Threats to the Critical Information Infrastructure Protection-CIIP posed by Modern Terrorism

Author
Metodi Hadji-Janev

Affiliation/Country
International relations and International security law, Republic of Macedonia

Abstract

The emergence of new non-state actors in the post Cold War reality have dramatically changed security environment around the globe. Modern terrorism practiced by Al Qaeda and its associated movement (AQAM) has posed serious threat to critical information infrastructure given the trend of connecting control systems that run these infrastructures to the internet. Although AQAM have not been successful to launch cyber-attack that will cause mass casualties, environment damage or financial effects, the possibility remain alarming since creativity in the age of globalization never ends. Additionally by using the so called "dot-com culture" modern terrorists effectively employ negative effects of globalization to rich to the societies' remote pockets and Islamic social nomads and thus enlarge their capabilities to affect our critical information infrastructure. Therefore to effectively protect our CII from modern terrorists we need to consider comprehensive and holistic approach build on direct and indirect mechanisms.

Introduction

The end of the Cold War and technological development has stimulated the process of globalization. On one hand globalization has spurred economy and improved our way of living. On the other it has stimulated environment where non-state actors including terrorist organizations have gained unimagined power. Using violent ideology especially after military response to 9/11 attacks, Al Qaeda have build global network of associated movements. Launching an ideological war these activists successfully have attracted many religious Islamic groups and individuals that were impressed with the idea to oppose.

Today Al Qaeda's and its associated movements' (AQAM) activities represent modern terrorism. They pose asymmetric, unconventional, and apocalyptic threats around the globe. In this context cyber-world has become both, battle-space for modern terrorists' ideological and information warfare and medium for global radicalization.

AQAM's interest to engage cyber-world for its own purposes raises serious alarm. Recent trend to connect control systems that run critical infrastructure to the internet makes these utilities especially vulnerable in the context of AQAM's interest. Thus many modern systems that run our everyday life and we depend on are also infrastructures that could be used to affect our security. Yet until today AQAM have not been successful to launch large scale cyber-attack that will cause mass casualties, environment damage or financial effects. Nevertheless security analyses and recent practice confirm that AQAM can affect critical information infrastructure both directly and indirectly.

On one hand there are many open possibilities for AQAM to attack critical Information Infrastructure. Their leadership's dedication to exploit internet, apocalyptic agenda and unconventional approach perfectly matches the possibility of threatening our CII. On the other, by using the so called "dot-com culture" modern terrorists effectively employ negative effects of globalization to rich to the societies' remote pockets and Islamic social nomads. Although many of the AQAM's supporters are second or even third generation Muslims (educated in West and raised surrounded by western values and culture), who have never met some of its leaders they have been radicalizes among other through internet. The practice (like in London attacks case for example) has shown that these self-radicalized individuals are equally or even more dangerous to detect and fight than the core AQAM cadre.

Therefore to effectively protect our critical information infrastructure and improve its resilience we need to consider comprehensive and holistic approach. This approach should include but is not limited to direct protective mechanisms like protective systems, supporting tools and technologies (with proper and timely updates), adequate and secure use of systems, general awareness of existing threats and appropriate security reporting. In addition indirect approaches that will reduce AQAM's ability to influence support must be also considered if we are to improve our critical information infrastructure protection and its resilience.

1. Process of globalization and the security environment after the Cold War

Influence of globalization and the emergence of new non-state actors in the post Cold War reality have dramatically changed security environment around the globe. This "*Big Thing*"-globalization as described by Friedman (2002) has become a driving force in international affairs (p xxi). Labeling it as a *tectonic shift*, Friedman describes globalization as an international system with its own rules and logic that influences the geopolitics and economics (p xxii). Despite the fact that globalization is largely associated with open markets and free trade many argue that globalization is technology driven.

Fukuyama (1992) claims that thanks to technology liberal democracies had grown sufficiently aware and interconnected to protect against cataclysmic warfare among superpowers, marking an end to the Cold War. Therefore he believes that the "*expansion of globalization occurs most rapidly in lands that nurture the freedom of expression and enterprise*" (p. 23-25). In this context Mead (2004), explains how "the glorious triumph of technology and entrepreneurial spirit over a decadent and stagnant era", offer "new and more dynamic opportunities to eliminate poverty and transform the human condition" (p. 71). Expansion of globalization supported by the development of technology supposed to reduce world poverty and contribute to a stable economic growth and peace (Stiglitz, 2003).

Another remarkable effect of globalization toward peace and stability is its influence on the evolution of social relationships from local to global. The development of technology has not just prompted the communications among corporate, groups and individuals but has also lowered the costs of communications. As a result globalization has shortened the distance among nations. Today many of the global systems and services that they provide are ran by private non-state actors. These systems and services are interlinked interconnected and go beyond national borders. They enable free flow of capital, goods, people and money. Their establishment in fact has destroyed hierarchical corporations that were once wedged among geographical, political and cultural boundaries. The new collaborations established through business connections, have not just mitigated hostility between groups and nations, but have also facilitated the spread of liberal-democratic values freedom, the rule of law, and human rights. Democratization usually associated with globalization thus has become an emergent trend that supposed to contribute to the world peace stability and global wealth. However, the 9/11 terrorist acts on the United States and subsequent "War on Terror" dramatically reveal that globalization could be a double edge sword.

Global flows of technology, goods, information, ideologies, and people can have destructive as well as productive effects. The disclosure of powerful anti-Western terrorist networks shows that globalization divides the world as it unifies, that it produces enemies as it incorporates participants (Kellner, 2004). The free flow of capital, goods, money and people did not filter the proliferation of the worst aspects of cultures everywhere. Greed, depravity, indulgence, instant gratification, and the capacity of nations to wage war and individuals to engage in terrorism are also result of the influence of globalization (Giddens, 1990, pp. 151–54). In fact not everybody see attempts for democratization and economic growth the same way, and does not use technology for what it has been designed.

Although democratization in an age of globalization was overwhelmingly accepted in the post communist world, many Muslim communities and individuals see these attempts as attack to the essential values that serve only to the West. They see democratization as dangerous disruptions that have spread throughout the world in the name of globalization. Western governments' policies to promote democracy through the essence of globalization (open markets and free trade), by some Muslim believers are interpreted as hypocrisy. According to these views Western policies urge poor countries to eliminate trade barriers while retaining their own systems of subsidies and trade protections. Some argues that globalization, has riled middle-class Muslim people from Meddle East to oppose the process of, as they saw, "westernization of the Muslim land" and came up with its own agenda (Kepel, 2005, p. 112).

