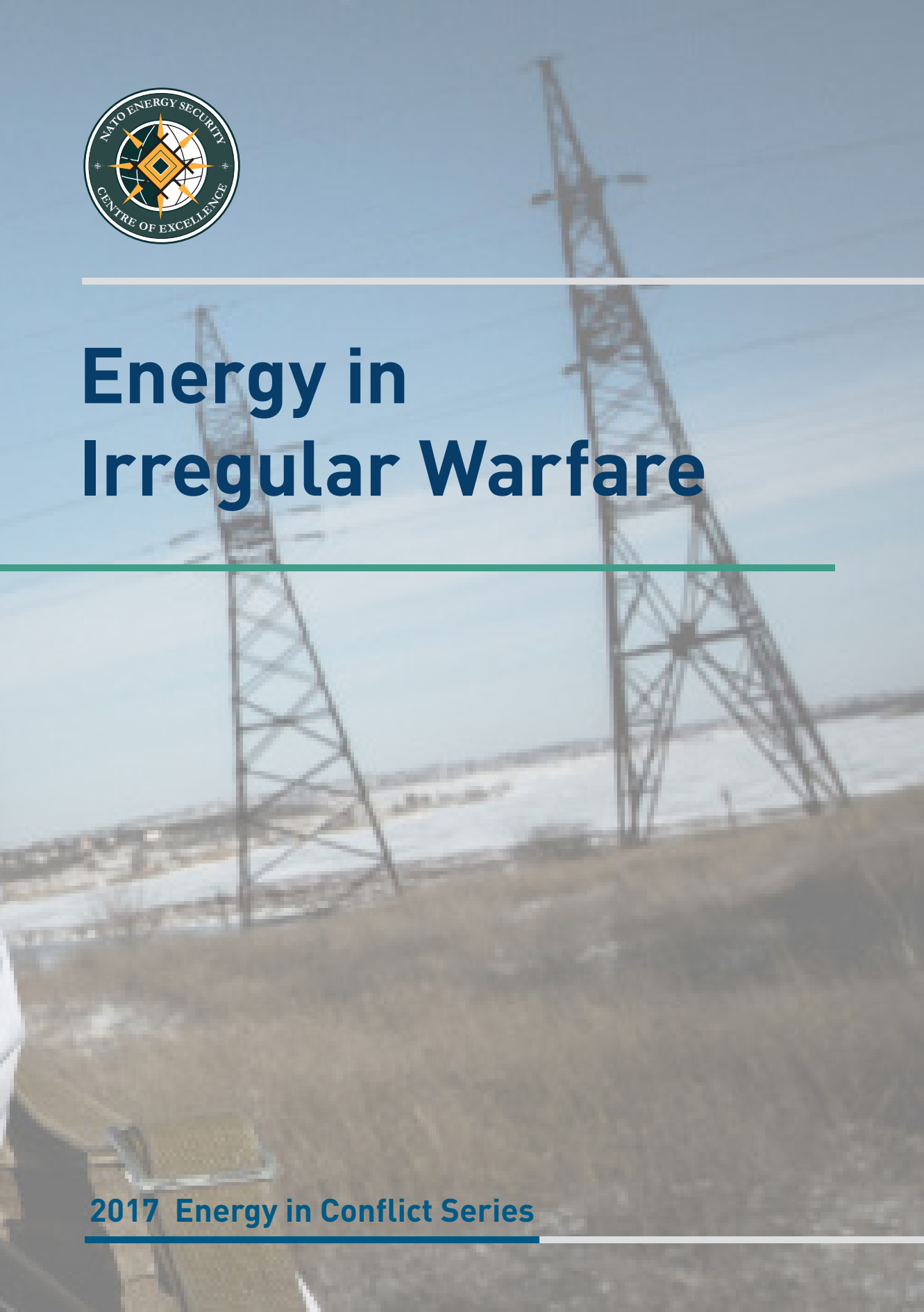


Energy in Irregular Warfare

2017 Energy in Conflict Series

2017 Energy in Conflict Series

Energy in Irregular Warfare

Part II of "Hybrid Warfare against Critical Energy Infrastructures Study"

Heiki Jakson, James Brendan Byrne,
Emanuele Nicola Cecchetti, Jan Ciampor,
Jaroslav Hajek, Maximilian Hausler, Kateryna Dubrova

Cover photograph by Vidmantas Balkūnas

2017

Contents

1 Introduction

The contemporary international security environment is characterized by the prevalence of military and non-military threats such as terrorism, proliferation of weapons of mass destruction, environmental disruptions, energy security threats, and human insecurity. Conflicts between state and non-state actors have become more frequent and a seemingly inevitable phenomena in international affairs, as interstate conflicts have declined and de-escalated in number. While competition among global powers remains a part of the international system, sovereign states tend to concentrate more on the non-military aspects of power and security maximization. Therefore, modern warfare is more associated with a wide use of unconventional tactics, strategies and irregular attacks.

In the modern era, conventional methods of warfare are generally complemented with techniques of insurgency, terrorism, sabotage, subversion and information warfare (U.S. Department of the Army, 2008).

The second part of the "Energy in Conflict" report addresses the issue of unconventional attacks against Critical Energy Infrastructure (CEI). Firstly, it will be analyzed how superpowers during the Cold War period planned to sabotage the CEI of the enemy. Next, the report also provides a brief review of cyber warfare against CEI in recent history. Lastly, it will be shown how CEI relates to asymmetric warfare, insurgency and terrorism.

2 Literature Review

A review of the literature can provide recognized definitions concerning modern warfare. According to modern definitions, Conventional and Unconventional Warfare (UW) are the main principles of the emerging concept of hybrid warfare, whereas UW falls under the definition of Irregular Warfare (IW), as the following examples show:

> *"Conventional warfare is a form of warfare between states that employ direct military confrontation to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory in order to force a change in an adversary's government or policies. The focus of conventional military operations is normally an adversary's armed forces with the objective of influencing the adversary's government. It generally assumes that the indigenous populations within the operational area are non-belligerents and will accept whatever political outcome the belligerent governments impose, arbitrate, or negotiate. A fundamental military objective in conventional military operations is to minimize civilian interference in those operations."*
>
> (U.S. Defence Department: The Irregular Warfare Joint Operating Concept (IW JOC), Version 1.0, dated 11 September 2007)

> *"Irregular warfare (IW) can be defined as a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. IW favours guerrilla[1] and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will. Activities such as, but not limited to, the following examples can be conducted as part of (IW): insurgency, counterinsurgency, unconventional warfare (UW), terrorism, counterterrorism (CT), foreign internal defence (FID), stabilization, civil military operations (CMO) security, transition, and reconstruction operations (SSTRO), strategic communications, psychological operations (PSYOP), information operations."*
>
> (U.S. Department of the Defence, 2007, & DODD 3600)

> *"Unconventional Warfare (UW) consists of activities conducted to enable a resistance movement or insurgency to coerce, disrupt or*

[1] "Guerrilla warfare is a form of irregular warfare in which a small group of combatants such as paramilitary personnel, armed civilians, or irregulars use military tactics including ambushes, sabotage, raids, petty warfare, hit-and-run tactics, and mobility to fight a larger and less-mobile traditional military." (Van Creveld, Martin (2000). "Technology and War II: Postmodern War?". In Charles Townshend. The Oxford History of Modern War. New York, USA: Oxford University Press).

> *overthrow an occupying power or government by operating through or with an underground, auxiliary and guerrilla force in a denied area"*
>
> (U.S. Department of the Army, 2008, 2)

> *"Unconventional Warfare (UW) is a general term used to describe operations conducted for military, political or economic purposes within an area occupied by the enemy and making use of the local inhabitants & resources"*
>
> (NATO NSA, AAP – 6 (2010); pp2-U-1; 1.04.1992)

The emerging concept of IW risks adding further confusion to what is unconventional in warfare. Along with many other operations, UW is now considered a component part of IW.

> *"Given the definition of IW includes combating threats from actions beyond conventional state to state military conflicts, it also includes asymmetric and indirect forces, allowing the definition to encompass a full range of conventional of not-conventional military tactics and other capabilities"*

When IW deals with combating growing threats from actions beyond conventional state-to state military conflicts, it also favors asymmetric and indirect forces, which allow it to employ a full range of conventional of not-conventional military tactics and other capabilities.

The list of activities considered in the IW definition is also useful in characterizing how IW is distinct from conventional warfare and its emphasis on major combat operations (MCO). Of particular note is that UW (including support for insurgencies), CT, FID, PSYOP, and CMO are core elements of IW. Thus IW is a more diverse and broader definition of warfare, whereas UW does not involve all the same activities, and subsequently falls under the definitive umbrella of IW (ARSOF, 2008).

UW usually encompasses irregular forces only; however, it can include use of (national) intelligence information, thus it does not automatically denote lethal force. The properly timed and positioned interdiction of lines of communication, popular uprisings, or sabotage of adversary's infrastructure, for example, can be flexible applications of combat power that place the enemy in a disadvantageous position:

> *"Sabotage is an act or acts with intent to injure, interfere with, or obstruct the national defence of a country by wilfully injuring or destroying, or attempting to injure or destroy, any national defence or war materiel, premises, or utilities, to include human and natural resources"*
>
> (U.S. Department of Defence, 2015, 211)

Some academics include Cyberwarfare as a part of part of UW, claiming that the cyber component can be viewed as one type of sabotage:

> *"Cyberwarfare has been defined as "sabotage actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."*
>
> (Clarke, Richard A. (2010) Cyber War, HarperCollins)

Thus, the theoretical view of "cyber" components varies depending of definition of cyberwarfare and cyberterrorism. Those definitions also are different from cyber-espionage, which falls under both conventional and irregular warfare, depending on the circumstances.

