Global Scientific JOURNALS

GSJ: Volume 6, Issue 6, June 2018, Online: ISSN 2320-9186

www.globalscientificjournal.com

FIGHTING SOCIAL TERRORISM THROUGH CYBER SECURITY

Fergus U. Onu

Email: *uche.fergus@gmail.com*, Gsm: *+2348034311177*

Department of Computer Science, Ebonyi State University, Abakaliki – Nigeria

ABSTRACT

Terrorism is a major problem of the world today. Terrorism has affected government policies, inflicted injuries on men and women and caused physical damages to both people and infrastructure across the world. Computer, networks, electronic and other resources are usually the prime targets of suchterrorist attacks. This paper highlights existing cyber threats, discover efficient techniques for handling them and spread the awareness of such discovered information. A detailed study of information from secondary sources which includes the rich content of the internet and physical libraries were used to reveal that terrorist groups take advantage of certain anonymity provided by the internet especially through the social media platforms to perpetrate their evil intentions. The revelation arms individuals, organizations and government agencies with the strategy to adequately prepare to address all their security deficiencies while on the internet and thereby enhances their, safety, productivity and overall preformance both in business, government and family life.

KEYWORDS: Terrorism, Electronic Resources, Terrorrist groups, Cyber threats, Cyber Security.

.

1.0 INTRODUCTION

Terrorism is now a global security challenge. Terrorists attack their targets in many ways and through different means. Most terrorist activities are carried out through the internet and other electronic systems. Terrorists hack bank accounts, classified government information and create fear on the citizens. They target civilians, civilian interest and civilian installations. But with the use of strong cyber security system techniques, information, lives and installations could be protected. Cyber security is the protection of computers and allied systems from theft or damage. The computer system is where most classified information are stored for future use. For this reason if it is not properly guided it could lead to disaster and loss of lives. Information needs to be guided and secured properly by the use of cyber security techniques to reduce risks, cyber security includes controlling physical access to the hardware, as well as protection against harm that may come through software and network access.

Terrorism frequently makes headlines on national and international dailies, threatening or attacking governments, private businesses and ordinary citizens in many parts of the world. It has become one of the most important threats to peace, security and stability in the world. But what does it mean? What is the nature of this threat? Who or what is threatened, who by whom and why? What can be done about it or how can we limit the impact of terrorism and make sure that terrorists do not have their ways again? These are just a handful of questions that will be addressed in this study.

Other concerns include: i) the essence of terrorism as instrument to achieve certain goals, in addition to an exploration of this phenomenon and the difficulties in defining it. ii) overview of the state to counter terrorism, what theories assumptions and conventional wisdom has it produced that could be of help in dealing with terrorism? We shall find out in this work

The killing of innocent souls throughout the world, the chaos and destruction of lives and properties brought about by terrorist stand as the motivation to this study. It will help us to protect the state and its inhabitants, safeguard the quality living standard by means of security mechanism to avert every possible threat. The relevance of this study is to show the various means of fighting terrorism. This work exposes the works of terrorist such as their methods, practices and how to stop them. Terrorism has been a great problem to the world at large but with the help of this work we will overcome their threats, expose their practices and also discuss how to fight them.

2.0 LITERATURE REVIEW

2.1 Terrorism and Social Terrorism

Terrorism in its broadest sense is the use of intentionally indiscriminate violence as a means to create terror or fear in order to achieve a political, religious or ideological aim (Fotna, 2015). It is used in this regard primarily to refer to violence against civilians or non combatants. Although the term has been in use since the 1970's, it initially became popular when journalists and politicians publicly introduced and started using the term "Islamic terrorists". The term has often been used politically as a term of abuse or denunciation both by insurgents groups and by government against each other (Winsnewski, 2008).

Broad categories of political organizations have been claimed to have been involved in terrorism in order to further their objectives including right using and left using political organizations, nationalist groups, religious groups, revolutionaries and ruling governments, the symbolism of terrorism has been to exploit human fear to help them achieve these goals. Terrorism related legislation has been adopted in various western states (Ruby, 2002).

The definition of terrorism has proven controversial, various legal systems and government agencies use different definitions of terrorism in their national legislations. Moreover, the International community has been slow to formulate a universally agreed legally bonding definition of this come. These difficulties arise from the fact that the term "terrorism" is politically and emotionally charged (Hoffman, 1998).

