches with respect to terrorist attacks on criti- cal infrastructures (Rudner, 2006, 2008b; Boin and Smith, 2006). For example, Church *et al* (2004) develop spatially oriented models to identify and counter the risk of interdiction (intentional strikes) to critical infrastructures.

Following the terrorist attacks in the United States in September 2001, the newly established US Department of Homeland Security (DHS) sought a method to specifically address terrorist risks to infrastructure in order to guide funding allocations. The DHS initially simply equated risk with population (R = P) to allocate funding to different regional entities. Soon thereafter, the DHS created a second formula that equated risk with the presence of a terrorist threat plus critical infrastructure and population density (R = T + CI + PD). This formula shifted funding in unexpected ways, with controversy erupting in 2004 when Wyoming received around US$28 per resident and New York only $4 (Masse *et al*, 2007). Further refinements led to a new formula in 2006: the level of risk is the result of threat times vulnerability times consequence (R = T×V×C). Within this model, *threat* represents the probability that an attack will occur and is gauged by the presence, intentions, history and capabilities of a terrorist group. *Vulnerability* denotes the security weaknesses associated with the infrastructure in question – including personnel, location and protection strategies – and measures the likelihood that an attack will be successful. The magnitude of the damage – the economic, human life and strategic/symbolic impact of an attack – is reserved for the *consequence* variable (see Department of Justice, 2005; Department of Homeland Security, 2009). Although the DHS has since tweaked with the weightings of the three variables (and whether they should be added or multiplied), the variables themselves have remained constant. Because of this model's specific focus on both terrorism and critical infrastructure, which comprises the nexus of concern addressed by this article, we use it to examine the risk of terrorist threat against renewable energy infra- structure, specifically the Desertec-related installations.

We assert that, having achieved fluency with these three factors, policy- and other decision makers will be in a better position to see 'where potential consequences would be highest and where protective measures and resiliency strategies can be focused' (Department of Homeland Security, 2009, p. 34). In

[page 9]

relating how the DHS' strategy for assessing risk in the United States can be used elsewhere, we seek to provide an impetus for better understanding – in general terms – terrorist risk to energy infrastructure. Using the Desertec project as our case study, we offer a method for specifically assessing and addressing the concerns over terrorist risks to Europe stemming from the import of renewable electricity from North Africa.

In our discussion of the threat, vulnerability and consequence components, we refer to higher and lower risk levels, following the US Department of Justice's (DOJ) 2005 elaboration on the DHS model, as summarized in Table 1 (note: the DOJ adopted the 2006 R = T×V×C formula). We use the DOJ criteria because, as confirmed in a telephone conversation between the corresponding author and a DHS representative on 22 June 2011, for security reasons the DHS does not disseminate its model's fine details. How- ever, the components of the model can be distilled from the primary DHS risk publication (Department of Homeland Security, 2009); the DOJ's (2005) application of the model; and from official reports to the US Congress describing the model (Masse *et al*, 2007; US Government Accountability Office, 2007; US Government Accountability Office, 2008).

Given the myriad possible interpretations of the question 'What is the risk posed by an attack on the infrastructure associated with the Desertec concept?', it is important to remove as much ambiguity as possible from the discussion. As a blackout in Europe seems to be the primary worry of Desertec critics, the risk of blackout – and of system failure – is the focus of and provides the context for our analysis. We also restrict assessment to four scenarios and, as recommended by Masse *et al* (2007), the authors of a US Congressional Research report on the DHS model, we privilege the questions

**Table 1:** Simplified DOJ criteria for risk assessments

| *Risk Level* | *Vulnerability* | *Criticality/impact* | *Threat* |
|---|---|---|---|
| Negligible/Low | Low vulnerability; difficult to access with effective security | Insignificant damage | Non-existent or group has no capabilities |
| Low | (no DOJ description) | Minor disruption | Existent and capable; no history |
| Medium | Moderately vulnerable; easy access with some-what effective security | Moderately disruptive | Existent, capable and with history, but no intentions |
| High | (no DOJ description) | Serious damage | Existent, capable, with history and intentions |
| High/Critical | Highly vulnerable; easy access with minimum/ insufficient security | Irreparable damage with loss of life | Existent, capable and targeting (preparing operations) |