When terrorism is defined as warfare of the fourth generation, it includes failed states, civil war and non-state actors. According to this, it can be suggested that terrorism is part of IW, due to the non-state component. The supposition that terrorism and irregular warfare involve the use of force strictly for political ends has recently been challenged (ARSOF, 2008). As stated in the Introduction, some suggest that politics is no longer the key driver of irregular conflict. In other words, wars of national liberation, ideological terrorism, and revolution have joined colonial small wars "in the museum of past conflicts". Instead, some suggest that contemporary and future irregular threats are driven by a mixture of culture, religious fanaticism, and technology (Kiras, n/d). For example:

> *"Terrorism is an unlawful use of violence or threat of violence often motivated by religious, political, or other ideological beliefs, to install fear and coerce governments or societies in pursuit of goals that are usually political."*
>
> (U.S. Department of Defence, 2008)

> *"Terrorism is an unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives."*
>
> (NATO NSA, AAP – 6 (2010); pp2-T-5; 1.09.1989)

However, other analysis suggest that terrorism can be seen as irregular warfare through the prism of "State terrorism". The State-sponsored terrorism is government support of violent non-state actors engaged in terrorism. Because of the pejorative nature of the word, the identification of particular examples are usually subject to political dispute (Maogoto, Jackson, Nyamuya, 2005)

According to this definition, it is possible to suggest that insurgency & counter-insurgency can be part of State-sponsored terrorism and activities, thus logically both of them fall under IW. Despite the fact that some of their activities might be overlapping, they are still standing for different practices:

> *"Insurgency is an organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict."*
>
> (U.S. Department of Defence, 2007)

> *"Insurgency may be defined as 'comprehensive civilian and military efforts taken to simultaneously defeat and contain insurgency and address its root causes"*
>
> Oxford Dictionary)

The last, but not the least, of this type of warfare is occurring between a standing, professional army and an insurgency or resistance movement. Asymmetric warfare can describe a conflict in which the resources of two belligerents differ in essence, and in their struggle they interact and attempt to exploit each other's characteristic weaknesses; for example:

> *"Asymmetric warfare could be defined as: "a form of warfare in which a non-state actor uses unconventional tools and tactics against a state's vulnerabilities to achieve disproportionate effect, undermining the state's will to achieve its strategic objectives"*
>
> (Ajey Lele, IDSA, 2014)

> *"Asymmetric warfare (or Asymmetric threats) is war/threats emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain disproportionate results"*
>
> (NATO NSA, AAP – 6 (2010); pp2-A-21; 1.10.2003)

Such struggles often involve strategies and tactics of unconventional warfare, the weaker combatants attempting to use a strategy to offset deficiencies in quantity or quality (Roberts, 2004). This is in contrast to symmetric warfare, where two powers have the same range of military powers and resources and rely on tactics that are similar overall, differing only in details and execution, despite the fact that such strategies may not necessarily be militarized (Stepanova, 2008). The

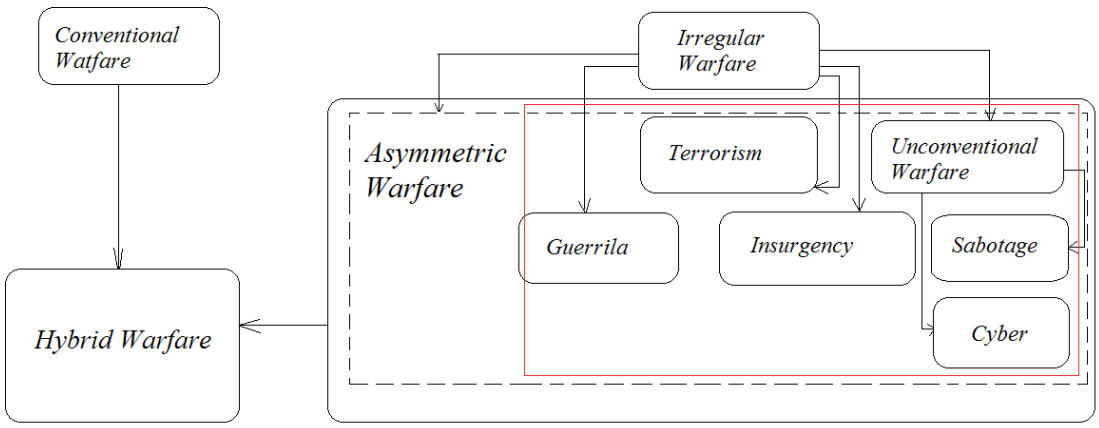


Figure 1 – The figure demonstrates intra-relations between concepts & definitions.

term is also frequently used to complement the warfare described as: "guerrilla warfare", "insurgency", "terrorism", "counterinsurgency", and "counterterrorism", violent conflict between a regular military and an informal, less equipped and supported, undermanned but resilient opponent. According to the academic concepts, asymmetric warfare is perceived as a form of irregular warfare.

However, it is important to note, that not all IW, UW, guerrilla warfare, insurgency, terrorism, counterinsurgency are necessarily asymmetric. A problem with efforts to define an asymmetric threat is that they imply strongly that the range of threats divides particularly into symmetric and asymmetric. It is difficult to qualify or quantify asymmetric threat if one extrapolates the argument "one person's terrorist is another person's freedom fighter" to "one culture's asymmetric threat is another culture's standard modus operandi" (Gray, 1997, p. 5).

The further struggle for a definition comes with attempts to define Hybrid warfare:

> *"Hybrid warfare is conducted by irregular forces that have access to the more sophisticated weapons and systems normally fielded by regular forces. Hybrid warfare may morph and adapt throughout an individual campaign, as circumstances and resources allow. It is anticipated that irregular groups will continue to acquire sophis¬ticated weapons and technologies and that intervention forces will need to confront a variety of threats that have in the past been associated primarily with the regular Armed Forces of states"*
>
> (Hoffman, 2006)

However, this definition is only widely recognized in Anglo-Saxon schools of thought, and varies from different military definitions, and non Anglo-Saxon academic schools. Such description of a hybrid threat as a mix of military capabilities does not facilitate any comprehension of an underlying logic that drives hybrid forces to manifest in a certain way. The complexity and evolvement of the definition creates a struggle to provide a theory of hybrid warfare that enables any predictions of hybrid behavior.

According to NATO hybrid threats "are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives." (NATO ACT, 23 Sept 2011)

Although this section presents some definitions and partly identifies and classifies them, the process of inquiry itself has unearthed additional questions that should be explored in order to fully understand the definitions of modern warfare.

The following sections will explore a number of case studies of asymmetric warfare, such as terrorism, insurgency, sabotage and cyber-attacks, which all fall under the concept of Irregular warfare.

3 Asymmetric Warfare

Traditional warfare is warfare conducted by the legitimate military forces of nation states, where the objectives are either conquering territory or defeating the enemy. Asymmetry in armed conflicts is interpreted as a disproportion of power between the warring parties, primarily in military and economic resources and capabilities (Long, n.d.). Firstly, the power disparities are not marginal but extreme. Secondly, the extreme imbalance in resources available to the parties is compensated for by the imbalance in resources needed to effectively confront the enemy. Thirdly, the higher power resources of the stronger actor by definition lead to asymmetrically damage and casualties of the weaker actor (STEPANOVA, 2008).

Asymmetric warfare is often used to describe insurgency, guerilla and terro-rism, as the concepts are interrelated. As discussed in the previous chapter, Terrorism is commonly defined as an unlawful use of violence aimed at specific target with the intention to create fear to achieve the underlying political motivated goals.

Insurgency is an organized use of subversion and violence to seize, nullify, or challenge political control of a region. It uses subversion, sabotage, and armed conflict to achieve its aims – overthrow an established government, establish an autonomous national territory within borders of a state, cause the withdrawal of an occupying power or the extraction of political concessions, or both, that are unattainable through less violent means (U.S. Department of Defense, 2010).

This section deals with the targeting of Critical Energy Infrastructure (CEI) by both insurgents and terrorists, drawing a comparison between them. It concludes with an analysis of DAESH as the most imminent threat in the Middle East, and de-scribes the military efforts of ISIS and the anti-ISIS campaign in connection with CEI. Data for this analysis was taken from the Global Terrorism Database (START, 2015)[3].

3.1 TERRORISM AGAINST CRITICAL ENERGY INFRASTRUCTURE

Given its strategic importance and evident vulnerability, CEI could be an attractive target for terrorist attacks. Terrorism is one of the tools used by organizations and individuals that wage asymmetrical warfare against a superior foe. Some groups use terrorism as the first step in an armed struggle, for example to raise public support for its cause up to the point of sufficient strength to conduct conventional warfare. It can sometimes also be used as a supplement to conventional warfare, when it is employed to distract the enemy and distract and disrupt the enemy

[3] Attacks against critical energy infrastructure are coded under "Utilities". Where is "utilities"? There are only three occurrences of the word in the report, none of which are "coded" and all occur before this point.

by attacking vulnerable targets at the enemy's rear. This strategy is used by the Afghan Taliban and also by ISIS (Stewart, 2015). In geographical distribution, 72 percent of past CEI attacks were concentrated in three countries, namely Colombia, Iraq and Pakistan, whereas transmission infrastructure was the target of 56 percent of all CEI attacks (Toft et al. 2010). According to Giroux et al. (2013), the vast majority of CEI attacks were successful.

3.1.1 TERRORIST ATTACKS AGAINST CEI IN NATO NATIONS

In December 1984, sabotage operations took place in Belgium, where in the 1980s communist groups were actively supporting the Marxist idea of the revolution. The group called "Cellules Communistes Combattantes" (CCC) was operating on a very high level, conducting several operations between 1982 and 1985. The "CCC" conducted an attack against the Central European Pipeline System in six different places, trying in this way to interrupt and to damage the whole energy system of Central Europe. The attack targeted six valve pits at six different hubs on Belgian territory. It was a significant strike against the Alliance, not because of the actual damage inflicted, but for the vulnerability it revealed.

