



POWER SHIFTS

DEMOGRAPHICS

CLIMATE CHANGE

GLOBAL FINANCIAL SYSTEM

SCARCITY

Issue Brief No. 08

---

# **Violent Non-state Actors:** Emerging threat to economic infrastructure

---

[www.worldforesightforum.org](http://www.worldforesightforum.org)



# World Foresight Forum

## Introduction

A decade ago, terrorists let the world know that economy matters to them. The choice of the World Trade Center (WTC) as a target of the 9/11 attacks was no co-incidence but a carefully crafted decision by the highest ranking echelons of Al Qaeda (AQ). Boastful of the successfully executed operation, Osama bin Laden declared that while AQ spent only \$500,000 on the event, the US lost at least \$500 billion, “meaning that every dollar of Al Qaeda defeated a million dollars [of America].” AQ is joined by a range of violent non-state actors (VNSAs) who have put economic targets on their “hit list”.

VNSAs are non-state, armed groups engaged in organized violence, which is used as a means to achieve their diverse objectives. These groups not only include terrorist organizations but also rebel groups, warlords, militias, paramilitaries, insurgents, criminal groups, youth gangs and pirates. The motivations behind their attacks vary, ranging from ideological and political to socio-economic and criminal reasons. Nevertheless, the VNSAs are bound together by the significant economic implications of their deeds. By targeting critical infrastructure, private companies and businesses as well as tourist hubs, VNSAs affect stock markets, foreign trade and investments. Moreover, the increased dependence of the world on ICT (see issue brief *Dealing with Cyber Security: accept vulnerability*) has enabled VNSAs to expand their methods of attack by targeting the virtual infrastructures of institutions, including banks and nuclear facilities. The seeds of uncertainty sown by these attacks increase transaction costs and lead to lost revenues and higher world prices. Aware of the impact of their actions, VNSAs call for the intensification of attacks on economically significant targets (see box 1). In the words of AQ’s second-in-command, Ayman Al-Zawahiri, “God willing, we will continue targeting the keys of the American economy.” This Issue Brief examines these instances of non-state violence, and offers a number of suggestions to protect economic targets.

2002

- AQ hardliner Abu Mu’sab al-Suri encourages the targeting of “companies, mines, engineers and agents of foreign companies, representatives of the Aramco company [in Saudi Arabia] that steal Muslim oil”
- AQ targets French oil tanker Limburg, resulting in immediate oil price increase of 1.3%



2004

- Saudi Sheik Abdullah bin Nasir al-Rashid declares targeting of energy infrastructure as legitimate means of economic jihad
- Osama bin Laden calls for attacks on energy infrastructure as part of economic jihad
- AQ online magazine encourages attacks on int’l companies, economic experts, investment operations of Jews and Christians in Muslim countries



2005

- AQ deputy Al Zawahiri reiterates Bin Laden’s message, calling for “attacks on the stolen oil of the Muslims”
- AQ-related website announces the goal to attack oil facilities
- A magazine published by the “Media Committee” of the Afghan mujahedeen declares July 2005 London bombings as a success because of their global economic impact



2006

- AQ operatives attempt to attack the largest oil refinery in the world, the Abqaiq oil facility in Saudi Arabia, accounting for one sixth of total global oil production
- News of the foiled attempt lead to immediate increase in oil prices by \$2



2007

- Sawt al-Jihad (Voice of Jihad) publishes an article entitled “Bin Laden and the Oil Weapon”, in which economic jihad and attacks on physical oil infrastructure are encouraged



2008

- Al-Zawahiri praises the devastating nature of the financial crisis, stating that it is caused by the nature of the capitalist system and the “aggressive Crusader nature”
- Bin Laden expresses his hope that the crisis will prevent the US from financing the war on terror and make the US less powerful