‘risk from what’ (in our case, from a single or coordinated attack) and ‘risk to what’ (to one or multiple targets). We further qualify our analysis, adding the question ‘risk for whom’, or, *risk for which partner, MENA or Europe?*
As our target audience comprises decision makers who influence regulatory and risk management decisions, we strive to *compare* risks across several scenarios so that resources can be appropriately allocated. For example, to avoid the risk of blackout caused by attacks, should funds be spent on eradicating terrorists or rather on improving infrastructure security? In an ideal world, both tasks should be undertaken; however, faced with the reality of scarce funds, decision makers must make difficult choices. To provide a basis for comparison, we evaluate these four scenarios:

- What is the risk that a single attack on an element of Desertec poses for MENA?
- What is the risk that a coordinated attack on several elements of Desertec poses for MENA?
- What is the risk that a single attack on an element of Desertec poses for Europe?
- What is the risk that a coordinated attack on several elements of Desertec poses for Europe?

Even though we are discussing the future, our data and knowledge reflect present conditions. Thus, we consider known terrorist threats and the vulner- abilities associated with existing technologies. Although Europe and North Africa are not yet linked on the scale envisioned by Desertec, we assess the vulnerabilities of such systems based on known technologies (which Dii pur- ports will be the basis for a future interconnected power system). We cannot, however, assess the consequence factor with known data, as realization of the Desertec vision has only just begun. For heuristic reasons, we base our responses on the goal of sourcing 15 per cent of Europe’s electricity from the MENA region (with 3 per cent of Europe’s total supply derived from Morocco-based projects).
Our assessments of higher/lower risks are derived from a variety of sources: the energy and electrical power industry experience of two of the authors; a comprehensive literature review; and from discussions and formal interviews held between March 2010 and May 2011 with solar industry executives, energy industry engineers, a security expert from the International Energy Agency, German Embassy officials in North Africa, and representatives of both the Dii and the Desertec Foundation.
Although we make qualitative remarks about risks, we do not assign specific numbers for the simple reason that we believe quantification – such as assigning, even hypothetically, a weight of ‘3’ versus ‘4’ to the vulnerability of a given electrical system – pulls the focus to numbers, which are hotly

debatable, and away from the search for a useful framework for understanding the pertinent issues, thereby detracting from the value of the exercise. This does not mean that we discourage later quantification – which will be neces- sary to compare risks – but that we think the quantification cart should not be put before the theoretical horse. In the next sections, we use the DHS risk assessment framework to analyze the scale-up of renewable energies in North Africa, examining the vulnerabil- ity of the infrastructure, the likely consequences of single versus multiple coordinated attacks and finally assessing the threat that terrorist groups pose to critical infrastructure.

**Vulnerability: The Weaknesses and Security of Renewable Energy Infrastructure**

The vulnerability of any infrastructure is a combination of its weaknesses and the security measures in place to prevent an attack. With the DHS model, one can assess the risks for individual assets, a class of assets, or 'networks, systems and defined combinations of these' (Department of Homeland Security, 2009, p. 34). As the risk of blackouts is our focus, we consider the vulnerability of an electricity supply system linking Europe and North Africa, rather than attempting to assess the risks of specific individual components. However, we do identify and evaluate the weakest nodes of such a system. The DOJ factors that pertain here are the availability and adequacy of physical security and response forces, and the infrastructure's location – for example, how accessible are the components of the system? How easily breached? In this section, we evaluate two dimensions of infrastructure vulnerability: physical and cyber.

**Physical vulnerability**

Securing power infrastructure is a daunting task because plants and transmis- sion infrastructure are necessarily spread out, making them difficult to defend. In Desertec's case, components will potentially span the entire MENA region, including several international borders. According to our interviews with experts, the weak points of electricity supply systems are easy for terrorists to identify; this, coupled with the dispersion of infrastructure, renders protection more costly. However, a large network also has some inherent resiliency, as terrorists would have to expend huge efforts to produce a large-scale effect. Furthermore, upfront knowledge of obvious vulnerabilities aids policymakers in the allocation of scarce funds.