The results that the CCC hoped for were not realized. Whilst the six valve pits were destroyed and there was a loss of oil products (443 m3) only small fires developed on some parts of the pipeline. The operation of the system was disrupted for several days, having a military impact close to zero (Alexander, 2012, p. 158). However, these attacks taught the Alliance an important lesson that a successful CEI attack against NATO nations was possible. Moreover, the attacks showed also that there was a need to withdraw all the unnecessary valves pits and better protect the others, especially the emergency take-off points. On the other hand, it was clear that the system was well-protected and well-designed, as the attacks resulted in low-level disruption.

Basque Euskadi Ta Askatasuna (ETA), the Basque nationalist-separatist terrorist group active in Spain and fighting for the establishment of an autonomous Basque territory, carried out 2,027 terrorist attacks in the period between 1970 and 2014 (START, 2015). CEI was, however targeted only 73 times, 3.6 percent out of all the ETA attacks during the covered period. Most of the attacks were bombings or explosions and in some cases also assassinations of utility personnel. The attacks did not cause any serious power supply shortages and damages were considered minor.

Since 1970 there have been 86 recorded terrorist attacks against CEI in the U.S., most of which took place during 1970s and 1980s. Since 2000, there have been four terrorist attacks against U.S. CEI in total (START, 2015). On April 16, 2013, the Metcalf transmission substation in California was attacked. Jon Wellinghoff, the former chairman of the Federal Energy Regulatory Commission said it was "the most significant [U.S.] domestic terrorist assault on the grid" (Madrigal, 2014). First, communication cables were cut to disable telephone services. Then the perpetrators started shooting at several transformers from outside of the fenced area. In less than an hour, in addition to customers in Gilroy and Morgan Hill that

were left without phone services for about 24 hours, there was $15 million in damages to the substation and it took utility workers 27 days to repair everything (Memmott, 2014). Nobody claimed responsibility for the attack and no suspects were identified; however, the event itself is widely acknowledged as an act of terrorism (Owen, 2015).

3.1.2 AL-QAEDA TERRORIST ATTACKS AGAINST CEI

Al-Qaeda is responsible for a number of terrorist attacks against CEI, mostly located in the Middle East and North Africa region (MENA) between 1998 and 2013. According to Global Terrorism Database (START, 2015), these attacks include, for example, (1) the 2002 attack on an oil tanker in the Bay of Aden; (2) five attacks on gas pipelines in Algeria; (3) 22 attacks on pipelines and four attacks on oil production and refining facilities in Yemen; (4) three attacks on gas system and power generation capacities in Iraq; and (5) an attempted attack on the world's largest oil producing center Abqaiq in Saudi Arabia in 2006.

Map 1: In Amenas gas fields, Algeria

An important element of terrorism in general, besides the actual use of violence, is making threats to attack CEI. For instance, Al-Qaeda has called for an economic jihad against energy infrastructure in the West in order to weaken Western military capabilities, since oil dependency is perceived by al-Qaeda as the west's

Table 1: Number of attacks against CEI by perpetrator

Perpetrator	Number of attacks (2000-2014)
FARC	170
Baloch Republic army	94
ELN	52
Al-Qaeda	42
PKK	23
ISIS	21
MEND	20

Source: START, 2015a

greatest strategic vulnerability (Braniff, 2011). Energy was mentioned for the first time in 1973 by bin Laden: "We must get this money back from the United States... Muslims are starving to death and the United States is stealing their oil"[4]. Economic warfare against CEI has received even higher priority in al-Qaeda's strategy after the U.S. intervention in Afghanistan and Iraq in the early 2000s (Toft et al. 2010). As a consequence of those invasions, so-called minister of propaganda of al-Qaeda Shaykh Abdullag bin Nasser al-Rashid extended the effort to theorize the Jihad against energy infrastructure. He adopted "Median strategy" to justify the terror against CEI and make "bleed America economically" (Karagiannis, n/d). As a result of such rational, al-Qaeda attacked a number of energy infrastructure facilities mainly in North Africa and the Middle East, however on October 6, 2002, the French oil tanker "Maritime Jewel" was attacked by a suicide bomber in international water. This attack was the first precedent of terrorist groups threatening a NATO nation which was justified as an act of defense of Muslims' common wealth against foreign aggressors (Williams & Urgo, 2008)

Even though existing research (Toft et al. 2010) points to lower importance of CEI in terrorist targeting, al-Qaeda has expressed considerable interest in CEI targets, mostly in the MENA region. Attacks against energy facilities, such as the attempted attack on Abqaiq complex in 2006, could potentially harm the interests of Western countries by disrupting the global oil market and thus increasing global prices. In fact, Saudi oil facilities have been under increasing number of assaults

[4] Osama bin Laden. "Declaration of Jihad Against the American Occupying the Land of the Two Holy Mosques" August 23, 1996.

since 2000 and the Saudi government is spending large amounts of resources on security (Scheuer, Ulph, & Daly, 2006).

In January 2013, one of the largest terrorist attacks in the history of energy industry took place in In Amenas, Algeria. Over four days an Al-Qaeda franchised group attacked the In Amenas natural gas production facility. The assailants took foreign workers as hostages purposefully not harming Algerian employees. 40 workers were killed during the attacks and the facility was shut down. A bullet hit a high voltage transformer causing a blackout in the area and a shutdown of the facility. Later, the assailants detonated a bomb at one of the processing trains that caused extensive explosion damage and a large fire at the facility. The production shutdown caused serious economic losses to the Algerian government, considering that the In Amenas facility alone contributes 20 percent of the country's total natural gas production (Statoil, 2013).

3.1.3 ASSESSMENT OF TERRORIST THREAT AGAINST CEI

This analysis focusses on terrorist activities of al-Qaeda in the MENA region and terrorist activities recorded in NATO member states.

It is important to consider the fact that terrorists in general are trying to provoke an emotional reaction which in general leads to the spread of fear and ultimately to diversion and inefficient use of funds. Therefore it is critical to analyze such threats more thoroughly before determining the appropriate policy.

Secondly, the analysis of terrorist activities of smaller terrorist groups active in NATO member states, such as the ETA, shows relatively low importance of CEI targeting for these terrorist groups, and in the case of CCC relatively low impact of these attacks on energy systems' operation.

Thirdly, it was demonstrated that terrorist threats from Islamist terrorist groups against NATO nations' CEI are relevant in the contemporary security environment but actual attacks on CEI have taken place mostly in the MENA region. However, due to global economic interdependence, the strikes on CEI in the MENA or Middle Eastern region will equally hurt the interest of Western states and companies by destabilizing international oil market and affecting prices. A successful terrorist attack against Saudi oil production facilities would most likely have an immense impact on global prices.

Additionally, according to previous research, even though the energy system appears to be vulnerable it still requires some skill and strategic knowledge of the infrastructure to be able to seriously damage it (Toft et al. 2010). Lilliestam et al. (2011) had analyzed DESERTEC's[5] vulnerability of electricity supply to terrorist attacks and concluded that these attacks are less likely to cause long-lasting outages and severe damage because a large number of simultaneous attacks are required to cause such impacts. According to Lilliestam's findings, it is very difficult for small terrorist groups or individuals to cause long-lasting outages because of their limited capacity and resources. In addition, these groups must carefully con-

sider attacking energy transmission infrastructure as this could also negatively affect neighboring countries' interests, for example an energy exporting state that is depending on that particular transmission infrastructure (Toft et al. 2010). That is why, despite the aggressive rhetoric of terrorist groups, economic targets remain less desirable than military ones. Damaging CEI might not only affect the exporter's neighboring countries, but also can cause significant economic and environmental damage, in particular electricity power cuts, which would make terrorist groups look less popular among targeted audience (Karagiannis, n/d).

3.1.4 DAESH – A CASE STUDY OF CEI AND ITS IMPORTANCE IN ASYMMETRIC WARFARE

Introduction

The so-called "Islamic State" is a militant movement that has declared a Caliphate in the territory of western Iraq and eastern Syria, territories that encompass about six and a half million residents as of 2014 (Laub, 2015). While the group has evolved from al-Qaeda in Iraq and has members with terrorist history, it is much more than a terrorist group. The group has demonstrated its ability to conduct insurgent warfare across large swathes of territory and has also engaged in conventional military battles against Syrian and Iraqi forces. In addition, after a certain period of occupying the territory, ISIS has shown the ability to govern the area, administer social services and even collect taxes (Stewart, 2015).

The role of Critical Energy Infrastructure in ISIS' military efforts

One of the features of ISIS' insurgent warfare is seizing and operating significant oil and gas networks in both Syria and Iraq, which ISIS uses as their main source of funding. Since 2014, ISIS has made strategic efforts to take control of regional oil production capacities. It has launched several military operations in key areas of northern Iraq, seized several oil fields and small refineries and, above all, it has continuously fought over the Baiji refinery, the largest in Iraq. The Baiji refinery still remains one of the most important economic assets in Iraq; before June 2014 it produced about half of Iraq's refined products. With an estimated daily production of as much as 50,000 – 100,000 barrels of oil[6], ISIS makes several millions of dollars in oil revenues every day (Daly, 2014).