Muslim believers that oppose democratization consider it as intrusions that disrupt the social order, exploit children and women, and threaten traditional cultures and moral behaviors (Frost, 2009, p. 83). These views more or less come from reluctance to accept liberal interpretation of pluralism (Roggio, 2009). Since this is a profusion of diversity it means that accepting democratization means accepting choice. Having a choice for these Muslim believers means departing from determinism (the essence of Islam) and thus challenging the social order (Berger, 2003 p. 5-12). Liberal choices such as homosexuality, or women being able to occupy prominent positions of authority, according to the opposing Muslim forces of democracy, are at odds with traditional values (Mead, 2004, p.73-75). Therefore as Huntington (1996) argues it would be naive to believe that just because the young men from the Middle East who wear jeans, drink a Coke and listen to rap will all accept democratic approach in conflict resolution with those who are at odds (p.58). As they argue due to the frustration caused by corrupted regimes, fear spread by these regimes and vengeance to these regimes and their supporters, liberal virtues – tolerance, compromise and reasons are unacceptable. Instead they choose to violently oppose to fight in the name of the religion with those who fight against them (Sohail H. H. & Miller, D. p.197)

Just to be clear many Islamic governments insists that there is no fundamental dichotomy between democracy and Islam. Bangladesh, Kuwait, Jordan, Turkey, Pakistan, Malaysia, Egypt, Indonesia, Tunisia, Algeria, and Nigeria identified themselves as democracies. The problem however is that Salafists have declared democracy an apostasy that must be ruthlessly exterminated (Sageman, 2004). Recent events in the so called "Arab Spring" has significantly undermined Al Qaeda's violent attempt (as a leader in this Muslim insurgent movement) to oppose the Authoritarian regimes. However, there are four things that one should bear in mind on this subject. First, the euphoria of Arab Spring has calmly frozen as spring turn in to summer and then autumn and winter came in (McKay, 2011, p.4-20). Second, wealthy Gulf states Saudi Arabia, the United Arab Emirates (UAE) and Qatar are still opposing the demands for change and they have even intervened in Bahrain and suffocated the demonstration for change. Third, we are not sure how the regional revolution will play in the context of stability and new environment. Fourth, Arab Spring has only addressed part of the Al Qaeda and its associated movements' demands i.e. removal of as they see the puppet regimes. Their global and apocalyptic demands are still in place (we will refer to this latter).

The evolution of the social relationship from local to global on a horizontal level is another residual effects of globalization that have influenced global security environment. The destructions of vertical usually government controlled boundaries and as a rasault, proliferation of the global corporate and enterprises have its own price. The same forces of globalization that have facilitated the growth of economies and encouraged cultural exchange throughout have also become available to violent Islamist groups led by Al Qaeda that practice global terrorism.

2. Al Qaeda and its Associated Movements: A Serious threat to Critical Information Infrastructure Protection-(CIIP)

The 11 September 2001 terrorist attacks in the United States, and its subsequent events have dramatically affected the Al Qaeda's ability to adapt and to evolve. Military response by the US led coalition to these attacks has not resulted in decisive victory, but had served to Al Qaeda's interest. Using violent ideology Al Qaeda have build global network of associated movements. Al Qaeda and its associated movements (AQAM) have soon took the advantage and begun to employ global systems and services that they provide. This has not just expanded their activities and influence but has also improved lethality and sophistication of their attacks. Availability of modern technology, especially information technology and communications have enabled terrorist groups' capacities to effectively oppose overwhelming military power in a unique way. Technology has, in short, made terrorism and its central strategy of asymmetric warfare more symmetric (Forst, 2009, p.167). Thus AQAM's terrorism became serious threat to critical information infrastructure-(CII), the very infrastructure that our society depends on. This however raises the questions on how and why modern terrorism practiced by AQAM became so powerful and hard to fight?

2.1. The evolution of Al Qaeda and its ability to adopt

Although threats posed by Al Qaeda existed before 9/11, according to some views, “failure of imagination” that these threats are real, had prevented serious action against them. Furthermore previous issues and confrontations that have caused the paradigm of “one’s man terrorist the other mans’ freedom fighter” inhibited coordinated and appropriate reaction on a global scale. It was after 9/11 event that the US, the EU and the UN have considered international terrorism as global threat. The White House, 2002; European Union, 2003; United Nation, 2004). However, the John Mearsheimer’s argument about that nostalgia for “Cold War terrorism’s predictability” has soon become evident (Merasheimer, 1990).

The US led coalition’s approach to confront Al Qaeda and its supporters in Afghanistan and at that time, suspected Saddam’s regime, was direct and conventional. It predominantly relayed on military as an instrument of national power. Without really understanding the threat during the Global War on Terror the US led coalition almost immediately had lost the initiative. The US and coalition warriors approach was by the book. The problem nonetheless was that the very approach was wrong.

During Operation Anaconda in Afghanistan, the US and Canadian troops have physically destroyed Al Qaeda (Van Evera, 2006, p.47-59). Following the US offensive strategy against Al Qaeda and its supporters, next stop, i.e. to deny Al Qaeda’s access to weapons of mass destruction, was Iraq. The approach was wrong because it failed to address “the war of ideas” and “to protect US and coalition homeland”. As a result the wrong approach which was military driven had created far more dangerous Al Qaeda in the middle of the military success. In fact, unintentionally they had created the *idea* of Al Qaeda.

The 2004 article in the Al Qaeda military journal *Al-Battar* argued that the destruction of the Afghan sanctuary has enabled a global expansion for Al Qaeda:

> *…In the beginning of their war against Islam, [the Crusaders] had announced that one of their main goals was to destroy the Al-Qaeda organization in Afghanistan; and now, look what happened? Thanks to God, instead of being limited to Afghanistan, Al-Qaeda broke out into the entire Islamic world and was able to establish an international expansion, in several countries, sending its brigades into every Islamic country, destroying the Blasphemers’ fortresses, and purifying the Muslims’ countries…*(Al-Battar, 2004).

Additionally, a Gallup survey on a question “…Should US attack the country(s) that has (have) served as a base for terrorist attacks”, conveyed in 14 countries from September 14 to 17, 2001 revealed that, though half of the respondents in almost all countries cheered for “extradition” and “trial”, only Israel and India supported “the military attack” (Ford, 2001). Another Survey run by Pew Center, had revealed that “many Muslims, even in countries with reasonably good relations with US such as, Nigeria, Indonesia and Pakistan (at least at that time) had feared that US may attacked them” (Pew, 2003). Wrong approach has also reflected in favor of Al Qaeda’s ability to gain popular support due to the tactical mistakes by the warriors on the ground. These tactical mistakes had strategic impact.

Early mistakes in the Global War on Terror (GWOT) have given unimagined advantage of Al Qaeda’s leaders. They were able to profit from these advantages and build upon the dichotomy of globalization’s effects on Muslims in the Middle East and perception of the Western policies as hypocrisy. The result was that the magnitude of radical Islam has begun to serve as a solution to the modern issues for many Muslim groups and individuals. In short Al Qaeda become fashion among radical and some non-radical but desperate Muslim youngsters around the globe that were unable to cope with the modernity. Thus the new phenomenon Al Qaeda and its associated movements have flooded the world.

2.2. Al Qaeda and its Associated Movements' Center of Gravity

AQAM have proven to be capable to take the initiative by shifting the fight on coalition soil. Attacks in Bali (2002), Madrid (2004), London (2005), Mumbai (2009) and Moscow (2010) attest that these non-state actors' agenda has become global, apocalyptic and critical infrastructure focused. Relying on a strategy of mass casualties AQAM's center of gravity is to indirectly (through public opinion) persuade US and Coalition authorities and keep them clear from Middle-East conflicts (Mark, and others, 2008, p.144). The only way to succeed in this is by attacking the weakest points of perceived enemies. Analyses of AQAM's modus operandi show that so far AQAM have identified two weak points among its perceived adversaries.

The first one is Western values (pursuit for democracy, stability, peace, and prosperity *per se*) and their application of the way of life in order to achieve greater quality. The second weak point identified by AQAM is modern civilian systems that support (i.e. sophisticated networks of services and infrastructure that move people, goods, energy, money, and information at higher volume and greater velocities) the Western values. These two points in fact match what we have previously considered as global counterterrorist coalitions' mistakes i.e. to address the potential war of ideas and to protect homeland.

In sum AQAM' leaders have realized the influence of Western public opinion on decision making. Therefore they have chosen it for its own center of gravity. In order to influence Western public opinion among other means AQAM have heavily employed critical information infrastructure-CII. These infrastructures are physical and information-based facilities, networks and assets, which if damaged or occupied (abused) by AQAM would have a serious impact on the well-being of citizens, proper functioning of governments and industries or other adverse effects.