The plants themselves are conspicuous, and as analysts have observed 'solar arrays installed along the Algeria–Morocco border would be easy targets for terrorists' (Porter, 2009, pp. 9–10). Remotely detonated bombs or rocket launchers could be used against such facilities and, as discussed in the Threat section, terrorists in the region have already demonstrated their capabilities

with explosives. One defense approach already deployed in North Africa is Algeria's militarized protection zones for its hydrocarbon assets, which are patrolled by aerial and ground forces and can only be entered with special permits. One (expensive) way to protect renewable energy infrastructure would be to allocate resources to implement a similar security plan.

In general, transmission hardware is exposed. High-voltage substations, transformers and particularly transmission lines are therefore difficult to protect, especially in remote and underpopulated areas. An advantage of the HVDC transmission lines envisioned to connect North Africa with Europe is that they run undersea. However, the lines connecting generation plants with- in and between countries (such as the HVDC feeder lines) would most proba- bly be built overhead. Some of these would pass through the Sahara, a very remote area in which terrorist groups have a stronghold.

That transmission lines are more assailable than electricity generation infra- structure (regardless of the disruption source) is borne out by the statistics. Simonoff *et al* (2007) note similarities in system disturbances between non- terror incidents in North America and incidents outside of North America in which terrorism was involved: 90 per cent of North American disruptions and two-thirds of international disruptions were specifically due to issues with transmission lines and towers.

**Cyber vulnerability**

Cyber vulnerability presents a serious challenge to infrastructure systems in general (Haimes and Longstaff, 2002). This is true for electrical power facili- ties and systems in particular, especially if the cost of physical attack is perceived by terrorists to be prohibitive. Indeed, as a recent Council on Foreign Relations (Masters, 2011) report indicated, through cyber attacks 'actors with limited financial or technical resources have the capability to compromise high-value targets'. Ebinger and Massey (2011) confirm that cyber threats against power systems are not just theoretical: during the 2008 war between Russia and Georgia, for example, cyber attacks against Georgian electrical systems were successful.

Watts (2003) highlights a number of potential hazards of electrical systems, finding that the more the system relies on information technologies, the more vulnerable it becomes to cyber security risks. Although many components of electric power systems are vulnerable to attack, control centers are among the most attractive targets for terrorists (Nerlich and Umbach, 2009), such as the remote control and monitoring systems often used for transmitting and receiving information, SCADA (Supervisory Control and Data Acquisition) (Kroeger, 2010).

Some SCADA systems monitoring electricity supply systems have already been subject to unauthorized access (Ryu *et al*, 2009). While SCADA systems remain a particularly vulnerable component of existing systems, smart meters

and distributed generation facilities are expected to increase security concerns in the future, as grid capabilities become more widespread and complex. Thus far, no universal measures exist for protecting against cyber attacks (Baker *et al*, 2009). As related by an interviewee for this article, one method of cyber protection could involve isolating as many computer systems as possible. The downside would be the loss of connectivity and efficiency, which carries certain opportunity costs that would have to be weighed against the possible risks and the benefits of mitigation.

**Mitigating factors**

As this analysis indicates, renewable energy infrastructure is potentially vulnerable to physical or cyber attacks. However, how likely would they be to cause a blackout in Europe? It is this possibility that constitutes the worst-case consequence of linking Europe to MENA power supplies. As we discuss in the next section, several mitigating factors obtain, such as the type of transmission lines, the extent of a region's or country's dependence on North African electricity, and the quality of contingency planning. As these factors do not deter attacks, but do affect the impact of an attack, the DHS refers to them as 'consequence mitigation measures' and considers them part of the consequence variable (Department of Homeland Security, 2009, p. 36).

**Consequence: The Impact of a Successful Attack**

According to both the DHS and DOJ, one must consider several categories of consequence, including human health, economic (direct and indirect), psycho- logical, symbolic and governance/mission impact. Within the literature, significant overlap exists between the descriptions of the psychological, symbolic and governance elements. The common denominator seems to be political fallout; for example, might an attack – particularly on a symbolic target – cause citizens to lose confidence in their government or national secu- rity forces? Would the state's ability to govern be impaired? To simplify matters, we have combined these concerns into a factor we call 'symbolic/ political'.