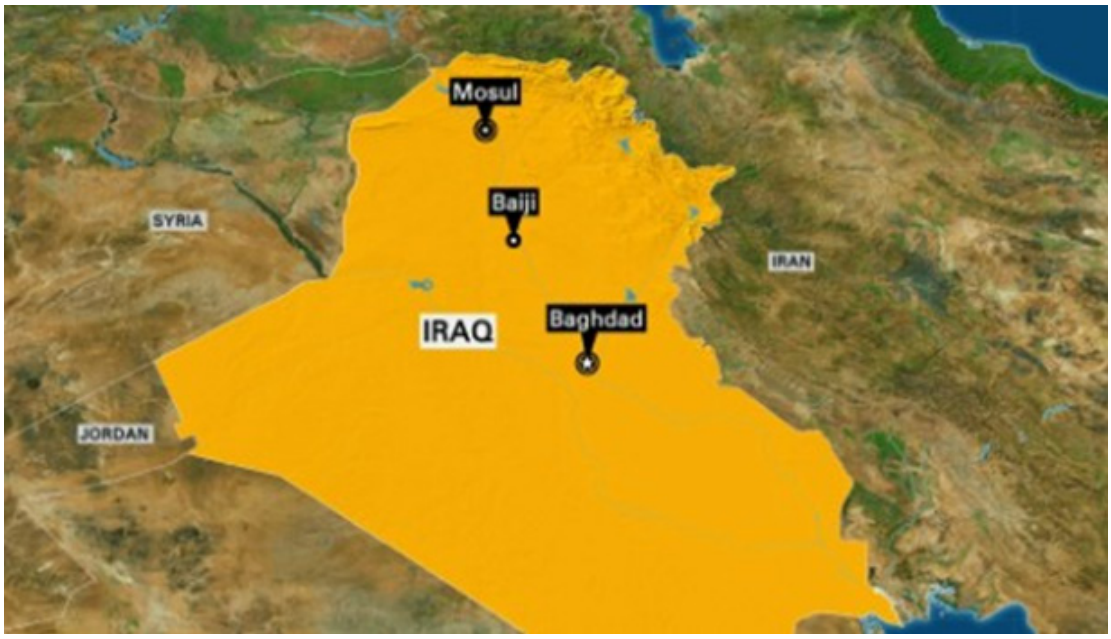
On 23 October 2015, Iraqi Prime Minister Haider al-Abadi, declared that Baiji was free from ISIS forces, and that the anti-ISIS troops had won a "valuable victory. Despite Iraqi victory, clashes between Iraqi Air forces and ISIS are periodically taking place due to its crucial geopolitical importance[7] (Mamoun, 2016)

In addition to using energy resources and energy infrastructure as a key source of income, critical energy infrastructure is also a target of ISIS' military operations. ISIS forces have been vandalizing Kurdish oil infrastructure in northern Iraq in

[5] DESERTEC is a large scale project of renewable energy production in the North Africa and Middle East region (Desertec 2015).

[6] Estimates vary significantly.

[7] Abdelhak Mamoun (4 May 2016). "Iraqi security forces foil ISIS attack north of Baiji, 60 extremists killed". Iraq news, the latest Iraq news by Iraqi News. Retrieved 27 May 2016.



Map 2: Baiji refinery is indicated on Iraq territory, between Baghdad and Mosul

order to deny the Kurd autonomous government a major source of re-venue (Daly, 2014). In March 2015, ISIS militants set oil wells on fire near the city of Tikrit, in order to thwart an attack by Shi'ite militias and government forces (Hameed & Evans, 2015). The aforementioned refinery in Baiji has also been a strategic target of ISIS military efforts. Since June 2014, when ISIS captured the city, there has been continuous fighting over this strategic asset. In May 2015, ISIS militants took control of part of the refinery complex and cut supply lines to a group of government forces. Later in May, ISIS forces set large parts of the refinery on fire, in an effort to thwart advancing government forces (Al Jazeera, 2015).

The Anti-ISIS Air Campaign

Oil revenues were one of ISIS' primary sources of income, allowing them to conduct widespread propaganda offensives, which bolstered recruitment. These funds also enabled ISIS to buy weapons, pay generous salaries to its members and cover their medical costs (Shatz, 2014). Significant sales of oil were made through the black market, which while providing lower revenue relative to international oil prices, still generated large cash-flows for ISIS.

As a result, the U.S-led coalition's policy has been to target the group's oil infrastructure with airpower, thereby reducing its financial resources and ability to conduct operations and wage war. This has been particularly important in the absence of ground forces, which the U.S. and its allies have been reluctant to commit. Meanwhile, much oil-related infrastructure is easily identified and targeted from aerial and satellite photography. Over six months, the bombing campaign destroyed 87 oil collection points and twelve other oil facilities all across Syria and Iraq (U.S. Central Command, 2015) causing a severe financial crisis for ISIS (Frankfurter Allgemeine, 2015).

Summary

ISIS as an insurgent militant group has expressed a profound interest in CEI. Control over oil wells and other CEI has generated substantial revenues and has provided the militants with means to continue with their military efforts against the Iraqi government. In addition, CEI has been considered as an attractive target for the ISIS forces and their leaders in their effort to weaken Bagdad and its military capabilities. CEI controlled by ISIS is also one the primary targets of the Anti-ISIS air campaign, considering its importance in the financing of ISIS' operations.

3.2 INSURGENCY AND CRITICAL ENERGY INFRASTRUCTURE

3.2.1 INTRODUCTION

Insurgent groups, in their efforts to overthrow governments or establish an autonomous national territory, can use a broad spectrum of tactics including blackmail, kidnap, covert political and military operations, coercion, assassinations of government officials, and direct attacks against military personnel and officials. Nance (2015) describes it as the kill, humiliate, punish and inspire strategy. Attacks against CEI also represent an attractive measure to strike the enemy government.

In many countries where insurgencies have occurred, CEI was an important element, target, or an instrument of warfare. The entire infrastructure suppor-ting the oil and refined products industry is quite complex and is vulnerable to damage by insurgencies with belligerent purposes. Refined products that are transported by truck convoys over long distances are specifically relevant in this manner. These trucks carrying explosive fuels represent an easy target for insurgent groups. They can be hijacked as a source of revenues or used as a weapon. Even small amounts of gasoline would be enough to cause significant damage. According to the study of the Army Environmental Policy Institute, one in every eight casualties of the U.S. Army in Afghanistan and Iraq had been connected to transporting fuel (Sullivan, 2014).

Insurgent attacks against energy export infrastructure can also lead to considerable losses for the enemy government, and can substantially weaken its military capabilities. Centralized energy systems controlled by the government might attract insurgent attacks in order to damage the government's credibility in the eyes of its citizens and potential investors and thus undermine its funding and economic stability. CEI is therefore an attractive target to control or to da-mage by insurgent groups.

3.2.2 IRA ATTACKS ON CEI

In 1917, the Irish Republican Army (IRA) emerged as an insurgent group when the Irish Volunteers refused to enlist in the British Army during WWI. Since then, with some modification, they are actively seeking to reunite the Republic of Ireland with Northern Ireland. In order to achieve this purpose they launched many attacks against the U.K. with different targets, some of which were CEI (Craig, 2010).

The first major IRA attempt to attack CEI was called S-Plan. S-Plan was made in 1939 when, within three days, fourteen attacks were made against British power stations, electricity pylons, telephone and telegraph cables (History Ireland, 2011). However, this produced a prompt and devastating response from the Special Branch of the U.K. and did not cause any major blackouts or industrial disruption. The campaign never achieved the intended goal (Craig, 2010).

The IRA's most successful infrastructure campaign was conducted later in 1971 in Northern Ireland. First, sporadic attempts to undermine the Northern Ireland's government were made in late 1969 by attacking electricity pylons. After a break in the summer of 1971, IRA almost managed to cripple Northern Ireland's electricity supply as at least thirteen successful attacks on the main electricity distribution systems, pylons and transformers were made. The IRA even crippled Ballylumford's B-station which was crucial to Belfast's electricity supply. It has been estimated that had several more supply lines been damaged, the entire eastern area of the province would have been without power for between 2 to 14 days" (2010).[8]

In 1996, the IRA organized its last campaign against CEI in London, in this case to humiliate the government. Although it was prevented by Britain's security services just before the attacks were launched, the campaign is worth mentioning due to its high level of readiness. The campaign involved detailed planning with perfect timing that could have "blacked out London completely for two days" (Craig, 2010).

The IRA's attacks on energy infrastructure and their attempts to do it shows that it is a very attractive form of sabotage, especially if one is aiming to compromise and humiliate the government. Even sporadic assaults can do serious harm. However, this case also demonstrates that preparedness to cope with such attacks is a key element in protecting CEL.

Illustration 1: Ballylumford's B-station

[8] Estimated by Tony Craig, professor in Modern history at the University of Staffordshire.

3.2.3 INSURGENCY IN COLOMBIA

Insurgency in South and Central America was a serious security threat from the 1970s till December 2016. Between 1990 and 2014, 28 791 attacks took place and 3089 (10.7%) of those attacks were targeted against CEI. 22 percent of CEI attacks in South and Central America took place in Colombia, and were in majority conducted by two groups – the Revolutionary Armed Forces of Colombia (FARC), and National Liberation Army of Colombia (ELN). These two groups have been the most active in the civil conflict in Colombia which has been raging since 1960s (START, 2015).

FARC and ELN targeted Colombian CEI in order to weaken government capabilities. The key CEI targets have been oil pipelines, mostly the Caño Limon-Coveñas pipeline, the second most important pipeline in the country with daily capacity of 220 000 barrels. Attacks such as these force oil companies to stop production while pipelines are being repaired or to transport oil by more expensive alternate methods such as rail transport. The attacks have been seriously damaging the Colombian economy, considering that oil represents half of its export revenue.

3.2.4 INSURGENCY IN THE NIGER DELTA

Insurgent activities against CEI in the Niger Delta, Nigeria, are mostly linked to the operations of the insurgent group 'Movement for the Emancipation of the Niger Delta' or MEND. MEND's mission is "to expose the exploitation and oppression of the people of the Niger Delta and devastation of the natural environment by foreign corporations and the government of Nigeria" (Tracking Terrorism, 2015).