2.3. Al Qaeda and Its Associated Movements actions against Critical Information Infrastructure: Is the threat real?

Much has been written about cyber-terrorism and terrorists' capability to affect cyber security. Although this mere trend has existed well before 9/11 cyber-terrorism has emerged as a great security concern after the attacks. Attacks in Bali in 2002 confirmed the speculations about AQAM desired targets i.e. critical infrastructure. A 2003 private study found that during the latter half of 2002, the highest rates for global cyber-attack activities were directed against critical infrastructure industry companies (Symantec, 2003 p. 48). Another report on industrial cyber-security problems using data from as far back as 1981, reportedly has found a 10-fold increase in the number of successful cyber-attacks on infrastructure Supervisory Control and Data Acquisition-SCADA systems since 2000 (ISA Expo, October 5, 2004). Until today we haven't witnessed successful large scale terrorist cyber-attack that has caused casualties. This elevates the question whether threats from AQAM to CIIP are real?

There is disagreement among the experts about the real danger that AQAM could cause to CIIP (Wallace, June 30, 2002). Part of the disagreement comes from the different approach in defining threat or cyber terrorism. This is to some extend understandable since there is no single definition about terrorism *per se*. Some experts focus on the intent (Denning, 2001, p. 241), while others focus on the effect that cyber-attack could cause (Verton, August 11, 2003). Some experts who focus on intent argue that AQAM are not threat to CIIP since they need the system. Nevertheless if they pose threat from cyber-world this threat comes from their ability of abusing internet and expanding the so called e-jihad.

Additional point for disagreement is the effects that AQAM could cause to CII. This is also understandable since not all countries around the world are equally developed and thus technology dependence differs. More developed countries are more vulnerable to cyber threats since they are more IT dependable. Furthermore there are different opinions among the experts from the same country (Lemos, 2002). Some observers have stated that because of U.S. dependency on computer technology, such attacks may have the potential to create economic damage on a large scale, while other observers have stated that U.S. infrastructure systems are resilient and would possibly recover easily, thus avoiding any severe or catastrophic effects (Wilson, 2005).

The contradicting results also come from the practice. In July 2002, the U.S. Naval War College hosted a war game called “Digital Pearl Harbor” to develop a scenario for a coordinated cyber-terrorism event. The simulated cyber-attacks determined that the most vulnerable infrastructure computer systems were the Internet itself. The exercise proved that attempts to cripple the U.S. telecommunications infrastructure would be unsuccessful because system redundancy would prevent damage from becoming too widespread. The conclusion of the exercise was that a “Digital Pearl Harbor” in the United States was only a slight possibility and that would affect computer systems that are part of the financial infrastructure (Jackson, August. 23, 2002). Nevertheless, discovered vulnerability in 2002 urged U.S. government’s officials to keep information secret until after the needed repairs were implemented on vulnerable Internet systems (Messmer, 2002). This vulnerability according to the FBI, if exploited could have caused many serious problems, such as bringing down widespread telephone networks and also halting control information exchanged between ground and aircraft flight control systems (Barton, 2002, p. A01).

2.3.1. Open possibilities for Al Qaeda and Its Associated Movements’ to attack Critical Information Infrastructure

Although AQAM have not been successful to launch large scale cyber-attack the possibility remains evident as the creativity in the age of globalization never ends. Former remains true since pursue for modernization and efficiency have complicated security of critical infrastructures and have made them reliable of information systems. Today utilities are especially vulnerable given the trend of connecting control systems that run critical infrastructure to the internet. Thus many modern systems that run our everyday life and we depend on are also CII that could be used to affect our security. A 2008 incident in Poland illustrates how simple it can be to compromise a control system by a 14-year youngster who has took control over the city's tram and have created chaos derailing 4 vehicles and injuring 12 people (SANS, January 15, 2008).

AQAM's leadership dedication to exploit internet raises the alarm with these regards. Its apocalyptic agenda and unconventional approach perfectly match the possibility of threatening our CIIP. The Maroochy Shire Queensland incident investigation in 2000 showed that the disaster (millions of liters of raw sewage spilled out into local parks and rivers) to this computerized system was man caused. Apart from the enormous cost to clean up such a mess (in this case more than a $175,000) the environmental, economic and social impacts of a compromise like this are potentially enormous, striking at the core of all levels of sustainability (Slay and Miller, 2008, p.74). Considering what we have previously concluded about the effects of globalization on systems and services' interconnectivity, this incident confirms that the cascade effects caused by such attacks pose greater threat than just damaging CII. This is especially relevant in the context of threats to energy industry companies who are reportedly attacked twice as often as other industries. The challenge is increasing since the large number of these attacks originates from the Middle East (Verton, 2002). Additionally, these statistics usually do not reflect intrusions directed at control systems which lack firewalls or intrusion detection systems, resulting in an under-reporting of the actual number of attacks (Shea, 2003, p.5). Moreover, when U.S. troops recovered Al Qaeda laptops in Afghanistan, officials were surprised to find its members more technologically adapt than previously believed. They discovered structural and engineering software, electronic models of a dam, and information on computerized water systems, nuclear power plants, and U.S. and European stadiums. Nevertheless, critics opposing that threat from cyber-terrorism is real argue that in this case nothing suggested that Al Qaeda individuals were planning cyberattacks, only that they were using the Internet to communicate and coordinate physical attacks (Weimann, 2004, p.8-9).

Experts argue about the different scenarios that could become possible in the context of AQAM threat to CIIP (Weimann, December, 2004). Even though some of these scenarios are exaggerated statistics show that AQAM threat to CIIP is evolving. Hence today we can argue that AQAM can directly affect CII by:

a) Destruction, modification or substitution of software needed by critical infrastructures;

b) Unauthorized access to sensitive or confidential information i.e. spying activities;

c) Attack that could limit access for the agents able to prevent or mitigate the results of the attacks and

d) Identity theft attacks for financial support or other subversive action.

a) Destruction, modification or substitution of software needed by critical infrastructures attacks and AQAM

Recent analyses show that the main tools used to attack critical information systems are malware (computer viruses, worms, logical bombs, Trojans) that modify, substitute and destroy information or block the computer systems. In many reports authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components. The US electricity grid network attack in 2009 for example, confirms the vulnerability of CII in this context (Siobhan, 2009). Today many countries are highly dependable on electricity. Additionally, efficiency and interest for profit urges corporate that manage these systems to digitalize the power grid. A cyber attack against the electric power grid, for example, could potentially destroy equipment and shut down power for an extended period of time, leading to loss of life and severe economic damage.

Arguments that there is no significant cyber-attack organized and executed by AQAM remain valuable as ever (Weimann, December, 2004). However, Bin Laden's and his followers interest for "cyber-world", educational magazines launched by AQAM and other reports about AQAM' interest in CII urge us to more carefully consider AQAM threat to CIIP. Significant intelligence reports have confirmed that Bin Laden had established hacker school which in fact, confirms AQAM' leadership commitment to compromise CII. Osama Bin Laden was also instrumental in creating a cyber university in Pakistan with an emphasis on ways to attack SCADA (Wilsker, September, 2004).