According to the DHS, consequence assessments are difficult as 'there is often a range of outcomes that could occur'. Recognizing the impracticality of making highly detailed consequence assessments, the DHS suggests that 'analysis based on expert judgment may provide sufficient insight to make in- formed risk management decisions in a timely manner' (both from Department of Homeland Security, 2009, p. 35). We adhere to this guideline and to their recommendation to assume 'reasonable worst-case conditions' and not 'to include numerous unlikely conditions' (Department of Homeland Security, 2009, p. 34). For these reasons, we limit our investigation to four scenarios. As attacks on electrical systems typically result in few deaths and therefore have

low human health impact, we leave this factor aside and concentrate on the economic (direct and indirect) and symbolic/political consequences.

**Economic consequences**

Significant capital investments would be at stake in any terrorist attack on renewable energy infrastructure. Direct costs would include losses related to the equipment itself (replacement, repair), whereas indirect and opportunity costs include revenue losses resulting from generation and capacity reductions. The replacement value of an entire plant is usually exorbitant: for example, the total cost of the Ouarzazate CSP plant currently under construction in Morocco is estimated to be around $800 Million (World Bank, 2011).

That both exporters and importers of power would incur significant losses in the case of disruption has been shown by Lilliestam and Ellenbeck (2011). Modeling North African exports to Europe in 2050, they find that a coordi- nated cutoff of electricity to Europe from the North African region as a whole (stemming from either political disagreements or a spectacular terrorist attack) would carry a much higher cost for the EU than for North Africa, but only initially: after just a few hours, the two parties' cost trajectories cross and switch directions. Any single North African country whose power exports were cut would suffer significantly greater losses than the EU importers.

In the early phases of increased renewable energy generation in the MENA region, the host countries would be at more risk for economic consequences simply because the first generated power is dedicated to domestic consump- tion. According to the German Aerospace Center (2006), which conducted many of the preliminary scientific studies of the Desertec concept, until 2020 no electricity would be exported, and from 2020 to 2030 only minimal exports would flow to Europe. Hence, depending on the degree of interconnection and the location of the attack, the domestic effects of terrorist attacks would be more serious than the effects for Europe; host countries therefore have a greater stake in protecting these facilities.

**Consequence mitigation measures**

Once an attack has occurred, how can the consequences be minimized? How can the ripple effect – the extent of the indirect costs – of an attack or an ensuing blackout be contained? There are at least two distinct strategies that could pertain to North African-generated electricity.

First, the European power grid has been disposed to blackouts in the past, but with vastly different regional consequences. The 4 November 2006 black- out in Europe began when an overhead line was intentionally taken out of service by power companies in northern Germany during a planned event. Because of miscalculations, power flows changed within seconds, tripping lines throughout the continent and causing a cascading blackout. This impacted 15 million households from Croatia to Germany to Portugal; even Morocco

[page 15]

through its AC link with Spain. However, Scandinavia remained largely unaffected, because the HVDC cables that link it to mainland Europe were immune to frequency disturbances and acted as a barrier (van der Vleuten and Lagendijk, 2010). The analysis of this event makes clear that electrical regions connected primarily via HVDC lines are generally less susceptible to cascading blackouts than those with AC links. This portends different consequences for North African countries (connected to each other by AC cables) than for the EU (to be connected via HVDC lines).
Second, the vulnerability of the entire system connecting North Africa and Europe is moderated by contingency planning, a standard power industry practice. Most grid operators have in place at least N-1 planning, which, through sophisticated modeling, identifies and compensates for weak spots in the grid. Ideally, transmission planners would have numerous N-1 contingen- cies in place. Cities, regions and countries with greater dependence on North African renewable power could implement N-1-1 planning, which models two components of a bulk power system failing, or even N-2, in which two components are simultaneously removed.
Although the Desertec goal is for Europe to import 15 per cent of its total electricity demand by 2050, a closer look into the possible import shares of the different European countries reveals that some might be more dependent than others. According to the German Aerospace Center (2006), by 2020, the main importers of solar energy would be Italy, Germany, France and Spain; by 2050, the main importers would increase to include the United Kingdom, Turkey and Poland. A disruption in electricity supply would have more serious repercussions for these countries than for those who import far less. The extent of the disruptions could be further contained by each country's transmission configuration and contingency planning.