The escalation of violence across the Delta is a complex and multi-faceted issue, encompassing attacks on oil infrastructure, but also civil violence among oil-producing communities, or against state security forces. The tactics deployed by the insurgents have been diverse, however, focus was on CEI and energy related targets. The preferred methods of MEND are demonstrations, blockades against oil facilities, occupations of oil platforms, pipeline sabotages, oil bunkering (theft), hostage taking and direct strikes (Watts, 2008).

According to Watts (2008, p. 23), between January 2006 and March 2007, more than 200 oil-worker hostages had been taken and 42 attacks on oil infrastructure had taken place. During this one-year period, MEND managed to reduce the oil output of Niger by one-third MEND managed to shut down more than of Nigeria's oil output. A report prepared for the Nigerian National Petroleum Company states that between 1998 and 2003, there were 400 incidents against company facilities each year and oil losses amounted to 1 billion USD annually. Considering that oil accounted for 80 percent of government revenues, a 30 percent drop in oil production caused by insurgent attacks resulted in significant economic / reputational damage to the government. It also dramatically influenced the economic security of the country (World Bank, 2015).

Map 3: Dark Blue line indicates Caño Limon-Coveñas pipeline in Colombia

3.2.5 THE BALOCH INSURGENCY

Baloch people are an ethno-linguistic group living in a territory spread between Iran, Afghanistan and Pakistan called Balochistan. The group has been widely marginalized in these countries as a minority and the region is considered as one of the poorest in the world.

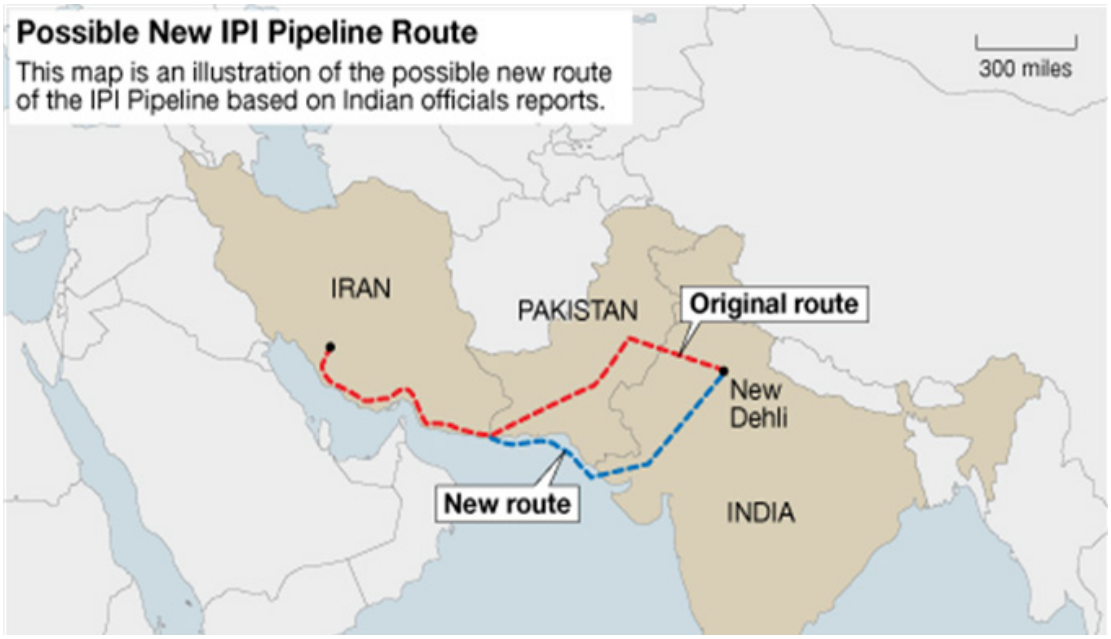
An ongoing cause of conflict is the construction of Gwadar, a Chinese-funded project aimed at developing a massive international port and a transportation hub in the Pakistani part of Balochistan. However, the Balochs have been excluded from the development process and are economically marginalized in the region. As a sign of protest, the insurgents attacked several Chinese workers and oil facilities in the Gwadar area. In 2004, three Chinese workers were killed in an attack. In 2013, the insurgents attacked a fuel truck convoy and destroyed four trucks. In March 2015, Balochi insurgents reportedly set five oil tankers on fire and kidnapped four truck drivers carrying fuel for a Chinese company (Rooney, 2010; Baloch, 2015).

Another source of conflict is expanded natural gas exploration and the proposed Iran-Pakistan-India pipeline (IPI), which is perceived by local Balochs as exploitation of the province by foreign companies (Kupecz, 2012). The insurgents have carried out mostly guerilla attacks on government installations such as rail lines, gas pipelines and transmission towers. Since 2000 there have been at least 515 attacks against CEI in Pakistan, where in 110 cases responsibility was claimed by Balochi insurgent groups, such as The Baloch Republican Army (START, 2015). There have been several blackouts caused by attacks against CEI. In January 2015, according to the Pakistani government, militants blew up a critical transmission line in Balochistan province and caused a wide-spread blackout, described as "Pakistan's worst ever", and which left 80 percent of the country without power (Masood, 2015).

3.2.6 ASSESSMENT THE INSURGENT THREAT AGAINST CEI

Insurgent groups in their military effort against the enemy government employ a broad spectrum of tactics. Their main goal is to discredit the government in the eyes of the public, with an additional aim of cutting a key source of income and support for the respective government. Insurgents also target the operations of foreign companies, whom they perceive as exploiters of local communities and energy, and thus want to expel them from their territories.

According to our findings, CEI, as a potentially vulnerable and critically important element of society, is an attractive target or an instrument in insurgent warfare. Energy infrastructure can be used as a weapon itself, or can be targeted in order to damage the government and its military capabilities or public support.



Map 4: Original and new route of the Iran-Pakistan-India pipeline (IPI)

3.3 UNCONVENTIONAL WARFARE

3.3.1 SABOTAGE

Sabotage should be considered and analyzed as a separate form of modern warfare, due to its unconventional nature of targeting CEI. According to the U.S. Department of Defense, sabotage is defined as:

> *"An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources"*
>
> (U.S. Department of Defense, 2015, 211).

Sabotage tactics have existed since ancient times, one of the first was the Trojan horse. The history of conflicts provides a lot of evidence of unconventional strategies throughout the past centuries where a specific targets could not be reached by conventional warfare, supporting the case studies below.

Sabotage schemes have been evolving up to the point of the most advanced and technological tactics of today, which may damage the target in a concealed way and from distance (from another country or continent) without risk of being identified (mainly applies to cyber-attacks).

During the Cold War sabotage plans were a part of bigger strategy, considering the bipolar nature of international system. The main "saboteurs" were agents of the U.S. and the U.S.S.R.

CEI was targeted with the main objective of destabilizing the economy and disrupting social stability. The first section will analyze the failed sabotage strategies of the Soviet Union and the USA, respectively; while the second part addresses the issues of cyber-attacks and sabotage against CEI in post-Cold war period.

3.3.2 SOVIET SABOTAGE PROGRAMS

All the sabotage projects reported in the following report have been taken from the enormous bibliography of espionage strategies presented by Vasili Mitrokhin. He was a senior archivist in the KGB during 1970s-80s, who collected classified material and then defected after the collapse of the U.S.S.R. He gave up all the documents to the British Secret Service (more than 25,000 pages). Professor Christopher Andrew and MI5 collected all the documents and created the "Mitrokhin Archive", which has proved to be rather trustworthy and useful. The archive describes many plans to target energy infrastructure in the United States, with an aim to create tensions amongst the population and make them to rebel against the government. In this way, as the Soviets thought, the capitalist system would have collapsed and the U.S. government would resign. The plans were mostly directed against the North American region, and targeted specific electricity power grids, city ports or pipelines. However, all the plans presented in the

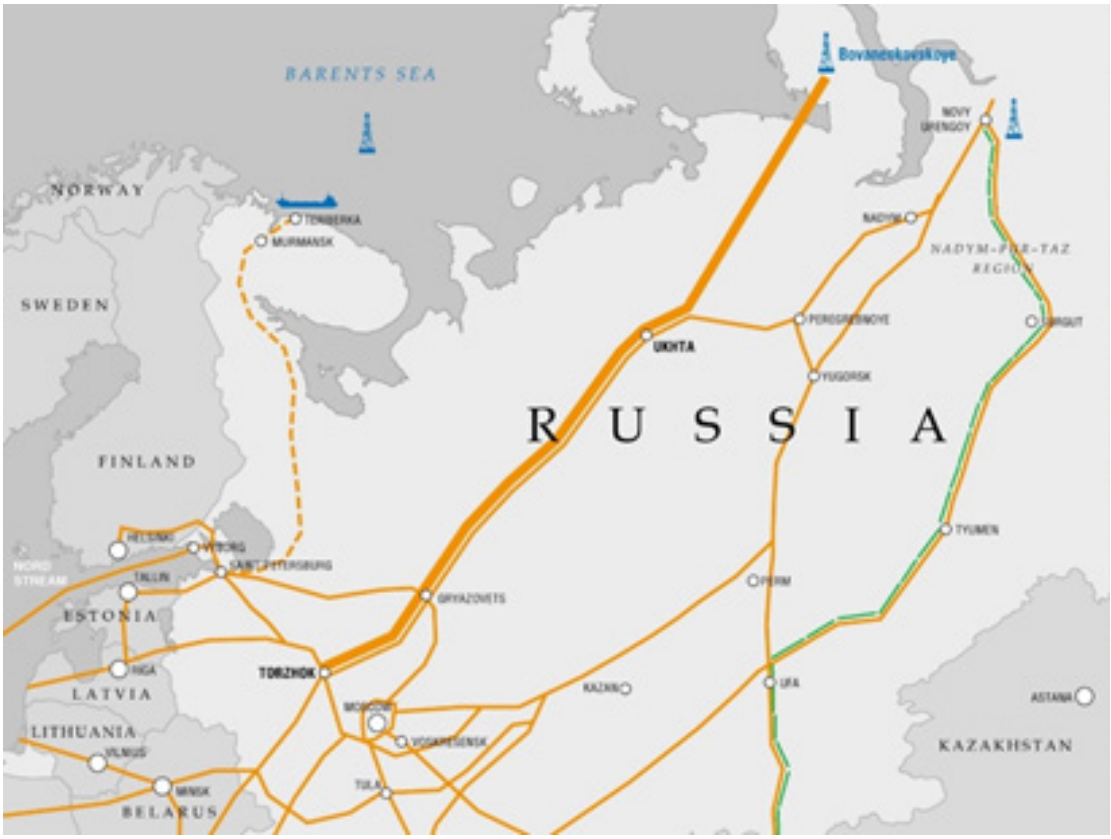
following subchapters were never implemented (Andrew & Mitrokhin, The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB, 1999).