"Al-Battar Training Camp" (the name of one of the magazines mentioned above), was introduced as online terrorist training camp offering education without necessity to travel. The sixth issue, published in March 2004, paid attention among other, on the importance of websites for communications up and down the chain of command (Mansfield, March, 2004). The second journal called "The Technical Mujahid" released by Al-Fajr Media Center in late 2006 in the first two issues covered information security technologies, including software tools for encryption (Denning, 2010).

b) Unauthorized access to sensitive or confidential information i.e. spying activities and Al Qaeda and its Associated Movements;

Electronic espionage is not strange for AQAM. Tools for spying of information exchange in computer networks are also widely used for destructive purposes. Clear example of such attacks represents breaking into the Pentagon's US$300 billion Joint Strike Fighter Project – a weapons program involving the development of a new fighter aircraft. An example of AQAM involvement in spying is the case of using simple password cracking tool available on the internet for free to hack e-mail account of a US diplomat in the Arab world in order to track him down (Ranstorp, 2004). In addition, the US National Infrastructure Protection System reported that AQAM had „sought information on (SCADA) systems available on multiple SCADA-related websites". They specifically sought information on water supply and wastewater management practices in the U.S. and abroad‟ (NIPC, January 30, 2007). Such information could be useful in planning either physical or cyber attacks to compromise SCADA-controlled critical infrastructures protection.

The forum Minbar ahl al-Sunna walJama‟a offered a hacking manual that was said to be written in a pedagogical style and discussed motives and incentives for computer-based attacks, including political, strategic, economic, and individual. The manual discussed three types of attack: direct intrusions into corporate and government networks, infiltration of personal computers to steal personal information (we will address this bellow), and interception of sensitive information such as credit card numbers in transit (Pool, October 11, 2005).

c) Al Qaeda and its Associated Movements' ability to launch cyber-attack that could limit access for the agents able to prevent or mitigate the results of the attacks

AQAM threats to CIIP could include cyber-attack that could limit authorities' access to prevent or mitigate the results of cyber attack and thus cause further consequences. The 2002 incident caused by "slammer" worm and above discussion about AQAM's dedication to cyber-terrorism and attack on CII explains why AQAM pose serious concerns for CIIP. As it was launched on internet, "the slammer" doubled in size every 8.5 seconds and infected more than 90 % of vulnerable hosts within 10 minutes. The worm was also released at a nuclear power plant in Ohio, USA and took command of the SCADA system causing operators to lose control for around six hours (Poulsen, August 19, 2003).

d) Al Qaeda and Its Associated Movements' ability to conduct identity thefts' attacks for financial support or other subversive action

Identity theft is one of the most common cyber-attacks. Usually inadequate computer security practices within organizations are biggest contributors to this. Boston College (with personal information for up to 106,000 alumni) and Chico State University of California (with information of about 59,000 students including their social security number) in March 2005, reported that a hacker had gained unauthorized access to computer database records (Bank and Conkey, March 24, 2005).

Although U.S. Department of Energy has tried to cover network intrusion in June 2006, officials acknowledged that names and personal information belonging to more than 1,500 employees of the National Nuclear Security Administration (NNSA) had been stolen. Additionally during the 2007, UK trial for 2005 London terrorists' bombing, accused revealed that 72 stolen credit cards were used to register over 180 Internet web domains at 95 different web hosting companies.(Onley, and Wait, August 21, 2006).

Evidence that London based associated Al Qaeda group also laundered money charged to more than 130 stolen credit cards through online gambling websites, clearly confirms that AQAM represent significant threat to CIIP due to technical challenges in cyber-world.

The above discussion over the AQAM' threat to CIIP raises issues that go beyond the question of *whether cyber-terrorism is taking place today or whether it is a serious threat for the future?* It actually showed that the modern technology has increased AQAM capability to threat CIIP and thus influence our way of living directly. It is more than evident that AQAM can do this at little cost and risk, and from anywhere in the world. Not only can they launch attacks through the Internet and directly damage the CII, they can cause cascade effects in support of terrorist objectives, regardless of whether these acts are characterized as cyber-terrorism or not. They do not need to worry about acquiring or manufacturing explosives, crossing borders, or funding their operations. Moreover, as Kellner (2006) argues, "*different groups gain access to technologies of destruction and devise plans to make conventional technologies, like the airplane, instruments of destruction then dangers of unexpected terror events, any place and any time proliferate and become part of the frightening*" (p.174).

This and previous discussions about AQAM's evolution and center of gravity have so far answered the question *how* and have only touched *why* AQAM represent such security threat. Discussing how AQAM have shifted the fight we have explained part of the problem. However many experts agree that the ability for AQAM to represent such threat comes from its ability to recognize existing challenges that largely influence effective CIIP.

3. Al Qaeda and its Associated Movements' Ability to Employ Challenges to Effective Critical Information Infrastructure Protection

Dependence on technology and pursue of computerization have accumulated our ability to incorporate the necessary safety features, including detection, prevention and mitigation standards and practices. The vulnerability created by these gaps affects not only utility services, but also databases and systems that maintain a variety of sensitive and confidential information that could be well used by AQAM

We will address challenges that affect CIIP from two aspects. First we will explain how different stakeholders' threat perception in the context of AQAM influence challenges to CIIP. Then by discussing technical challenges we will explain why and how AQAM's have became capable to affect CIIP.

3.1. Different stakeholders' threat perception

Although AQAM' agenda is global and apocalyptic all stakeholders involved in CIIP do not share the same threat perception regarding potential AQAM's attack. Different threat perceptions often come either from different stakeholders' technological development or different stakeholders' interests. Different stakeholder's threat perceptions usually pose challenges for effective CIIP for several reasons such as:

- Different definition to CII,
- Different approach in managing CIIP,
- Different legal approach toward privacy and
- Different security considerations among stakeholders.

We will address these challenges separately.

3.1.1. Defining Critical Information Infrastructure Protection as a Challenge

Even though CIIP is importnat stakeholders and experts disagree over the definition of CIIP. Different stakeholders' threat perception influence different definition for CII. Defining different systems and services as critical reflects the security measures that are taken toward effective CIIP (Joplin, 2007). This dichotomy opens the possibility for AQAM by employing global interconnected information systems to attack less protected systems and cause global effects.

Existing differences among other basically come from different states' information and technological development. The expansion of globalization was as we have seen largely supported by the growth of technology. Today communications or information systems and services that they provide are crucial to the functioning of a modern economy, security, and other essential social values. These systems' availability, reliability, vulnerability and resilience have therefore dramatically affected modern virtues. As a result markets, as well as Governments around the globe depend on them to function properly.

Pursue for cost reduction and efficiency have also introduced information systems in other areas. As we have seen from the above these systems are needed to support the work of other critical infrastructures, from power distribution and water supply to transportation and finance. On the other hand we have also seen that internet and globalization have enabled these systems and services that they provide to expand beyond national borders and increase the importance of some actors. Thus availability, reliability, vulnerability and resilience of these systems and services, although in a different way, affect many stakeholders. Different affection results in different threat perception (Keneth, 2005, p.12-18).

Therefore some states (regarding their development) consider CII only the first level i.e. the communication and information systems that are crucial for functioning of a modern economy, security and other essential social values. Others have also developed SCADA (previously discussed) and thus consider this under the CII and have build measures for its protection. Countries that doesn't need SCADA (since are less developed) usually need cheaper and different software. Different software requirements to support these systems however could inhibit the ability for coordinated response (Gaudin, July 19, 2002).

Effective response to security breaches for example, require large numbers of parties to coordinate and make appropriate necessary investments. The motivation that one conscientious network owner has to invest in security measures is reduced if the owner believes that other connected networks are insecure. The situation is further complicated since assigning liability for security breaches is difficult. In many situations user cannot easily identify the source of the problem i.e. whether it was due to the user's software or software used by others (Donzelli and Setola, December 18-20, 2001). Hence we will address technical challenges later usage different software lead us to next challenge to effective CIIP posed by different threat perception.