2.1.1 History of terrorism

Terrorism comes from the French word "Terrorisme" (Shariat 2015) and originally referred specifically to state terrorism as practiced by the French government during the 1793 – 1794 reign of terror. The French word terrorisme in turn derives from the latin verb "Terrere" meaning "To frighten" (Kim 2001). The Jacobins coming to power in France 1792 are said to have initiated the reign of terror, after the Jacobins lost power, the word terrorist became a term of abuse. The first half of the 20th century saw two events that influenced the nature of conflict to the present day. The effects of two World Wars inflamed passions and hopes of nationalists throughout the world, and severely damaged the legitimacy of the international order and government. The age of modern terrorism might be said to have begun in 1968 when the Popular Front for the Liberation of Palestine (PFLP) hijacked an El Al airliner en route from Tel Aviv to Rome. While hijackings of airliners had occurred before, this was the first time that the nationality of the carrier (Israeli) and its symbolic value was a specific operational aim. Also a first was the deliberate use of the passengers as hostages for demands made publicly against the Israeli government. The combination of these unique events, added to the international scope of the operation, gained significant media attention. The founder of PFLP, Dr. George Habash observed that the level of coverage was tremendously greater than battles with Israeli soldiers in their previous area of operations. "At least the world is talking about us now." (Stevenson 2010)

Another aspect of this internationalization is the cooperation between extremist organizations in conducting terrorist operations. Cooperative training between Palestinian groups and European radicals started as early as 1970, and joint operations between the PFLP and the Japanese Red Army (JRA) began in 1974. Since then international terrorist cooperation in training, operations, and support has continued to grow, and continues to this day. Motives range from the ideological, such as the 1980s alliance of the Western European Marxist-oriented groups, to financial, as when the IRA exported its expertise in bomb making as far afield as Colombia (Stevenson 2010)

2.1.2 Current State of Terrorism

The largest act of international terrorism occurred on September 11, 2001 in a set of co-ordinated attacks on the United States of America, where Islamic terrorists hijacked civilian airliners and used them to attack the World Trade Centre (WTC) towers in New York City and the Pentagon in Washington, DC. The effects of 9/11 had a significant impact on the American psyche and led to global reverberations. Other major terrorist attacks have also occurred in New Delhi (Indian Parliament attacked); Bali car bomb attack; London subway bombings; Madrid train station bombings; attacks in Mumbai (hotels, train station and a Jewish outreach centre), Nigeria, Pakistan, Paris, and more. The operational and strategic epicenter of Islamic terrorism is mostly centered in Pakistan, Afghanistan and parts of Syria.

The Boko Haram terrorist attacks in the North East Nigeria, Chad and Repoblic of Benin has brought terrorism closer to us in this part of the world.

2.1.3 Types of terrorism

1. Civil Disorder: This is a form of collection violence interfering with the peace, security and normal functioning of the community.
2. Political terrorism: violent criminal behavior designed to generate fear in the community or substantial segment of it for political purposes.
3. Non-political Terrorism: Terrorism that is not aimed at political purposes but which exhibits conscious design to create and maintain a high degree of fear for coercive purposes but the end is individual or collective gain rather than achievement of a political objective.
4. Quasi terrorism: It is not the main purpose of the quasi terrorist to induce terror in the immediate victim as in the case of genuine terrorist, but the quasi terrorist uses the modalities and techniques of the genuine terrorist and produces similar consequences and reactions. For example, the gang that takes hostages is a quasi terrorist whose method are similar to those of the other terrorist but whose purposes are different.
5. Official or state Terrorism: This refers to a nation whose rule is based upon fear and oppression that reach similar to terrorism or such proportions.
6. Religious terrorism: The validity and scope of religious terrorism is limited to an individual’s view or to a groups view or interpretations of that beliefs system teachings. Most terrorist act throughout history have been performed on religious ground with the goal to either spread or enforce a system of belief. (Hudson and Schneider 2002)

2.1.5 Social Terrorism

Social terrorism is a process of organized physical and mental violence directly against the citizen, society and the state which aims to enforce a different religious or political ideology (Abraham 2008).

Terrorist organizations intend to build permanent alliances with local criminal structures with antisocial individuals or with underage persons and through them in future commit not just assassinations but also spread their brutal propaganda throughout the world (Hudson 2002). Brutal propaganda is one of the most effective militant instrument of terrorist organizations attempting to seek revenge and intentionally turn hatred against all western aggressions who have stirred up civil war on their territory, took lives of hundreds of thousands of people, force millions into poverty and to leave their home and country.

2.1.6 Causes of Social Terrorism

The following among other things are the causes of social terrorism.