**Symbolic/political consequences**

The impact of an attack must also be evaluated in political terms at both the domestic and international level (Shull, 2006). On the domestic level, a successful attack would raise questions about the ability of security forces to protect critical infrastructure and cause the public and investors to question the degree of stability in the country. Furthermore, if contingency planning fails, a blackout will occur, the duration of which will vary from place to place and is a function of the robustness of the network, as well as of the planning efforts of the local entities involved. To the extent that such planning efforts are carried out by politically connected bodies, their failure can be represented as political. In this way, a blackout can have an effect on local political trajec- tories. Surveys have shown that a majority of the public in the United Kingdom generally views government as playing some role in the electricity industry. Furthermore, particularly noteworthy system failures can bring unwanted attention to broader developments in the industry. In the United Kingdom,

[page 16]

a series of blackouts in 2003 raised questions about privatization efforts at the time (Brayley *et al*, 2005, pp. 2–4); in the Desertec context, failures could bring negative attention to a wide variety of political and economic trends in the area, ranging from privatization to international integration efforts.
In sum, assessing the consequences of an attack on an electricity supply system poses great challenges; particularly when political and economic damages are nebulous and blend together. At the scale envisioned by Desertec supporters, there is a vast range of potential negative outcomes of an attack, from the temporary shutdown of a single power plant to system-wide cascading blackouts.

**Threat: The Terrorist Presence in North Africa**

The DOJ (2005, 7) recommends that several threat factors be considered: the existence of a terrorist group; its history ('demonstrated terrorist activity in the past'); its capabilities; its intent, and whether the group is targeting, that is, preparing for operations. Whereas existence, history and capabilities are easy to establish – thanks to several databases that track such data – intent and targeting are more nuanced. The intent of a terrorist group is a critical factor that should be considered in resource allocation. To evaluate intent, one must consider 'how closely the results of a type of attack align with "high-level" objectives' of the terrorists (US Government Accountability Office, 2007,
p. 28), which we undertake in this section.
If a group intends to attack energy infrastructure, then the next step would be to ascertain targeting, which is beyond this article's scope and is best left to intelligence professionals (but it is fairly safe to say that, given the low amount of renewable energy infrastructure in MENA, there is not much for terrorists to target at the moment). We single out Morocco in this section because it has become the Dii's prime focus and the site of the first cooperation project. As our discussion illustrates, the insights gleaned from the Moroccan infra- structure case can be applied to other North African countries.

**Terrorist group existence, history and capabilities**

Recent examples of terrorist activities in Morocco include the coordinated Casablanca bombings in May 2003, resulting in the deaths of 33 civilians (with 12 suicide bombers carrying out the attacks), and the bombings in Casa- blanca in 2007 and Marrakesh in 2011 (Human Rights Watch, 2011; Mekhennet and Erlanger, 2011). Al Qaeda has identified Morocco as a target because of the government's involvement in the *War on Terror* (al Arousni, 2011). However, most activity within Morocco (planning or actual attacks) has come from small, decentralized cells, many with clear connections to Al Qaeda (Atwan, 2006). Security forces have been vigilant against militants crossing from Algeria into Morocco; the suspected and real involvement of

Algerians in terrorist acts in Morocco has been a source of past conflict be- tween the two countries and contributed to the closing of their mutual border in 1994 (Botha, 2008).

The groups active in Morocco – as well as in the Maghreb in general – are predominantly Islamist. The START Terrorism tracking center at the Univer- sity of Maryland lists three main groups in Morocco: the Moroccan Islamic Combatant Group (or GICM, using its French acronym), Salafia Jihadia and Takfir wal-Hijra. The GICM supports Al Qaeda and strives for an Islamist state in Morocco; Salafia Jihadia is also loosely connected to Al Qaeda and has targeted international tourists in Morocco (they were behind the 2003 Casablanca bombings); and Takfir wal-Hijra is indeed an international funda- mentalist group, but does not seem to be particularly focused on activities within Morocco (START, 2011).

Although the existence of terrorist groups with histories of operations and proven capabilities might seem to confirm the concerns of Desertec's critics and could cause alarm for the concept's backers, what are the actual intentions and motivations of these groups?