3.1.2. Different approach in managing CIIP as a challenge

Even though some countries and organizations have recognized the importance of effective CIIP and have similar definitions of what is considered to be CII different strategic approaches also represent challenge to effective CIIP. The issue of establishment of different strategies is not just present among different states or private actors, but also exists due to a different international organizations' interest in CIIP. Thus the advantage of cooperation could potentially turn in a huge disadvantage especially when these different strategies could result in different standardizations (Messmer, February 14, 2003).

The NATO 2007 Annual Report addressing this issue conclude that from 4 countries studied (France, United Kingdom, Germany and US) with regards to their strategic approach for critical infrastructure protection-(CIP), including information infrastructure too, all 4 countries have different strategic approach in CIP (Joplin, 2007). This issue is even more complex due to the EU interest in CIIP (CIIP, 2009, p.149).

On the other hand global AQAM' threats and potential of global and atomized effects of cyber-attacks on CII undermine economic and political issues and standards. AQAM's presence in remote pockets of South-East Europe and reports about its supporters' cyber-efficiency from the region pose serious challenges not just for CIIP but for security in broader context in many European countries members to NATO and

EU. Many of the South-Eastern states follow Euro-Atlantic standardization. However, the issue arises when they also follow some other organizations' approach for example UN standardization (For example Macedonia is 11th country n the World that have accepted Disaster Risk and Reduction plan, which differ from NATO and EU approach in Crisis management approaches). This could potentially affect software procurement (they will be free to follow principal of efficiency and law costs in bilateral procurement which will result not just in different software standards but different software).

3.1.3. Different legal approach toward privacy as a challenge for effective CIIP

Legal issues also challenge effective CIIP from AQAM's threats. These challenges come from the necessity to prevent potential Cyber-attack on CII. In his report for US Congress Wilson notes that preoperative surveillance characterizes the early stages of many cyber-attacks. He claims that for success secret planning may be conducted in Internet chat areas, where hackers meet anonymously to exchange information about computer vulnerabilities, or new cyber-attack tools (Clay, 2005).

However, limiting factor for either preventing a cyber-attack or identifying the attackers is a lack of data revealing evidence of pre-operative surveillance and on-line planning activity that is traceable back to terrorist groups.

In order to undermine these disadvantages intelligence agencies should monitor computer chat rooms where AQAM' individuals are meeting. Nevertheless this raises the question that has already caused turbulence in liberal and legal world. Different threat perception urges some state to push the balance between duty to protect and liberal values. Regarding the threat perception US has until now usually preferred public safety. European alias on contrary, have always had great concerns for protection of individual rights. This discrepancy hold potential for serious challenges toward effective and coordinated CIIP if one considers similar challenges in the recent counterterrorist efforts (Birkinshaw, 2010 p. 42–43).

3.1.4. Different security considerations among the stakeholders as a challenge to effective CIIP

AQAM have proven that is easy to employ modern systems we rely upon and use them against us. Development of these systems in virtual security vacuum in the age of globalization has made them soft targets. The architects of these networks and infrastructures are usually concerned with profit. In fact, the cost reduction and efficiency is their highest priority (Barber, March 1992, p. 24).

At the same time the growing dependence on these networks had not been matched by parallel focus on their security. On a contrary as Stephen Flynn (2004) argues "*…security considerations have been widely perceived as annoying speed bumps in achieving their goals (referring to the architects of these systems), …As a result the systems that underpin our prosperity are soft targets*…" (p. x).

Recent practice shows that private corporate have been reluctant to be involved in intelligence sharing, especially if that hurts the profit (Gallis, 2004, p. 124-126). Furthermore many argue that much of the cyber-attacks remain unreported (Clay, 2008, p.28-29). To some extent this is result of the states' lost ability to attribute its power in this age of globalization. Traditionally, private actors were objects, not subjects of international politics. States, or groups of states acting through international institutions, might try to regulate their behavior, but the private groups had little responsibility for setting norms (Treverton, 2003, p.51). In fact, today private sector owns many of critical “levers” that on one or another way have enabled states’ monopoly in the past. These issues nevertheless confirm more than ever the necessity of global and holistic legal approach toward establishment of legal standards with international consensus.

3.2. Al Qaeda and its Associated Movements’ ability to employ technical challenges for effective Critical Information Infrastructure Protection

AQAM have already been attracted by cybercrime potentials to exploit technical challenges that make government and civilian critical infrastructure systems easy targets (Krebs, 2007, p. D01). Criticizing globalization as an essential instrument for the rapid spread of terrorist causes Ralph Peters (2005) in this context claims that *“(T)he Internet, for all its practical utility, has been the greatest tool for spreading hatred since the development of movable type for the printing press. Islamist fanatics, neo-Nazis and pedophiles now can find each other with startling ease...*”. As a result it could be argued that today computer networking technology has also straddled the boundaries between cyber-warfare, cybercrime, and cyber-terrorism. Credible arguments on the other hand, could undermine all of the above mentioned challenges and any further discussion on AQAM threat to CIIP since the proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine. However, linkages do exist between terrorist groups and criminals that allow AQAM networks to expand internationally through internet.

Sharm-el Sheikh and London attacks during 2005 were facilitated by on-line training. Terrorists have been quick not only to adopt the latest communications technologies, such as cell phones, but also to exploit the highly competitive market by finding vendors willing to sell to purchasers that refuse to give their names (Sims, 2007, p.393). A 2007 trial in the U.K. revealed a significant link between Islamic terrorist groups and cybercrime. In June 2007, three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, pled guilty, and were sentenced for using the Internet to incite murder. The men had used 110 different stolen credit cards at online web stores to purchase items to assist fellow jihadists in the field - items such as night vision goggles, tents, global positioning satellite devices, and hundreds of prepaid cell phones and more than 250 airline tickets (Krebs, 2007, p. D01). The 2007 testimony revial how existing technical challenges represent significant opportunity for AQAM and threaten CIIP.

One of the greatest challenges of cyber-attacks is to identify the attacker. New and sophisticated cyber-tools allowed AQAM to remain unidentified while they direct cyber-attacks through the Internet (Greene, 2007). This is why the proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine. On the other hand lack of significant evidence of cyber-terrorism reduces concerns and open possibility for AQAM.

Challenges addressed previously (regarding the threat perceptions) have opened an important issue about the vulnerabilities in software and computer system configurations. As we saw different threat perceptions result in different definition of CII or different strategy approach which influences the quality in software products.

Vulnerabilities exist largely as a result of poor security practices and procedures, inadequate training in computer security, or poor quality in software products (NIPC, 2003). Nevertheless there is significant amount of experts who criticize the commercial of the shell software for releasing new products with errors. For example in September, 2003, Microsoft Corporation announced three new critical flaws in its latest Windows operating systems software. Security experts predicted that computer hackers may possibly exploit these new vulnerabilities by releasing more attack programs, such as the "Blaster worm" that have targeted other Windows vulnerabilities causing widespread disruption on the Internet (Jaikumar, 2003, p. 1). Similarly in 2012 Microsoft again admitted that users of its "Xbocks" Live network are being hacked, but has denied that it was any hardware, software or networking flaw. Nevertheless, Microsoft only thought without certainty, that its customers were hijacked by cyber criminals (Farrell, 2012).

Approximately 80 % of successful intrusions into US federal computer systems reportedly can be attributed to software errors, or poor software product quality (Green, Nov. 2002). Security concerns regarding the AQAM threat to CII arise since there is little evidence of improvement in the security features of most products. Therefore different actors' interest, (previously discussed), reflect in the context of technical challenges too. In his testimony before the House Select Committee on Homeland Security, Richard D. Pethia, claimed that

> … *developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities....We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until their customers demand products that are more secure, the situation is unlikely to change."* (Pethia, 2003).