Operation Doris (1967)

During the 1960s the reconnaissance observed the increased number of border crossing in the region of the Lake of the Woods, the International Falls in Minnesota, and the Glacier National Park in Montana. The KGB perceived that Kerr Dam on the Flathead River in Montana was the largest power supply system in the world. The plan was to find a weak spot (codenamed DORIS) on the South Fork River below the dam, where a series of pylons on a steep mountain slope could be brought down, which would take a lengthy period of time to be repaired. The plan also entailed the simultaneous sabotaging of the Hungry Horse Dam on the Flathead River (Andrew & Mitrokhin, 2015).

Target "Granit"

Operation Target Granit was a two-step plan prepared by the U.S.S.R. secret service against the U.S. The first step was to disrupt power lines and pipelines in specific areas of the United States. A blackout in the East and Midwest as well as massive pipeline fires in Texas and California would have been followed by a strike against the New York City skyline, identified by KGB as "Target Granit". A network of piers and warehouses that lined the Port of New York, which includes



Map 5: Eurasian gas system. Green line indicates Urengoy–Surgut–Chelyabinsk gas pipeline.

ships' berths, warehouses, communications systems and port personnel, were the priority targets of the KGB officers (Andrew & Mitrokhin, 2015).

Operation Kedr - "Cedar" (1959-1971)

The operation was prepared at the Soviet embassy in Ottawa in 1959. The preparation took twelve years and contained a detailed intelligence of Canada's oil refineries, oil and gas pipelines from British Columbia to Montreal. The potential targets were photographed and vulnerable points were identified. The goal of this operation was to be prepared to sabotage the oil and gas facilities (Andrew & Mitrokhin, The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB, 1999).

Siberian gas pipeline sabotage (U.S. - 1982)

In this operation, the U.S. used KGB plans to sabotage the Soviet Urengoy–Surgut–Chelyabinsk gas pipeline. It is alleged that the KGB intended to steal Canadian Supervisory Control and Data Acquisition system (SCADA), in order to manage the pipeline. The CIA was informed of the Soviet intentions to steal the control system (described as "Farewell Dossier", (Weiss, 2008)). After careful consideration, the plan was to create faulty software, so the Soviets would steal operating system which would not function properly. The CIA claimed that in June 1982 an explosion in one of the pipelines in Russia was caused by the flawed software - although it was never confirmed. Some analysts said that while there were no casualties from the pipeline explosion, however, the significant damage to the Soviet economy was made (Reed, 2004).

Conclusion

The goal of sabotage is to hamper the national defense of the enemy through covert means. During the Cold War, sabotage was considered an attractive way to strike enemy interests, especially by the U.S.S.R. military. Although the plans were never executed, their existence displays the importance of CEI in strategic thinking.

3.3.3 CYBER ATTACKS

Introduction

Sabotage in modern warfare often takes the form of cyber-attacks, which take advantage of CEI reliance on ICT. Technologies provide a means to attack the enemy from distance, sometimes through third parties, which leaves no proof of the perpetrator. Cyber warfare is considered to be a part of modern warfare and its importance is expected to increase in the future.

Cyber-attacks and sabotage against CEI have taken place in recent history (such as the Stuxnet malware attack against Iranian nuclear facility) which have showed the great potential of cyber warfare in political and military conflict. Cyber operations like this also display the vulnerability of energy infrastructure to external attacks that are often concealed. Therefore, it demonstrates the need for broader security objectives to minimize the risk of attack the protection of vital infrastructure of national energy systems.

> *"Today's developing "information age" technology has intensified the importance of critical infrastructure protection, in which cyber security has become as critical as physical security (...)"*
>
> (Spellman & Bieber, 2010, p. 112).

In recent years, there has been an increase in the number of cyber-attacks, therefore they constitute a growing threat for organizations and governments throughout the world. According to U.S quantitative analysis, every day more than a dozen utilities servers are under cyber-attack, ranging from phishing to malware infections, in order to break through and compromise the system. Some servers are targeted more than 10 000 times per month. (Brodkin, 2013).

CEI such as power generations facilities, water treatment facilities or oil and natural gas pipelines are not exempt from this threat. CEI relies heavily on SCADA control networks and Industrial Control Systems (ICS), collectively called Information and Communications Technology (ICT). These networks were designed to provide management and control reliability, however many such systems did not provide a mechanism to prevent unauthorized access or deal with cyber security threats originating from external networks (Spellman & Bieber, 2010). According to Onyeji, Bazilian and Bronk (2014, p. 58) "the threat on CEI from cyber-attacks is significant and growing as energy system operations become more electronically interconnected". Cyber-attacks on CEI have the potential to impact service of the infrastructure and hence threaten energy security of nations and public safety.

Cyber warfare is considered to be a part of modern warfare and its importance is expected to increase in the future. Several nations are currently working to develop cyber warfare doctrines and capabilities. For example, China has allegedly invested large sums in personnel and information infrastructure for cyber warfare, and since 2002 China has allegedly conducted cyber espionage on the U.S Department of Defense – "operation Titan Rian" (Gervais, 2012). Such rapid development of cyber warfare pushed U.S to adopt more cyber-defensive strategy. The U.S. Department of Defense adopted the "Strategy for Operating in Cyberspace" and ratified as a non-member of the Council of Europe its convention on Cyber-Crime, more commonly known as the Budapest Convention, which creates a framework for cyber defense, warfare, cooperation and crimes, fraud and cyber-terrorism, respectively (European Parliament, 2014). Nowadays, the United States, Iran, China, Israel and other nations around the world have committed to the establishment of military cyber units, which advances their defensive framework. At the same time, the offensive use of those units can be considered a per se armed attack, which falls under the Article 51 of the UN Charter, and allows nations to exercise collective or individual self-defense (Gervais, 2012).

In the Russo-Georgian war of 2008, Russia allegedly conducted cyber-attacks against Georgian targets. K.K. Kakachia (2011) suggested, that the primary Russian intention was reintegration of post-Soviet territories into a Russia-oriented security system (CSTO), where Russia can play a leading role in the Commonwealth of Independent States (CIS) countries' energy complex. Closer Georgian

integration with NATO would threaten Russia's energy hegemony and security as a whole. At this point the regional energy infrastructure became a target in the conflict, which signifies transition from theoretical to practical actions. Prior to the invasion, specifically on 19 July 2008, the security service was informed about a Distributed Denial of Service (DDoS) attack against various Georgian websites (Shakarian, 2011).[9]

According to the analysis of the U.S. Cyber Consequence Unit (2009), during this phase of the conflict, Russia purposely avoided permanently damaging Georgian SCADA targets. A. Kozlowski (2014) argued that hackers were able to target SCADA system, however those attacks were not detected. It is possible to argue that the Russian intentions were to test their skills, abilities and technologies to carry out limited attacks.

Cyber warfare and its relevance in modern conflicts is a complex issue and this chapter serves only as a brief overview of recent cyber-attacks connected to CEI.

Baku-Tbilisi-Ceyhan (BTC) Pipeline

On 5 August 2008 an explosion occurred on the BTC pipeline on Turkish territory. According to U.S. intelligence officials, the perpetrator was Russia. The Kremlin

Map 6: Major pipelines in Caspian region. Light green line indicates Baku-Tbilisi-Ceyhan (BTC) Pipeline

[9] In the first phase, hackers primarily launched distributed denial of service (DDoS) attacks that targeted Georgian government and media websites, rendering them unavailable. In the second phase, the attacks expanded to financial institutions, businesses, western media (CNN and BBC) and other websites. The attacks had a significant informational and psychological impact on Georgia as it isolated the country from the outside world (Shakarian, 2011).

discursively disapproved the construction of the BTC pipeline, due to its circumvention of Russian territory, and consequently a potential loss of influence over energy exports from the Caspian region.

Some days after the explosion, Russian fighter jets dropped bombs on the borderline with Georgia. Simultaneously, Alexander Dugin (an advocate of Russian expansionism and at that time advisor to the Russian Parliament) stated that the BTC pipeline was "dead". However, from recent investigations (Lee, Assante, & Conway, 2014), it appears that the cause of the explosion was not a physical attack but a cyber-attack: hackers had shut down alarms, and cut off communication systems, and super-pressurized the crude oil in the line, provoking an explosion. However, the Turkish government publicly blamed a malfunction and PKK terrorists claimed credit for it. Western media claimed that Russia had a di-rect interest by cutting the West's vital energy connection to the Central Asia and Caspian Sea. Georgia and Caucasian states would have no choice but to obey to Kremlin (Kakachia, 2011)

Stuxnet Operation in Iran (2009-2010)

On 23 November 2010, it was announced that uranium enrichment at Natanz, Iran, had ceased several times because of a series of major technical problems. It was believed to be caused by the Stuxnet malware, designed to attack industrial PLC (programmable logic controllers), which are used to control machinery. A "serious nuclear accident", which shutdown some of its centrifuges, occurred at the site during the first half of 2009. Statistics provided by the Fede-ration of American Scientists shows that the number of enrichment centrifuges operational in Iran rapidly declined from approximately 4,700 to about 3,900 around the time that the incident would have occurred. The attack was designed to enforce a change in the centrifuge's rotor speed. Firstly, raising the speed and then lowering it. This would likely cause excessive vibration and distortions, which would destroy the centrifuge. If the goal was to quickly destroy all the centrifuges in the Fuel Enrichment Plant (FEP) - Stuxnet failed. However, if the goal was to destroy a limited number of centrifuges and set back Iran's progress in operating the FEP – the operation had relative success, as it made detection of the malware difficult (Anderson, 2012).