**Strategic intent**

As our vulnerability discussion has indicated, attacks on energy infrastructure are likely to be successful. However, do energy attacks correspond to the goals of the groups in Morocco? As two of these groups are allied with Al Qaeda, we will focus on Al Qaeda's intentions. Because terrorists select their targets depending on how well the expected outcome of an attack corresponds to their *ideology*, the ensuing *intimidation effect* (number of deaths), the target's *symbolism*, the *feasibility* of an attack and whether an attack affects their *external stakeholders* (Toft *et al*, 2010), we will consider these factors.

Using decision analysis tools, Keeney and von Winterfeldt (2010) analyzed Al Qaeda's statements and writings and ascertained that the group has numer- ous strategic and fundamental objectives, ranging from typical organizational maintenance goals such as recruitment to 'maintaining support from the Muslim masses' to military goals of killing 'large numbers of infidels (from pages 1805 and 1811, respectively)' and specifically attacking US targets. Regarding the criteria mentioned above, none of Al Qaeda's primary objectives would be directly fulfilled by attacking renewable energy facilities and power infra- structure. Furthermore, an attack on such infrastructure would conflict with two of Al Qaeda's goals: power infrastructure attacks typically cause few deaths and, if Al Qaeda caused a blackout, it would risk harming its enemies and supporters alike, possibly producing a backlash effect.

But what if new groups emerge with different ideologies and objectives? This prospect is, of course, as likely in North Africa as anywhere else; however, for a terrorist group to be specifically interested in renewable energy infra- structure, these targets would have to be extremely powerful symbols of the

group's grievances. If groups emerged with the objective of ridding North Africa of all Western influence or of stopping greater North–South coopera- tion, then the Desertec concept, *in general*, could have its opponents. Mitigat- ing against this issue, however, is the absence of a 'Desertec' company that will own branded plants and infrastructure. The primary promoters of the Desertec concept, the Desertec Foundation and the Dii, are not project devel- opers. What the Desertec Foundation and the Dii envision is hundreds of plants spread throughout the region, with myriad owners. Moreover, even if a plant or transmission infrastructure was identified as 'Desertec', a terrorist group attacking it would still invite the same risks that Al Qaeda seeks to avoid: harming opponents and supporters alike through a blackout.

Electrical systems have a built-in 'defense mechanism': outages affect everyone. In contrast, careful attacks against oil and gas infrastructure and other assets allow terrorists to target their opponents and spare their supporters. In Nigeria, for example, the Movement for the Emancipation of the Niger Delta (MEND) has a long history of successful, highly disruptive and costly attacks against oil industry targets. The oil industry and oil extraction symbolize exactly what MEND opposes, and thus attacks on them correlate with the group's objectives. Moreover, the consequences of an attack against oil and gas infrastructure and assets are discriminate; attackers can be fairly confident that their operation will harm opponents and leave supporters unscathed. This is not true for the electric power industry.

This difference between various kinds of energy assets raises an important issue: although many scholars have noted increased attacks on energy infra- structure in recent years, they are primarily concerned with oil and gas infrastructure (Fedorowicz, 2007; Jopling, 2008; Giroux, 2009) – perhaps for the very reasons illuminated here. We argue that the insights from our discussion of renewable energy and from the Toft *et al* (2010) study can be applied broadly to terrorist groups and electric power infrastructure around the world: greater electricity interdependence provides an inherent security measure as terrorists cannot discriminate between opponents and supporters.

**Assessing Risk to EU-MENA Renewable Energy Infrastructure**

Diversification of supply is often touted as a method to enhance energy security (Yergin, 2006). However, the Dii's 2009 announcement of its vision of supplying 15 per cent of Europe's electricity from the MENA region combined with the statistic that terrorist attacks in North Africa and the Sahel have increased by more than 550 per cent since September 2001 (Alexander, 2010) elicited concern that the Desertec plan would render Europe's supply less rather than more stable.

Having explored the vulnerabilities, consequences and threats facing renewable energy in North Africa, we now analyze the justification for concerns about dependence on MENA by answering our four questions,

representing four scenarios with different combinations of 'risk to what', 'risk from what' and 'risk for whom'. To assess the risks of the scenarios, we apply the DHS framework to the Desertec case. We use the DOJ criteria to analyze Threat, Vulnerability and Consequence separately and then in our summary derive a composite picture.