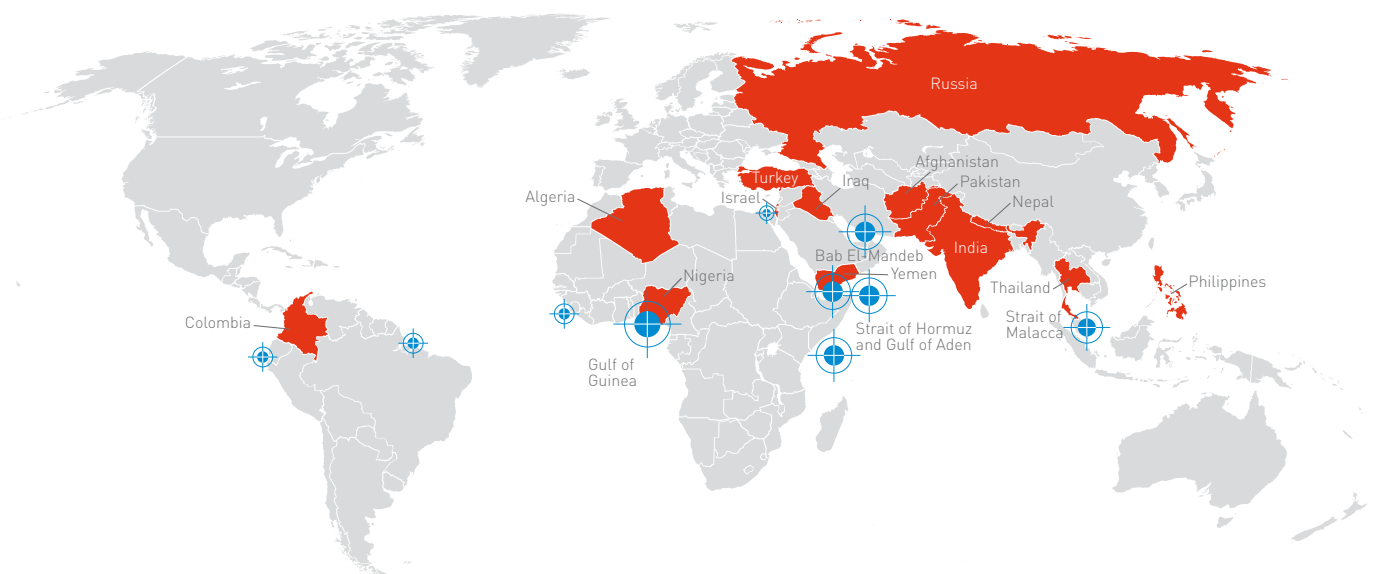


2009

- Members of Al-Fallujah Jihadi Forum are encouraged to increase their activity targeting oil pipelines and refineries in Iraq
- Jihadists also conclude that the financial crisis will result in the disintegration of the USA and Europe/day’s US crude oil imports

## Violent Non-state Actors: Emerging threat to economic infrastructure

### THE HOT SPOTS OF ENERGY INFRASTRUCTURE ATTACKS



Sources: World Incidents Tracking System, International Maritime Bureau

Figure 1: Map of On- and Off-Shore Energy Infrastructure Attacks by VNSAs

Non-state violence against economically significant targets will increase and its impact on the globalized world will be more severe.

#### Attacks on critical infrastructure

The extreme vulnerability of critical infrastructure, including energy infrastructure, electric grids, bridges and dams, has made it an easy target for VNSAs. The attacks on energy infrastructure not only encompass the bombings of pipelines, oil wells or reservoirs, but also the hijacking and looting of fuel tankers, kidnapping of foreign oil workers and stealing of oil for criminal purposes. Moreover, it can be expected that VNSAs will start using cyber attacks to disrupt the functioning of energy facilities as well as trade in electricity and gas. In fact, the EU has recently stated that of all threats to EU energy supply, cyber attacks are probably “the most

feared”. The reasons for anxiety have been underscored by recent cases of espionage when, for instance in 2009, the US electricity grid was reportedly breached by Russian and Chinese cyber spies. Moreover, was Iran’s nuclear centrifuge facility in Bushehr infiltrated by a Stuxnet worm, designed to cause a serious risk of nuclear catastrophe on a par with Chernobyl if the facility came online.

The sustainable campaigns led by VNSAs in countries such as Iraq, Colombia and Nigeria (see figure 1) have resulted in the diminished capacity of these countries to produce oil or gas at their maximum capacity. In Nigeria, for instance, officials reported in September 2008 that daily oil production had been cut by about 1 million bpd, representing 40% of what the country had produced before the Movement for the Emancipation of the Nigerian Delta (MEND) began its campaign in 2006. Such production cuts cost states and private companies



# World Foresight Forum

---

millions in lost revenues, and they result in decreased foreign investment. The oil theft in Iraq, for instance, costs the state approximately \$12 billion a year.