3.4 IMPLICATIONS OF ASYMMETRIC WARFARE FOR CEI

The concept of asymmetric warfare as warfare between belligerents of relatively extreme differences in military capabilities is usually applied to the phenomena of insurgencies and terrorism (Brown, 2007). Attacks from insurgent and terrorist groups against CEI pose a potential threat. However, insurgent and terrorist groups differ in their perception of relative importance of CEI in their operations. (Brown, 2007)

To terrorist groups, CEI is a relatively low-priority target in comparison to other military strategic targets, however al-Qaeda has shown interest in targeting CEI in the MENA region. Therefore it is essential to analyze terrorist threats against

CEI and determine appropriate policy and protection measures.

Insurgent groups such as MEND in Nigeria or the Baloch Republican Army in Pakistan employ a broad spectrum of tactics and are therefore likely to consider CEI as an attractive target or an instrument of warfare. According to our findings, between 2000 and 2014, FARC operating in Colombia has conducted the highest number of attacks among perpetrator groups. However, Pakistan experienced the highest number of CEI attacks in general, followed by Colombia and Iraq.

Since 1970, the highest number of CEI attacks has been recorded in South and Central America notably during the most violent stages of civil conflicts in South America, especially in Colombia. The number of attacks in South and Central America has fallen rapidly since then. However, the number of attacks against CEI since 2000 has increased in the MENA region and South Asia, mostly because of a steep increase of CEI targeting in Pakistan, Iraq and Yemen.

The importance of CEI in asymmetric warfare is unquestionable regarding the threat posed by ISIS in the Middle East and North Africa. Specifically, attacks on oil infrastructure are an imminent threat to the stable balance of powers, global realm, energy prices, and therefore this threat to CEI should be of major concern to Western countries.

Table 1: Number of attacks against CEI by region

Region	1970-1979	1980-1989	1990-1999	2000-2014	Total
North America	59	18	12	13	**102**
South and Central America	31	1986	843	247	**3107**
Europe	50	95	52	59	**256**
Sub-Saharan Africa	10	103	192	76	**381**
Middle East and North Africa	15	32	43	463	**553**
Asia	12	83	83	729	**907**
Australasia and Oceania	0	3	1	0	**4**
Total	**177**	**2320**	**1226**	**1587**	**5310**

Source: START, 2015a

4 Concluding remarks

This report analyzed an unconventional warfare and attacks against CEI. The focus of the study shows the relationship between CEI and unconventional warfare, such as sabotage, cyber-attacks, insurgency and terrorism. The examples presented demonstrate that CEI has been and continues to be an attractive target in unconventional warfare.

Sabotage is an act of interference with the national defenses of a country, and has been used during various conflicts in the past. During the Cold War, the U.S.S.R. developed plans to sabotage U.S. CEI in order to destabilize the American society (although these plans may seem "rather amateurish"). In modern warfare, sabotage often takes the form of cyber-attacks which are conducted throughout third parties from great distance in a covert way. Attackers can relatively easily gain access to unprotected control networks of infrastructure (SCADA, ICS) and thus can easily disrupt operation of the infrastructure.

Considering the development of cyber warfare doctrines of major powers such as Russia, China, and the U.S., cyber warfare is being regarded as a part of modern warfare and its prominence is expected to further increase in the future. Cyber-attacks against CEI can lead to potential conflicts and therefore are an imminent threat and must be protected against in order to strengthen national defense, energy security, and public safety.

During the NATO Warsaw Summit in July the NATO countries recognized cyberspace as a fifth 'domain of operations', next to the conventional domains of land, sea, air, and space.

Attacks from insurgent and terrorist groups against CEI also pose a potential threat. However, insurgent and terrorist groups differ in their perception of relative importance of CEI in their operations. According to existing databases and recent research, terrorist groups, choose their targets on criteria under which CEI is not as attractive as human targets. CEI is not a primary object of terrorist operations however, al-Qaeda has recently

attacked CEI such as oil production capacities, pipelines and refineries. CEI is not the most desirable target for terrorist groups to attack due to potentially problematic consequences of attacks. It is necessary to analyze terrorist threats not only against domestic infrastructure but also against energy exporting infrastructure in the energy producing regions, mostly notably the MENA region, considering their importance in global energy market stability.

It is crucial to understand that small terrorist groups or individuals do not have sufficient capacity and skills to cause long-lasting energy outages and are seldom motivated to target CEI, therefore their priority is given to terrorizing and spreading fear among populations. On the other hand, highly capable insurgent groups often express interest in CEI and we argue that CEI in asymmetric conflicts has been an important target and an instrument of warfare. We mainly refer to the military activities of ISIS in the Middle East as well as to the anti-ISIS campaign led by the U.S. and its allies. We believe that these circumstances create an urgency for policy makers to include CEI protection measures in counter-insurgency strategies.

The U.S. and its allies must acknowledge evident vulnerabilities in energy systems that could negatively affect their fighting capabilities. For example, sabotage and cyberattacks on energy infrastructures can potentially lead to loss of energy supplies for military forces and thus loss of combat power. In addition, disabling generation facilities such as power plants could cripple any modern, energy-dependent society and thus create further challenges for security. Therefore, cyber-defense and counter-sabotage measures should be focused on neutralizing the threats in regards to CEI.

In counter-insurgency operations specific measures must be taken in the area of CEI protection. Considering that insurgents tend to attack fuel supply lines of enemy forces such as truck convoys, storage depots and distribution centers, substantial effort must be put into protecting this infrastructure in order to avoid loss of lives, supplies, combat power and financial resources. Moreover, in regard to insurgents using energy resources as a significant source of revenues, military efforts should be directed to eliminate financial schemes and thus hamper their military capabilities.

5 References

Agayev, V., Akhundov, F., & Aliyev, F. T. (1995). World War II and Azerbaijan. Azerbaijan International, 50-55.

Al Jazeera. (2015, March 25). ISIL fighters set Iraq's Beiji oil refinery ablaze. Al Jazeera, pp. http://www.aljazeera.com/news/2015/05/isil-fighters-set-iraq-baiji-oil-refinery-ablaze-150525122055089.html.

Al-Azzawi, S. N. (2013). Crimes against Humanity: The Destruction of Iraq's Electricity Infrastructure. The Social, Economic and Environmental Impacts. Global Research.

Alexander, P. (2012). Europe's red terrorists: The fighting communist organizations. London: Routledge.

Anderson, N. (2012). Confirmed: US and Israel created Stuxnet, lost control of it. Ars Technica.

Andrew, C., & Mitrokhin, V. (1999). The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB. New York: Basic Books.

Andrew, C., & Mitrokhin, V. (2015). The Mitrokhin Archive– The KGB in Europe and the West. Penguin: London.

Baloch, K. (2015, March 27). Chinese Operations in Balochistan Again Targeted by Militants. The Diplomat.

Barnhart, M. A. (1988). Japan Prepares for Total War– The Search for Economic Security, 1919–1941. London: Cornell University Press.

Becker, P. W. (1981). The Role of Synthetic Fuel in World War II Germany. Air University Review.

Boyne, W. J. (1997). Linebacker II. AirForce Magazine.

BP. (2015). BP Statistical Review. https://www.bp.com/content/dam/bp/pdf/energy-economics/statistical-review-2015/bp-statistical-review-of-world-energy-2015-full-report.pdf.

Braniff, B. a. (2011). Towards global Jihadism: Al-Qaeda's strategic, ideological and structural adaptations since 9/11'. Perspectives on Terrorism.

Brodkin, J. (2013, May 22). Power company targeted by 10,000 cyberattacks per

month. Retrieved from Ars Technica: http://arstechnica.com/information-technology/2013/05/power-company-targeted-by-10000-cyber-attacks-per-month/

Brown, B. P. (2007). Irregular Warfare (IW) Joint Operating Concept (JOC). Department of defence United States of America.

Carter, J. (1980). The American Presidency project. Retrieved from http://www.presidency.ucsb.edu/ws/?pid=33079

Cordesman, A. H., & Wagner, A. (1990). The Iran-Iraq War – Chapter 7: Phase Four: Stalemate And War Of Attrition On The Land . In The Lessons of Modern War - Volume II . Westview Press .

Craig, T. (2010). Sabotage! The Origins, Development and Impact of the IRA's Infrastructural Bombing Campaigns 1939-1997 . Intelligence and National Security, Volume 25.

Cressy, D. (2011). Saltpetre, State Security and Vexation in Early Modern England. Past and Present, 212.

Curzon, L. (2015, November 25). Oil and War Mix: Having the former has meant winning the latter. Retrieved from http://www.defenddemocracy.org/media-hit/oil-and-war-mix-having-the-former-has-meant-winning-the-latter/

Dahl, E. J. (2000). Naval Innovation: From Coal to Oil. JFQ.

Dalmacijaa, B., Ivancev-Tumbasb, I., Zejakb, J., & Djurendic, M. (2003). Case Study of Petroleum Contaminated Area of Novi Sad After NATO Bombing in Yugoslavia. Soil and Sediment Contamination: An International Journal 12.

Daly, J. C. (2014). The Islamic State's Oil Network. Terrorism Monitor 12 , http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=42942&no_cache=1%20-%20.VaTZSk0cSUk#.VlcHIj_ouUk.