*Scenario 1: What is the risk that a single attack on an element of Desertec poses for MENA?*

The DHS/DOJ criteria for assessing threat include the existence, history, capabili- ties and intentions of a terrorist group. Applying these filters to the MENA region, we find that terrorist groups exist and are capable, but have no history, of attack- ing electricity supply systems. For the groups associated with Al Qaeda, such attacks even have potential downsides: they typically cause a low number of casu- alties and carry the risk of harming and alienating supporters. In line with the DOJ (2005) evaluation criteria in Table 1, we find that the threat element is low.

As our analysis reveals, it would be feasible that terrorists might find an in- dividual structure against which they could wage a successful attack; thus, vulnerability for this element is high/critical. Vulnerability of the entire inter- connected power system, however, is low. We assert that a single physical attack – unless it were a 'one-in-a-million' lucky hit – such as the 'overgrown trees' that caused a multi-state blackout in the United States in 2003 would be unlikely to cause a blackout (OECD/International Energy Agency, 2005; Minkel, 2008). Moreover, we assume that the electricity regulators and grid operators have established reasonably robust contingency planning measures that could handle the loss of a single structure.

The direct economic consequences for Morocco, or for any of the MENA countries, would depend on the ownership structure of the assets: if locally owned, then the costs for Morocco would be substantial. Revenue losses might also be high and would depend on the amount of generation lost relative to the country's overall production (and its ability to avoid a blackout). Similarly, the amount of export revenue lost would depend on the country's amount of exported electricity. However, the political risks are different: an attack – even a minor one – would raise questions about government preparedness and earlier anti-terrorism efforts, and it could impact investor confidence in the host nation. We thus rank consequence for Scenario 1 between low and medium.

*Scenario 2: What is the risk that a coordinated attack on several elements of Desertec poses for MENA?*

As the number of attacks increases, so does the likelihood of a blackout. Because a blackout would hurt both opponents and supporters (the 'backlash effect'), we assume that terrorist groups would be less likely to pursue such a coordinated course of action and therefore categorize the threat factor as negligible to low. Indeed, the threat of a coordinated attack may be even lower

than that of a single attack. However, if a group did decide to attack, we believe that the vulnerability of the attacked elements would be high. With numerous plants, lines and other infrastructure to choose from, determined terrorists would most likely find some exploitable vulnerable points and the chance of a blackout would increase. For coordinated attacks, the economic and political consequences could increase significantly, particularly if tradi- tional contingency planning measures failed.
The economic and political consequences for the MENA countries involved would also be quite high. Lilliestam and Ellenbeck (2011) argue that a black- out in Europe would be short-lived and that the MENA host countries would bear the brunt of the economic damage. However, the political fallout would be even worse than in Scenario 1.

*Scenario 3: What is the risk that a single attack on an element of Desertec poses for Europe?*
The difference between this scenario and Scenario 1 is the 'risk for whom' element. The threat and vulnerability remain the same. If no blackout in Europe ensues, then indirect costs would be negligible. Direct economic costs would accrue to the owner of the damaged infrastructure – whether a MENA or European entity. The political costs to Europe of an isolated event would most likely be minimal, but a blackout would cause more dire political fallout. As a blackout is more likely to occur with a coordinated attack, the implica- tions associated with that will be explored in Scenario 4.

*Scenario 4: What is the risk that a coordinated attack on several elements of Desertec poses for Europe?*
A blackout in Europe, caused by a coordinated attack, would be disastrous and the worst-case scenario for all involved, but would still not qualify under the DOJ worst-case criteria, which pertain to cases of 'irreparable damage'. According to Lilliestam and Ellenbeck (2011), a blackout would not entirely debilitate the system. However, the direct and economic costs would be extreme, ranking as 'high' on the DOJ scale. For the European partners, it would raise serious questions about international cooperation and about forming new energy dependencies. Given the cautious way in which the EU goes about its planning and decision-making processes, such an attack could hinder similar deals from being struck elsewhere and other Desertec components or similar projects from being realized.