In response to complaints, the software industry reportedly has made new efforts to design software with more secure code and with architectures that are more secure. However, many software industry representatives reportedly agree that no matter what investment is made to improve software security, vulnerabilities will continue to exist (Charney, 2003, p. 9).

Efforts for conducting software standardization as process also come with challenges. Many organizations and security services have established a list of reliable software companies. Process also known as a certification and accreditation under common criteria usually sink under the pressure of time and technological boom. Even for the most organized administration this process take time almost a year and is costly. AQAM and cyber-criminals' adaptability could undermine these efforts with ease (Messmer, 2003).

At the same time, computer hackers and AQAM intentionally scan the Internet to find and infect computer systems that are miss-configured, or lack current software security patches. Even computers with current software security patches installed may still be vulnerable to a type of computer network attack known as a "Zero-Day exploit". Information about computer vulnerabilities could be easily found "black market". For example, Bob Francis (2005) explains that:

> *a list of 5,000 addresses of computers that have already been infected with spyware and which are waiting to be remotely controlled as part of an*

> *automated “bot network” reportedly can be obtained for about $150 to $500. Prices for information about computer vulnerabilities for which no software patch yet exists reportedly range from $1,000 to $5,000. Purchasers of this information are often organized crime groups, various foreign governments and companies that deal in spam”* (Francis, January 28, 2005).

4. What needs to be done to improve critical infrastructure information protection and resilience from AQAM?

Without holistic and comprehensive approach that will consider national, regional and international efforts including critical information and infrastructure resilience improvement there will be no effective CIIP from AQAM threats. Additionally challenges and AQAM’s modus operandi discussed above, urge us to consider additional methods that go beyond traditional security concepts. Effective CIIP should therefore consider all stakeholders in a way where public sector adapts its role to stimulate corporate social responsibility efforts. Legislative and judicial activists must reflect this orientation if we are to secure our livelihoods and individual rights. Abuses and poor security management must have penalties and sufficiently discourage information mismanagement and abuse. This in turn will limit the opportunities available to terrorists.

Beside direct defensive and preventive measures and mechanisms against potential threat to CIIP one must consider indirect approach toward effective social engineering that will suffocate AQAM’ recruiting capability.

4.1. Direct mechanisms (approach) toward effective critical information infrastructure protection from Al Qaeda and its associated movements

Clausewitz (1989) has long ago argued that to wage war effectively one must understand its true nature without mistaking it, or trying to turn it into, something it is not (p.88). In this context Christine Fair and Bryan Sheperd’s (2006) quantitative research into the support base for terrorism led them to conclude that broad generalizations were invariably inaccurate and thus counter-terrorist interventions must be highly tailored towards highly detailed, country specific target audiences’ (p:51-52). Rational of the complex system analyses of AQAM’s modus operandi in the age of globalization is that effective holistic approach requires centralize planning and decentralize execution. Although there is no ideal model for organizing CIIP and there is no strategy or approach that could guarantee 100% protection or resilience, centralize planning should consider all stakeholders especially private actors. Direct approach toward effective critical information infrastructure protection from Al Qaeda and its associated movements should focus on coordinated efforts among all stakeholders in three directions. First, protective system such as encryption of communication and data; second, mechanism and supporting technologies with proper and timely updates; and finally, people involving policies and procedures for the proper use of systems and general awareness and security reporting. All three must be considered to ensure one’s system and networks are secured.

Nevertheless comprehensive worldwide study conducted for German Government on critical infrastructure protection claims that one of the key issues in this area is lack of cooperation among public and private sectors.

The study included over 20 countries and has identified three general models in the business. First, functions and competencies relating to critical infrastructure protection (CIP) are spread between different organs and attempt is made to integrate the private sector at all levels of CIP. Second approach – All hazards approach, according to the study entails both the protection of critical IT infrastructures and also the physical protection of critical infrastructures. In this approach there is no clear separation between the components and ministries of defense have generally emphasized role. Third approach according to the study is special case which include Chinese model where no cooperation between stakeholders exist. Big “take away” from the study in the context of our debate is that “cooperation between the public and private sectors at the strategic planning level is often totally absent or else only of a rudimentary nature”.

Helpful tool to overcome this issue is to build upon the international efforts such as the European Commission, which began to promote and endorse public policy initiatives to stimulate corporate social responsibility. Although business driven this cooperation’s initiatives regarding the changing role of the business in society, investments, trade and building sustainable development could be quite helpful to stimulate cooperation in effective CIIP from AQAM threats. For example, in 2002, the European Commission published ‘The Communication concerning Corporate Social Responsibility: A business contribution to Sustainable Development (EC 2/7/2002). Additionally such cooperation and efforts should be crucial especially for indirect approach while building social stability (we will refer to this later).

Direct cyber security will not be achieved if we do not consider efforts to improve CII resilience. These efforts should include, but are not limited to employment of a strong security policy design, implementation of a comprehensive disaster recovery plan, application of the latest security technologies, conducting regular security audits, working with law enforcement when security breaches do occur etc.

Zadek & Swift (2002), argue that one of the biggest challenges for governments in the globalized world is to find a way to design and implement public policy that will generate leadership and partnership-based innovation (p.22). The UK experience with overcoming crisis in governance proved that partnership projects, with governments, companies and civil society organizations working together could lead to collective action to address demands that cannot be met by the state (Moon, 2004, p. 3-27).

Since threat to CIIP posed by AQAM as we discussed above could affect all society in many ways policies like this are welcome to provide for central planning. Although central planning will undermine or reduce technical challenges (discussed above) some of the technical issues regarding different standards in software procurement or security programs will be also reduced if not solved.

In addition projects like this will reduce differences among states and other actors in defining CII and model of approach in CIIP. Benefits of these innovative actions for cooperation and their systematic acceptance and application among all stakeholders will further reduce difference in legal approach and security perception.

Small poll that I had ran in Macedonia especially for this paper within 12 middle Macedonian companies shows that 92.3 % of the companies' employees don't distinguish between cyber-crime and cyber-terrorism. Although most of the answers focus on two forms of cyber attack, still and damage data, only a few understood the difference. What is also interesting is that expectations for an attack are very low even some of them indirectly are included in IT maintenance of the Ministry of defense.

Although this poll was limited the point that it makes is that one of the reasons for different approaches, threat perceptions and maybe other challenges to effective CIIP is lack of education and awareness for the threat. Governmental efforts toward increasing corporate social responsibility through different clusters of activities that will enhance education and awareness are more than welcome. Since other researches pay in depth attention to specific techniques that could increase resilience and act preventively for CIIP we will not discuss such measures.

4.2. Social stability as a key to reduce AQAM's ability to threaten CIIP

In his speech during Brooking institution forum Fukuyama (2003) pointed that, "...*terrorism practiced by Al Qaeda is nothing but means to an end*". Kilkullen (2005), on the other hand argues that solution to address AQAM should not focus exclusively on the classic counterterrorism approach but on counterinsurgency (p. 597). Much of the literature dealing with the issue focuses on efforts that will reduce insurgents' ability to recruit the populace and gain support.

Discussion about AQAM's modus operandi among other revealed that idea of Al Qaeda and its ability to oppose is the driving force that connects different Muslim groups and individuals. However many claims that stimulation to join that idea comes from the social frustration caused by the gap between poor and the rich and as interpreted, *Western aggressive idea for democratization* (Kepel, 2005; Roy, 2004). Fixed between dictatorship and depression on one hand and western top-down globalization followed by technology and wealth many Muslims easily turned in to a prey of social isolation (Leiken, 2005; Bawer, 2005). Other who migrated faced substantially higher unemployment rates for Muslims than for mainstream society, radical indoctrination, and governmental neglect (Sullivan and Partlow, 2006, p.14).