Dews, E. (1980). Pol Storage as a target for Air Attack: Evidence from the World War II Allied Air Campaigns against Enemy Oil Installations. Santa Monica: Rand Note.

Dixon, H. (2013, May 16). Hour by hour: how the Dambusters raid unfolded. The Telegraph.

Eichholtz, D. (2012). War for Oil: The Nazi Quest for an Oil Empire. Potomac Books.

Engdahl, F. W. (2004). A Century of War. Retrieved from http://www.engdahl.oilgeopolitics.net/History/Oil_and_the_Origins_of_World_W/oil_and_the_origins_of_world_w.HTM

Engdahl, F. W. (2007). Oil and the Origins of the Great War. History Compass 5/6, 2041-2060.

European Parliament. (2014). Cyber defence in the EU: Preparing for cyber warfare? Brussels: European Parliament.

Foryth, R., & Laurier, J. (2015). Luftwaffe Mistel Composite Bomber Units. Oxford: Osprey Publishing.

Frankfurter Allgemeine. (2015, February 2). Extremisten handeln mit Leichen kurdischer Gefallener. Frankfurter Allgemeine, pp. http://www.faz.net/aktuell/politik/ausland/naher-osten/islamischer-staat-extremisten-handeln-mit-leichen-kurdischer-gefallener-13441928.html.

Futrell, R. F., & Moseley, L. S. (2012). The United States Air Force In Korea, 1950-1953. Literary Licensing.

Gendron, A. (2010). Critical Energy Infrastructure: Protection in Canada. Defence R&D Canada Centre for Operational Research & Analysis.

Gibson, M. W. (2012). British strategy and oil, 1914-1923. Glasgow: University of Glasgow.

Giroux, J., Burgherr, P., & Melkunaite, L. (2013). Research Note on the Energy Infrastructure Attack Database (EIAD). PERSPECTIVES ON TERRORISM 7.

Hameed, S., & Evans, D. (2015, March 5). Islamic State torches oil field near Tikrit as militia advance. Reuters, pp. http://www.reuters.com/article/2015/03/05/us-mideast-crisis-iraq-idUSKBN0M10Z420150305#LmlJdEm8v3O5lZcQ.97.

Hart, L. (1991). Strategy. New York: Penguin.

History. (2015, November 25). Operation Rolling Thunder. Retrieved from History: http://www.history.com/topics/vietnam-war/operation-rolling-thunder

Hobbs, D. (2011). The British Pacific Fleet: The Royal Navy's Most Powerful. Barnsley: Seaforth Publishing.

Husain, T. (1995). Kuwaiti Oil Fires: Regional Environmental Perspectives. Elsevier Science Ltd.

Ike, N. (1967). Japan's Decision for War: Records of the 1941 Policy Conferences. Stanford: Stanford University Press.

Keegan. (1946). Effects of Strategic Bombing. USSBS.

Khadduri, M. a. (1997). The war in the Gulf: The Iraq-Kuwait conflict and its implications. Oxford University Press.

Kupecz, M. (2012). PAKISTAN'S BALOCH INSURGENCY: History, Conflict Drivers, and Regional Implications. International Affairs Journal 20.

Laub, Z. (2015, November 16). The Islamic State. CFR, pp. http://www.cfr.org/iraq/islamic-state/p14811.

Lee, R. M., Assante, M. J., & Conway, T. (2014). Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack. ICS Defense Use Case.

Lilliestam, J., & Ellenbeck, S. (2011). Energy security and renewable electricity trade--Will Desertec make Europe vulnerable to the "energy weapon"? Energy Policy, 3380-3391.

Long, D. E. (n.d.). Countering Asymmetrical Warfare in the 21st Century: A Grand Strategic Vision. Strategic Insights.

Lovins, A., & Lovins, L. H. (1982). Briitle Power: Energy Strategy for National Security. Brickhouse Publishing.

Madrigal, A. C. (2014, February 5). Snipers Coordinated an Attack on the Power Grid, but Why? The Atlantic.

Masood, S. (2015, January 25). Rebels Tied to Blackout Across Most of Pakistan. NY Times.

McCarthy, J. R., & Rayfield, R. E. (1985). Linebacker II: A view from the Rock. Office of Air Force History .

Memmott, M. (2014, February 6). Sniper Attack On Calif. Power Station Raises Terrorism Fears. NPR.

NATO, ACT. NATO Countering the Hybrid Threat: http://www.act.nato.int/nato-countering-the-hybrid-threat

Nance, M. W. (2015). The Terrorists of Iraq– Inside the Strategy and Tactics of the Iraq Insurgency 2003-2014. Boca Raton: Taylor & Francis Group.

Naval History and Heritage Command. (2015, November 25). V: "THUNDER AND LIGHTNING"- THE WAR WITH IRAQ. Retrieved from Naval History and Heritage Command: http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/u/us-navy-in-desert-shield-desert-storm/the-war-with-iraq.html

Nixon, R. (1973, November 7). Th Presidents's address to the nation outlining steps to deal with the emergency.

Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber Security and Critical Energy Infrastructure. The Electricity Journal 27, 52-60.

O'Rourke, R. (1988). The Tanker War. Proceedings Magazine 114.

Osborn, P. R. (2000). Operation Pike: Britain versus the Soviet Union, 1939-1941. Westport, CT: Greenwood Press.

Owen, B. (2015, November 26). Shock the system? Electrical grid, comms attacked near San Jose. Retrieved from http://www.bob-owens.com/2013/04/shock-the-system-electrical-grid-comms-attacked-near-san-jose/

Powers, A. J. (1951, April 3). The carrier-borne aircraft attacks on oil refineries in the Palembang (Sumatra) area in January 1945. Supplement to the London Gazette, pp. 1803-1813.

Rainey, S. (2011, October 10). Dambusters raid: background. The Telegraph.

Reed, T. C. (2004). At the Abyss: An Insider's History of the Cold War . New York: Presido Press Trade.

Rooney, J. J. (2010). The Baloch Insurgency and 21st Century Asian Energy Security. The Prague Journal of Central European Affairs, 81.

Rouleau, E. (1995). America's Unyielding Policy Toward Iraq. Foreign Affairs .

Scheuer, M., Ulph, S., & Daly, J. C. (2006). Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy. Washington: The Jamestown Foundation.

Shakarian, P. (2011). The 2008 Russian Cyber Campaign against Georgia . Military Review.

Shatz, H. J. (2014, September 8). How ISIS funds its reign of terror . Daily News, pp. http://www.nydailynews.com/opinion/isis-funds-reign-terror-article-1.1931954.

Spellman, F. R., & Bieber, R. M. (2010). Energy Infrastructure Protection and Homeland Security . Lanham, Maryland: Government Institutes.

START. (2015, November). Terrorism. Retrieved from START: http://www.start.umd.edu/gtd/search/Results.aspx?search=terrorism&sa.x=0&sa.y=0

Statoil. (2013). The In Amenas Attack: Report of the investigation into the terrorist attack on In Amenas. . Oslo: Statoil.

STEPANOVA, E. (2008). TERRORISM IN ASYMMETRICAL CONFLICT IDEOLOGICAL AND STRUCTURAL ASPECTS. Solna: Oxford University Press.

Stewart, S. (2015, November 26). The Difference Between Terrorism and Insurgency. Stratfor.

Sullivan, P. (2014). The Energy-Insurgency Revolution Nexus: An Introduction to Issues and Policy Options. Journal of International Affairs, 116-146.

Takeyh, R. (2010). The Iran-Iraq War: A Reassessment. The Middle East Journal 64, 365-383.

The Dambusters raid: How effective was it? (2013, May 15). BBC.

Tracking Terrorism. (2015, November 26). Movement for the Emancipation of the Niger Delta (MEND). Retrieved from Tracking Terrorism: http://www.trackingterrorism.org/group/movement-emancipation-niger-delta-mend

Trudgian, N. (2015, December 11). Operation Tidal Wave - The Ploesti Mission .

Retrieved from Air Art NW: http://www.airartnw.com/tidalwave.htm

Tucker, S. C. (2001). Encyclopedia of the Vietnam War: A Political, Social, and Military History. Oxford University Press.

U.S. Central Command. (2015, February 3). Feb. 3: Military Airstrikes Continue Against ISIL in Syria and Iraq. Retrieved from U.S. Central Command: http://www.centcom.mil/en/news/articles/feb.-3-military-airstrikes-continue-against-isil-in-syria-and-iraq

U.S. Cyber Consequences Unit. (2009). U.S. Cyber Consequence Unit U.S. Cyber Consequence Unit U.S. Cyber Consequence Unit. U.S. Cyber Consequences Unit.

U.S. Department of Defense. (2010). Department of Defense Dictionary of Military and Associated Terms. U.S. Department of Defense.

U.S. Department of Homeland. (2015, November 24). What Is Critical Infrastructure? Retrieved from Department of Homeland: http://www.dhs.gov/what-critical-infrastructure

USSBS, O. a. (1946). Oil in Japan's War (. Pacific War No. 51.

Watts, M. J. (2008). Curse of the Black Gold: 50 Years of Oil in the Niger Delta. New York: Powerhouse Books.

Weiss, G. W. (2008). The Farewell Dossier: Duping the Soviets. CIA Library.

Wolborsky, S. L. (1994). Choke hold: The attack on Japanese Oil in World War II. Alabama: School of Advanced Airpower Studies .

Yergin, D. (1991). The Prize: The Epic Quest for Oil, Money, and Power. FreePress.

Yergin, D. (2011). The Quest: Energy, Security, and the Remaking of the Modern World. Penguin Press.

NATO Energy Security Centre of Excellence

Šilo g. 5A, LT-10322 Vilnius, Lithuania
Phone: +370 706 71000
Fax: +370 706 71010
Email: info@enseccoe.org
www.enseccoe.org.