The attacks on energy infrastructure do not, however, only affect local economies. The anticipation of future attacks incurs a risk premium and thus affects stock markets. According to experts from the Zurich-based Center for Security Studies, due to political instability caused by sustained campaigns targeting the energy infrastructure in producer regions such as Nigeria and Iraq in the 2004-2008 period, this risk premium, sometimes also referred to as the "terror premium", increased the prices of oil by \$4 - \$25 a barrel. In addition, the attacks also sustain high transaction costs. This is due to the security measures that states and companies take in response to the attacks, including the hardening of targets such as pipelines or the hiring of security companies to patrol the infrastructure.

Non-state violence targets not only the energy infrastructure but also other critical infrastructure such as transportation, dams, and bridges. For example, on 11 March 2004 terrorists carried out coordinated attacks on Madrid's commuter trains. The devastating attacks left 191 dead and more than 1800 wounded. Less than a year later on 7 July 2005 four suicide bombers attacked London's public transport, in which 56 people were killed and more than 700 injured. The recent arrest of a Saudi student, who planned attacks on hydroelectric dams in the US, indicates that critical infrastructure will remain an attractive target for militants.

## Attacks on businesses

---

Targeting of businesses has been on the agenda of VNSAs for decades. The rationale behind the IRA campaign in Northern Ireland in the 1970s as well as Banda Aceh's campaign in Indonesia was that by targeting businesses, future investment would decline and thus negatively impact on the creation of new job opportunities. Fewer jobs would, in turn, increase popular dissatisfaction

and thus weaken the government. As the Global Terrorism Database notes, attacks on businesses by VNSAs have increased in recent years.

The strategies employed to target businesses have also changed tactics over time, incurring additional costs. For instance, in October 2010, the Yemeni based AQ group attempted to ship a package containing an explosive to the US. Although the attempt was foiled, Al Qaeda in the Arabian Peninsula declared its intention to start using more small-scale attacks on US-bound cargo planes. As a result, the US Congress introduced a bill calling for 100% cargo screening, a measure estimated to cost \$6 billion per year. European businesses have not been spared attacks by VNSAs either. Greece is one country to have noted the sharpest increase in the targeting of businesses by domestic VNSAs such as the Revolutionary Struggle group (see figure 2).

The business targeting strategy also often involves kidnapping of foreign workers aimed at deterring companies from maintaining their operations in the respective countries as well as for high ransoms (see box 2). The funding of groups such as ETA in Spain and the New People's Army in the Philippines is known to come mainly from extortion of businesses. Consequently, these VNSAs actions also result in decreased foreign direct investment (FDI) and a negative effect on economic growth. For instance, it is estimated that terrorist activities in Spain between 1975 and 1991 led to an average annual FDI decrease of 13.5%.