Innovative mechanisms of governance that will focus on social stability and improvement of the quality of life are more than welcome and will contribute to more effective CIIP. These interventions are generally regarded as public sector responsibilities, nevertheless, private sector and international and local nongovernmental organizations are often better adjusted to act toward reducing these sources.

Clear example of such creative mechanism is the case with the innovator of the "Sasser worm" that has been hired as a "security software programmer" by a German firm. He is responsible for firewalls, which will stop suspected files from entering computer systems. Other mechanisms like this are also available to close the social gaps. All of these efforts along with direct efforts and specific techniques to protect CII will improve its resilience and reduce AQAM's capacity to threaten CIIP.

Conclusion

The emergence of new non-state actors in the post Cold War reality have dramatically changed security environment around the globe. Modern terrorism practiced by Al Qaeda and its associated movement has posed serious threat to our security. AQAM's interest to engage cyber-world for its own purposes raises serious alarm in the context that utilities are especially vulnerable given the trend of connecting control systems that run critical infrastructure to the internet. Although AQAM have not been successful to launch cyber-attack that will cause mass casualties, environment damage or financial effects, the possibility remain alarming since creativity in the age of globalization never ends.

AQAM's interest to affect our way of life through cyber-world urges us to consider measures to improve critical information infrastructure protection and resilience. Regarding the AQAM's center of gravity effective CIIP in an age of globalization requires holistic and comprehensive approach. This approach should consider, protective systems, supporting mechanisms and technologies with proper and timely updates of people involving policies and procedures for the proper use of systems and general awareness and security reporting. However, we will not accomplish effective CIIP without strong security policy design, implementation of a comprehensive disaster recovery plan, application of the latest security technologies, conducting regular security inspections, implementing advanced training and cooperation with law enforcement when security breaches do occur etc.

Direct mechanisms like technical, legal, political, security or military solutions, remain as valuable as ever, but implemented alone could only postpone the threat. Hence we must consider social stability if we are to mitigate modern terrorists' ability to threat cyber-security. Innovative mechanisms of governance that will focus on social stability and improvement of the quality of life are more than welcome and will contribute to more effective CIIP. Partnership projects, between governments, companies and civil society organizations working together could lead to collective action to address demands that cannot be met by the state or private corporations alone. Finally this will contribute to the environment that will accumulate recruiting energy of AQAM.

References

1. Al Battar (2004), Available at: http://siteinstitute.org/bin/articles.cgi?ID=publications9504&Category=publications&Subcategory=0,

2. Bank, D. and Conkey, C. (March 24, 2005). *New Safeguards for Your Privacy*. The Wall Street,

3. Barber, R. B. (March 1992). *Jihad vs. McWorld*. The Atlantic,

4. Barton G. (June 27, 2002). *Cyber-Attacks by Al Qaeda Feared*. Washington Post

5. Bawer, B., (2005). *While Europe Slept: How Radical Islam is Destroying the West from Within.* New York: Doubleday,

6. Berger, P. L (2003). *The Cultural Dynamics of Globalization*," in *Many Globalizations: Cultural Diversity in the Contemporary World*. In: P. L. Berger and S. P. Huntington, (Ed.), (p. 1-16). New York: Oxford University Press,

7. Birkinshaw, P. (2010). *Freedom Of Information: The Law, The Practice And The Ideal*. Cambridge University Press,

8. Charney, S. (2003). *Statement before the House Committee on Armed Services made by Chief Security Strategist, Microsoft, on the issue: Terrorism, Unconventional Threats and Capabilities.* Hearing, (July 24, 2003). Information Technology in the 21st Century Battlespace, Subcommittee,

9. Clausewitz, C. (1989). *On War*, trans. Michael Howard and Peter Paret, Princeton University Press, New Jersey,

10. Clay, W. (2005). *Computer Attack and Cyberterrorism: Vulnerabilities and Policy issues for Congress*. Congressional Service Research for Congress,

11. Clay, W. (2008). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. CRS Report,

12. Denning, D. E. (2010). *Terror's Web: How the Internet is Transforming Terrorism*. In: Y. Jewkes and M. Yar, (Ed.) *Handbook on Internet Crime*. Willan Publishing,

13. Denning, D. (2001). *Activism, Hactivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy*. In Arquilla J. and Ronfeldt, D., (Ed.) *Networks and Netwars*, (p.241). Rand Corporation,

14. Donzelli, P. and Setola, R. (18-20 December 2001). *Putting the Customer at the Center of the IT System – A Case Study* (paper presented at the *Euro-Web 2001 Conference – The Web in the Public Administration*), Pisa, Italy,

15. European Union. (2003). *A Secure Europe in a Better World, A European Security Strategy*. Brussels, The European Council,

16. Fair, C. C. and Sheperd, B. (2006). Who Supports Terrorism?, Evidence from Fourteen Muslim Countries. *Studies in Conflict and Terrorism*, *29(1),* 51-74,

17. Farrell, N. (February 09, 2012). *Microsoft admits Xbox hacks*. TechEYE.net, From: http://news.techeye.net/security/microsoft-admits-xbox-hacks,

18. Ford. P. (September 27, 2001). *Why Do They Hate Us*, The Christian Science Monitor,

19. Forst. B. (2009). *Terrorism, Crime and Public Policy*. Cambridge University Press: Cambridge,

20. Friedman T.L. (2002). *The Lexus and the Olive Tree: Understanding Globalization*. New York: Farrar, Straus and Giroux,

21. Flynn, S. (2004). America the Vulnerable. New York: Harper Collins, p. x,

22. Fukuyama F. (1992). *The End of History and the Last Man*. New York: Free Press,

23. Fukuyama F. (2003). *Summary of Fukuyama's comments on terrorism made at a Brookings Institution forum*, May 2003. From: http://www.brook.edu/dybdocroot/Comm/events/summary20030514.pdf,