1. Ethnic, religions or political ideology
2. Social injustice, hunger or poverty
3. Desperation, helplessness or hopelessness
4. Social rift, social disharmony
5. Humiliation, slander or defamation of character
6. intent aggression, perverse behavior etc

2.1.7 The Intent of Terrorist Groups

A terrorist group according to Williams (2008) commits acts of violence for the following reasons among others. -

i. Produce widespread fear
ii. Obtain worldwide, national, or local recognition for their cause by attracting the attention of the media
iii. Harass, weaken, or embarrass government security forces so that the government overreacts and appears repressive
iv. Steal or extort money and equipment, especially weapons and ammunition vital to the operation of their group
v. Destroy facilities or disrupt lines of communication in order to create doubt that the government can provide for and protect its citizens
vi. Discourage foreign investments, tourism, or assistance programs that can affect the target country’s economy and support of the government in power
vii. Influence government decisions, legislation, or other critical decisions
viii. Free prisoners
ix. Satisfy vengeance
x. Turn the tide in a guerrilla war by forcing government security forces to concentrate their efforts in urban areas. This allows the terrorist group to establish itself among the local populace in rural areas.

2.1.8 Types of Terrorist Incidents

The most common types of *terrorist incidents* include:

i. **Bombing:** this is the most common type of terrorist act where typically inexpensive and easy to make improvised explosive devices (IEDs) are used to construct bombs. Modern IEDs are smaller and are sometimes difficult to detect. They sometimes use common, non-military components for the production of the IEDs. Terrorists can also use materials that are readily available to the average consumer to construct a bomb (Robert 2003).

ii. **Kidnapping and Hostage taking**: Terrorists use kidnapping and hostage taking to establish a bargaining position and to elicit publicity. Kidnapping is one of the most difficult acts for a terrorist group to accomplish, but, if a kidnapping is successful, it can gain terrorists money, release of jailed comrades, and publicity for an extended period. Hostage taking involves the seizure of a facility or location and the taking of hostages. Unlike a kidnapping, hostage taking provokes a confrontation with authorities. It forces authorities to either make dramatic decisions or to comply with the terrorist's demands. It is overt and designed to attract and hold media attention. The terrorist's intended target is the audience affected by the hostage's confinement, not the hostage.(Robert 2003)

iii. **Armed Attacks and Assassinations**: Armed attacks include raids and ambushes. Assassinations are the killing of a selected victim usually by bombings or small arms. Drive by shootings is a common technique employed by unsophisticated or loosely organized terrorist groups. Historically, terrorists have assassinated specific individuals for psychological effect (Snyder 2009).

iv. **Arson and Fire Bombing**: Arson and fire bombings are easily conducted by terrorist groups without a sophisticated equipment and well organized, equipped, or trained terrorist organization. An arson or fire bombing against a utility, hotel, government building, or industrial centre portrays an image that the ruling government is incapable of maintaining order (Robert 2003).

v. **Hijackings and Skyjackings**: Hijacking is the seizure by force of a surface vehicle, its passengers or its cargo. Skyjacking is the taking of an aircraft, which creates a mobile, hostage barricade situation. It provides terrorists with hostages from many nations and draws heavy media attention. Skyjacking also provides mobility for the terrorists to relocate the aircraft to a country that supports their cause and provides them with a human shield, making retaliation difficult (Abraham 2008).

vi. **Nuclear / Radiological / Biological / Chemical terrorist attacks**: Historically, terrorist attacks using nuclear, biological, and chemical (NBC) weapons have been rare. Due the extremely high number of casualties that NBC weapons produce, they are also referred to as weapons of mass destruction (WMD). However, a number of nations are involved in arms races with neighboring countries because they view the development of WMD as a key deterrent of attack by hostile neighbors. The increased development of WMD also increases the potential for terrorist groups to gain access to WMD. It is believed that in the future terrorists will have greater access to WMD because unstable nations or states may fail to safeguard their stockpiles of WMD from accidental losses, illicit sales, or outright theft or seizure. Determined terrorist groups can also gain access to WMD through covert independent research efforts or by hiring technically skilled professionals to construct the WMD. Though not technically weapons of mass destruction, but terrorists could also use non-weapons grade radioactive nuclear material (like that from medical use or waste from energy production) to create a "dirty bomb" which, though not destructive on a nuclear scale would render the impacted areas uninhabitable due to radiation (Snyder, 2009).