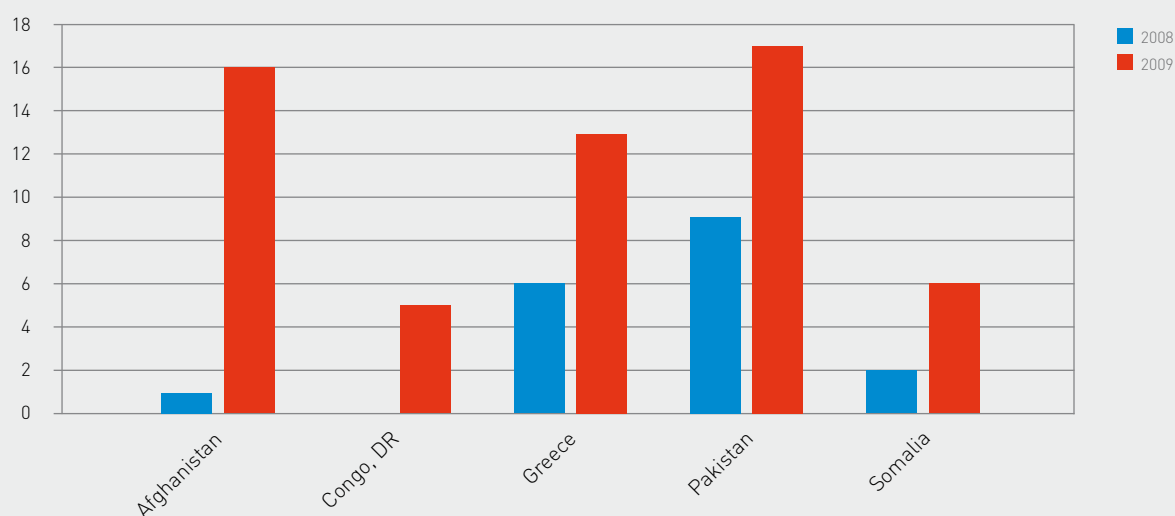
## Attacks on tourism

---

In many countries, tourism is a major source of government revenue as well as employment. Based on the premise that tourists are not going to return if they know that the place is plagued by terrorist activities, VNSAs aim to weaken state economy (see figure 3). The attacks on the tourist industry also have a spill-over effect into neighboring countries. According to some estimates, a typical terrorist attack in Spain scares away

## Violent Non-state Actors: Emerging threat to economic infrastructure

### COUNTRIES WITH BIGGEST INCREASES IN BUSINESS TARGETING



Data Source: Worldwide Incidents Tracking System (WITS)

Figure 2: Countries with the biggest increases in business attacks.

### THE COST OF PIRACY

- Piracy costs the world economy **\$7 billion - \$12 billion a year**.
- The excess costs of **insurance** due to piracy: **between \$460 million and \$3.2 billion**, out of which **\$148 million** is paid in **ransoms**.
- **Re-routing costs** add between **\$2.4 billion** and **\$3 billion** to annual shipping costs.
- **92%** of the attacks and hostage-takings occur off the coast of **Somalia**.
- As piracy spreads further off Somali coast, marketers incur **additional costs** of \$500,000 to \$1 million to hire a tanker of 80,000 metric tonnes.
- 2010: **53 vessels** successfully **hijacked** and a **record 1,181 hostages** taken.
- Some of the recent significant piracy attacks include:
  - **2008** hijacking of Saudi super tanker *Sirius Star* off Somali coast, which led to an immediate \$1/barrel increase in oil prices.
  - **2010** record ransom of \$9 million paid for the release of Greek super tanker *Maran Centaurus* hijacked by Somali pirates.
  - **2010** hijacking of product tanker *Valle di Cordoba* by Nigerian VNSA off the coast of Benin, which resulted in 5,000 tonnes of stolen oil.
  - **2011** hijacking of Greek supertanker *Irene* off Oman carrying \$200 million worth of crude oil, representing 20% of one day's US crude oil imports.

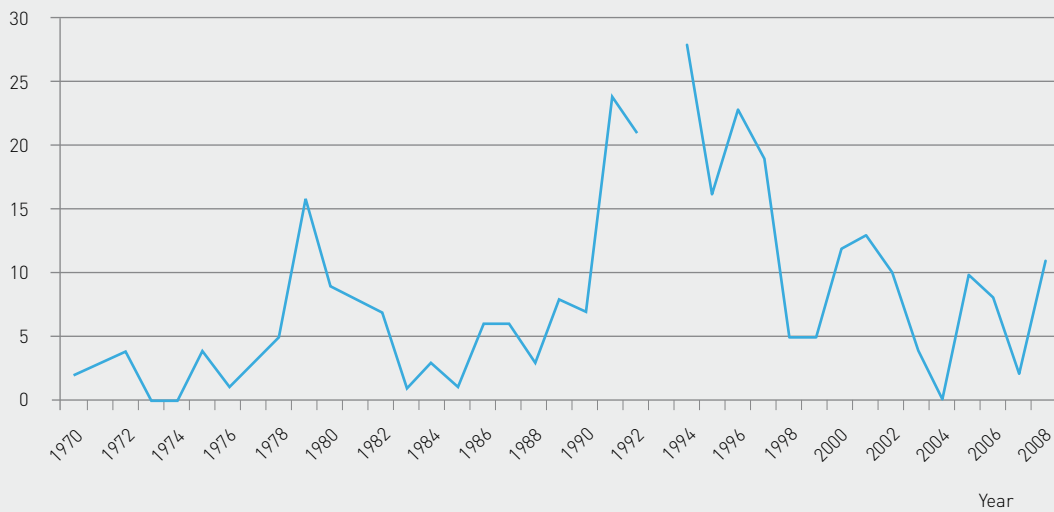
over 140,000 tourists. The well-known terrorist attacks in the Egyptian town of Luxor in 1997 caused tourist revenues to fall by 53% and the 2003 attacks in Bali cost the government \$5 billion in lost tourism revenues, accounting for approximately 2% - 3% of GDP.