**Conclusion**

To summarize, across all scenarios, the overall likelihood of an attack is low and, although an electrical system linking MENA and Europe – as well as its component parts – has different degrees of vulnerability, the consequences of

[page 21]

even the worst attack would be manageable and would not fulfill the highest criteria set by DOJ of 'irreparable damage'. The scenario producing the worst outcome, our

investigation indicates, would be for the MENA countries if renewable energy infrastructure was subjected to coordinated attacks. How- ever, what do our analysis of the worst-case scenario and the possible level of damage indicate for policymakers? First, although terrorist groups should always be observed and efforts should be made to stop them and interfere with their plans, the groups themselves contribute less to the overall level of risk than the vulnerabilities of electricity supply infrastructure. Thus, our analysis indicates that reducing the vulnera- bility of the system and its component parts would bring the greatest returns. In other words: improving security and contingency planning may be a better use of scarce resources than undertaking expansive, cross-border anti- terrorism efforts – although this may be attractive to policymakers as it demonstrates to the public that 'something is being done'.

Most major energy facilities have effective security, typically comprised of private sector forces supplemented by host government personnel. The Algerian energy sector has largely been safe from terrorist attack because of heavy investments in security and protection. Pipelines are monitored and key facilities are heavily protected. Foreign energy firms have also introduced rigorous security measures (Giroux, 2009). A similar set of private–public measures should be extended to renewable energy infrastructure in the region. As one of the interviewees stated, the integrated solar combined cycle plant being built in Hassi R'Mel in Algeria is under the protection of the Algerian military in order to preclude a terrorist attack. Another expert interviewee emphasized that, in the oil and gas industry, there has been a push to bench- mark and transfer 'best practices', a behind-the-scenes effort involving the US military, among others. It would behoove the renewable energy industry to learn from and adopt the approach to security of the fossil fuel industry.

Even with top security, it would be impossible to guard all infrastructure, and thus the most vulnerable nodes should be identified. Our expert interviews indicate that the weakest point of the system might be the transformer stations. Using the DOJ criteria, to secure these stations, they should be made extremely difficult to access and should have both sufficient on-site protection and response forces. Concerning the electrical system itself, policymakers and industry participants could encourage enhanced N-1 contingency plan- ning on both sides of the Mediterranean. Systematic and rigorous contingency planning could also safeguard against natural hazards.

In addition to transferring best practices, a number of other initiatives for protecting critical infrastructure have recently been introduced. In 2004, the EU began working toward a common framework for the protection of critical infrastructure through the European Program for Critical Energy Infrastructure Protection. In 2007, the Organization for Security and Co-operation in Europe

[page 22]

(OSCE) adopted a decision on Protecting Critical Energy Infrastructure from Terrorist Attack. The OSCE has also created an Action against Terrorism Unit, one of whose main areas of action is Critical Energy Infrastructure Protection. It prepared a special bulletin in January 2010 entitled 'Protecting Critical Energy Infrastructure from Terrorist Attacks'

that covered a range of pertinent topics such as threat assessment, oil and gas infrastructure protection, electricity infra- structure protection and cyber security. Last but not least, the Dii – as indicated in an early 2011 interview – consults with security experts and incorporates se- curity considerations into its site recommendations.
Our article has these interlinked objectives: to extend the DHS risk assess- ment framework beyond the United States and to advance the debate about what might be the most appropriate methodologies for examining terrorist threats to critical infrastructure. We believe that the DHS framework offers great promise. It is flexible enough to allow decision makers to compare broad categories of risk; it could, for example, be used to assess the risks of importing renewable electricity from MENA versus natural gas from Russia. The frame- work also facilitates resource allocation by revealing – for specific projects – the factors that contribute relatively greater or lesser risk. One of the goals of our case study was to systematically elucidate the terrorist risks to renewable energy infrastructure linking Europe and the MENA region. After applying the DHS framework, we posit that there is solid ground for countering some of the hyperbolic comments that have circulated since the announcement of the Desertec concept; for example, no one 'with a shoulder-launched missile can take out the electricity supply for Europe'.

**Acknowledgements**

The authors wish to thank the reviewers and editors for their feedback and support, as well as Christine Brandstaett and Martin Palovic of the Bremer Energie Institut and Ioana Bedreaga of Jacobs University for their helpful con- tributions. We also express our gratitude to Franz Trieb and his colleagues at the Deutsches Zentrum fuer Luft- und Raumfahrt (German Aerospace Center) for allowing us to use their map of the potential transmission infrastructure connecting European demand centers and concentrated solar power sites in the Middle East North Africa region.