24. Gallis E. P. (2004). *European counterterrorist efforts: Political will and diverse responses*. Nova Publishers,

25. Gaudin, S. (July 19, 2002). *Security Expter: U.S. Companies Unprepared for Cyber Terror*. Datamation,

26. Green, J. (Nov. 2002). *The Myth of Cyberterrorism*.Washington Monthly,

27. Greene, T. (October 24, 2007). *Storm Worm Strikes Back at Security Pros*. NetworkWorld.com,

28. Giddens, A. (1990). *The Consequences of Modernity*. Cambridge: Polity Press,

29. Huntington, S. P. (1996). *The Clash of Civilizations and the Remaking of World Order.* New York: Simon & Schuster,

30. Jaikumar, V. (September 15, 2003). *Attacks on New Windows Flaws Expected Soon*. Computerworld, vol. 37, No. 37,
31. Joplin, L. (2007). *The Protection of Critical Infrastructure*. NATO Parliamentary Assembly, Annual Session 162 CDS 07,
32. Keneth, C. (2005). *Ensuring (and Insuring?) Critical Information Infrastructure Protection*. Report of the 2005 Rueschlikon Conference on Information Policy, Rueschlikon, Switzerland,
33. Kellner, D. (2005). *Globalization, Terrorism and Democracy: 9/11 and its Aftermath,* in: *Confronting Globalization: Humanity, Justice and the Renewal of Politics* (pp. 172–188). Basingstoke [etc.]: Palgrave Macmillan,
34. Kellner, D. (2006). *Globalization, Terrorism and Democracy : 9/11 and its Aftermath,* in: P. Hayden (Ed.), *Confronting Globalization: Humanity, Justice and the Renewal of Politics,* (pp. 172–188). Book News, Portland,
35. Kellner, D. *Globalization, Terrorism, and Democracy: 9/11 and its Aftermath.* Available at: (http://www.gseis.ucla.edu/faculty/kellner/),
36. Kepel, G. (2005). *The War for Muslim Minds: Islam and the West*. Cambridge, MA: Harvard University Press,
37. Kilcullen, D. (2005). *Countering Global Insurgency*. The Journal of Strategic Studies. *28*(4), 597 – 617,
38. Krebs, B. (July 6, 2007). *Three Worked the Web to Help Terrorists*. The Washington Post,
39. Krebs, B. (July 6, 2007), *Three Worked the Web to Help Terrorists*, The Washington Post, p. D01,
40. Krim, J. (September 24, 2003). *Security Report Puts Blame on Microsoft*. Washingtonpost.com,
41. Leiken, R. S. (2005). *Europe's Angry Muslims*. Foreign Affairs, July–August,
42. Lemos, R. (August 26, 2002). *What Are the Real Risks of Cyberterrorism?*. ZDNet,
43. Mark E. S., Huckabey M. J., Schindler R. J. and Lacey J. (2008). *The Terrorist Perspectives Project, Strategic and Operational Views of Al Qaeda and Associated Movements*, Naval Institute Press,
44. Mansfield, L. (March, 2004). *Everything You Always Wanted to Know About Becoming a Terrorist, but Were Afraid to Ask*. Northeast Intelligence Network,
45. McKay, A. (2011). *The Arab Spring of Discontent*. e-International Relations available at: http://www.e-ir.info/wp-content/uploads/arab-spring-collection-e-IR.pdf,
46. Mead, R. W. (2004). *Power, Terror, Peace and War: America's Grand Strategy in a World at Risk*. New York: Alfred A. Knopf,
47. Merasheimer, J. (August 1990). *Why We Will Soon Miss The Cold War*. Atlantic Monthly,
48. Messmer, E. (July 9, 2002). *President's Advisor Predicts Cyber-catastrophes Unless Security Improves.* Network World Fusion,
49. Messmer E. (February 14, 2003). *White House issue "National Strategy to Secure Cyberspace,* Network World Fusion,
50. Moon, J. (2004). *Government as a driver of corporate social responsibility: the UK in comparative perspective.* ICCSR, Research Paper Series, 20-2004. ICCSR, University of Nottingham,

51. NIPC. (January 30, 2002). *Terrorist Interest in Water Supply and SCADA Systems*. Information Bulletin 01-001, The U.S. National Infrastructure Protection Center,

52. National Infrastructure Protection Center (NIPC). (April 15, 2003) *The list of the 10 most commonly exploited vulnerabilities for Windows systems and for Unix systems*,

53. Onley, D. and Wait, P. (August 21, 2006). *DOD's Efforts to Stave off Nation-State Cyberattacks Begin with China*. Government Computer News,

54. Peters, R. (May 23, 2005). *Myths of Globalization*, USA Today,

55. Pethia, R. D. (2003). *Testimony before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity*. In: *Science, and Research and Development*, *Overview of the Cyber Problem — A Nation Dependent and Dealing with Risk*, *(hearing, June 25, 2003).* CERT/CC, Software Engineering Institute, Carnegie Mellon University,

56. Pew survey, (2003) retrieved from: http://people-press.org/reports/display.php3?ReportID=185,

57. Pool, J. (October 11, 2005). *Technology and Security Discussions on the Jihadist Forums.* Jamestown Foundation,

58. Poulsen, K. (August 19 2003). *Slammer Worm Crashed Ohio Nuke Plant Network*, Security Focus,

59. Ranstorp, M. (2004). *Al-Qaida in Cyberspace: Future Challenges of Terrorism in an Information Age*. in L. Nicander and M. Ranstorp (Ed.), *Terrorism in the Information Age – New Frontiers?*. Stockholm: Swedish National Defence College,

60. Roggio B. **(**February 18, 2009). *Sufi Mohammed 'hates democracy' and calls for global Islamic rule*,The Long War Journals,

61. Roy, O. (2004). *Globalized Islam: The Search for a New Ummah* (New York: Columbia University Press, 2004,

62. Sageman, M. (2004). *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press,

63. SANS (2002). *FBI Twenty Most Critical Internet Security Vulnerabilities*, SANS News,

64. SANS. (January 15, 2008). *Polish Teen Faces Charges for Allegedly Manipulating Train System (January 11, 2008)*. SANS News bites, Volume: X, Issue: 4. From: http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=4#sID310,

65. Sims, E. J. (2007). *The Contemporary Challenges Of Counterterrorism Intelligence* in: *Countering terrorism and insurgency in the 21st century: international perspectives*. In: J. J. F. Forest, (Ed.), *The making of a terrorist: Recruitment, training and root causes. Vol 1: Recruitment,* (p. 393). London: Praeger Security International,

66. Siobhan G. (April 8, 2009). *Electricity Grid in U.S. Penetrated By Spies*. Wall Street Journal,

67. Stephen, F. (2004). *America the Vulnerable*, New York: Harper Collins,

68. Stiglitz, J. E.(2003), *Globalization and Its Discontents*. New York: W.W. Norton

69. Sohail H. H. & Miller, D. (2001). *Boundaries and Justice: Diverse Ethical Perspectives* (eds.), p.197 Princeton N.J.: Princeton University Press,

70. Symantec. (February, 2003). *Symantec Internet Security Threat Report*,

71. Shea, A. D. (February 21, 2003). *Critical Infrastructure: Control System and Terrorist Threat*. Congressional Research Service - CRS,

72. Slay, J. and Miller, M. (2008). *Lessons Learned from the Maroochy Water Breach*. in: E. Goetz and S. Shenoi (Ed.), *Critical Infrastructure Protection,* IFIP International Federation for Information Processing, Volume 253,(pp. 73–82). Boston: Springer,
73. Sullivan, K. and Partlow, J. (August 13, 2006). *Young Muslim Rage Takes Root in Britain*. Washington Post,
74. The White House. (2002). *The national Security Strategy of the United States of America*, Washington DC, September,
75. Treverton, F. G. (2003). *Reshaping the National Intelligence for an Age of Information*. Cambridge University Press,
76. United Nation. (2004). *High-level Panel on Threats, Challenges and Change, A more Secure World: Our Share Responsibility*. New York, UN,
77. Van Evera, S. (2006). *On Every Front : A Strategy for the War on Terror*, in *How to Make America Safer: New Polices for National Security.* In: Stephen Van Evera, (Ed.) p.47-59. Cambridge, MA The Tobin Project 2006,
78. Verton, A. (August 11, 2003). *Definition of Cyber-terrorism*. Computerworld,
79. Wallace, B. (June 30, 2002). *Security Analysts Dismiss Fears of Terrorist Hackers*. San Francisco Chronicle,
80. Weimann G. (December, 2004). *Cyberterrorism, How Real is the Threat?*, Special Report, United States Institute for Peace. Washington, DC, From: http://www.usip.org/files/resources/sr119.pdf,
81. William J. (August 23, 2002). *War College Calls Digital Pearl Harbor Doable*. Government Computer News,
82. Wilsker I. (September, 2004). *Cyber Terrorism A Portent of Thing to Come, Golden.* Triangle PC Club From the September*,* 2004 issue of the I/O Port Newsletter,
83. Wilson, C. (2005). *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congress Research Service- CRS,
84. Zadek, S. and Swift, T. (2002). *Corporate Responsibility and the Competitive Advantage of Nations*. Copenhagen: The Copenhagen Centre & AccountAbility,