In the case of countries where tourism is a developing sector of the economy, VNSAs' activities have an equally adverse effect. In Mauritania, for instance, it is estimated that tourism declined by 50% because of frequent terrorist attacks. Similarly, the growing tourism sector in Niger came to a halt in 2010 due to increased kidnappings conducted on behalf of Al Qaeda in Islamic Maghreb. As a result, some of the northern regions of Niger were operating only at 10% - 15% of their possible capacity.



# World Foresight Forum

ATTACKS ON TOURISM



Data Source: Global Terrorism Database (GTD)

Figure 3: Historical trend of terrorist attacks on tourism

## The New Approach

Current trends indicate that the number of attacks on economically significant targets, notably businesses, airports, tourism and transportation, has been rising since 2007. Moreover, the statements made by VNSAs such as AQ or MEND call for the intensification of attacks on the energy infrastructure, so it is reasonable to expect that the targeting of economically significant objects will remain high and possibly increase in the future. The vulnerability of economic targets makes them easy prey for VNSAs. At the same time, the interdependence of countries around the globe makes them even more susceptible to the economic implications of such attacks. This is especially acute in regard to the energy infrastructure as the West is heavily dependent on oil and gas from volatile regions. With the oil supply tight, even simple attacks on the energy infrastructure could result in supply disruptions and skyrocketing oil prices.

Given the status quo and future projections, governments should invest in measures that will improve their strategic anticipation as well as resilience. Multi-sector security partnerships and resilient public-private thematic networks on the protection of critical infrastructures should be created, also to safeguard virtual networks. Policy makers and private actors should proceed with some urgency to create a commonly shared database that would track all attacks against economically significant targets. External partnerships between different states and private actors should also be used more efficiently. A good model for building external partnerships seems to be the one used by the US and Colombia. This model was built on the premise that it would be bad for both the host country (Colombia) as well as the guest country (US) if major energy infrastructures became disrupted. It was therefore more profitable for the US to invest some of its

## **Violent Non-state Actors:** Emerging threat to economic infrastructure

---

revenue to improve Colombia's infrastructure protection than to leave the entire responsibility for security on the Colombian side.

Finally, the efforts of international organizations such as the Organization for Security and Cooperation in Europe (OSCE), Asia-Pacific Economic Cooperation (APEC), Organization of American States (OAS) and North Atlantic Treaty Organization (NATO) should be enhanced and made more efficient. As most of these organizations already have critical energy infrastructure security on their agendas, it is now the time for them to improve coordination and identify crucial areas where a common approach could add value to the protection of economically significant targets.

11-15 April 2011

The Hague, The Netherlands



This publication is part of a series of WFF Issue Briefs that offer background information on themes to be addressed at the [World Foresight Forum](#). The Issue Briefs aim to inform and stimulate the debate on global challenges. The views and opinions expressed here are those of the authors and do not necessarily express the official views of the WFF or any of its speakers or sponsors.

World Foresight Forum is an initiative of \_\_\_\_\_



Authors: Islam Qasem, Anna Michalkova, Marjolein de Ridder

Copyright: 2011 World Foresight Forum (WFF). All rights reserved. No part of this Issue Brief may be reproduced and/or published in any form by print, photo print, microfilm or any other means without previous written permission from the WFF. All images are subject to the licenses of their respective owners.



**World Foresight Forum (WFF)**

Lange Voorhout 16  
2514 EE The Hague  
The Netherlands

T +31 70 363 6503  
F +31 84 215 3165

[info@worldforesightforum.org](mailto:info@worldforesightforum.org)  
[www.worldforesightforum.org](http://www.worldforesightforum.org)