2.1.9 Some Systems at risk of Terrorism

The following are some systems that terrorist groups set as their prime target.

i. **Computers and electronic systems:** Currently, most electric devices such as computers, laptops and cellphones are prone to terrorist attacks because they usually connect to other devices in network.

ii. **Financial system:** Websites and applications that accept or store credit card numbers, brokerage accounts and bank accounts information are prominent hacking targets because of the potential for immediate financial gain. These gains can be from transferring money making purchases or selling the information on the black market (Chariad, 2013).

iii. **Utilities and industrial equipment:** Computers control functions at many utilities including cordination of tele-communications equipment, the power grid, nuclear power plants and valve opening and closing in water and gas networks. The internet is a potential attack vector for such machines if connected (Pagliery, 2015).

iv. **Aviation:** The aviation industry relies so much on a series of complex systems mostly controlled by wireless transmission. A simple power outage in an airport can cause a problem with ripple effects worldwide how much more a radio transmission equipment that controls aircraft over seas and oceans. Attack is especially dangerous because radar surveillance only extends 175 to 225 miles offshore. There is also potential for attack within an aircraft (Jin 2014).

v. **Large corporations:** Large corporations are common targets, in many cases this is aimed at a financial gain through identity theft and involves data breaches. Medical records have been targeted for use in general identity theft, health insurance fraud and impersonating patients to obtain prescription drugs for recreational purposes or resale (Melvin, 2014).

vi. **Automobiles:** If access is gained to a car’s internal control area network, it is possible to disable the brakes and turn the steering wheel, computerized engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced diver assistance system.. Cyber security of automobiles does not just involve the production but also the discovery and patching of vulnerabilities (Kang, 2016).

vii. **Governments:** Government and military computer systems are commonly attacked by activists and terrorists, local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personal records, and financial systems are also potential targets as they are now all largely computerized (Liptak, 2015). Passports and government identity cards that control access to big facilities can be valuable to cloning.

viii. **Medical Systems:** Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated. These include both hospital diagnostic equipment and implanted devices like pacemakers and insulin pumps. There are many reports of hospitals being burned and hacked, viruses and data breaches of sensitive data stored on hospital servers (Jeremy, 2012).

2.2 Cyber Security

Cyber security refers to the body of technologies, processes and practices designed to protect networks, devices, programs and data from attacks, damages or unauthorized access, cyber security may also be referred to as information technology security (Angus, 2002). Unlike the automobile industry, the technology industry is struggling to protect itself from people and organization trying to access information to data and intellectual rights using vandalism or theft (Timothy 2016).

2.2.1 Types of Cyber Security

The two major types of cyber security are:

i. Software security: This consists of server protection and security systems from viruses and other malicious software programs and data security through theft prevention and safe computer practices, it refers to ways in which attacks can be launched on data streams and software without any physical interaction of different devices or hardware.

ii. Hardware security: This Refers to practices regarding how physical devices and computer hardware are handled and overseen. The physical servers, mainframes that often house various networks and internet websites can be damaged resulting in loss of data or they could be physically attacked in an effort to steal information directly from the system through data transfer between the devices (Baker 2016).

2.2.2 Elements of Cyber security

The Elements of Cyber security as listed by Sageman (2004) include:

i. **Application security:** Application security embraces steps taken through an information application's life cycle to thwart any attempts to transgress the authorization limits set by the security policies of the underlying systems. The security protocols set the right exceptions in the systems that are inherently flawed owing to design, development and deployment, upgrades or maintenance. The applications are only concerned with controlling the utilization of resources given to them.

ii. **Information security**: Involves safeguarding sensitive information from illegitimate access usage, disruption, alteration, reading, inspection, damage or recording. This is an assurance that critical data is not lost when any issues like natural disasters, malfunction of system, theft or other potentially damaging situation arises.

iii. **Network security**: This refers to comprehensive security policies and provisions adopted in an adaptive or proactive manner by the network administrator for preventing and monitoring unauthorized access, deliberate misuse, alteration, denial of service for a computer host and other network accessible interaction related sources. It involves checking the priviledges and rights of users to validate the legitimacy of users and grant them access to networks data or allow for exchange of information.

2.2.3 The Importance of Cyber Security

Cyber security is important because government, military, corporate financial and medical organizations collect, process and store a large amount of data on computers and other devices. A significant portion of these data can be sensitive information like intellectual property, financial data, personal information or other types of data for which unauthorized access could have grievious negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing business. Cyber security describes the discipline dedicated to protecting the information and the systems used to process, store and transmit them. As the volume and sophistication of terrorism grows, companies and organizations especially those trusted with safeguarding information relating to national security, wealth or financial records needs to take steps to protect their sensitive business and personnel information (Peter, 2003). This fact makes cyber security very important.

2.2.4 Typical Cyber Security Job Title and Descriptions.

Cyber security is a sensitive career that involves a lot of personnels. Below are some of the job titles involved in cyber security.

i. **Security analyst:** Analyzes and assesses vulnerabilities in the infrastructure, investigates using available tools and counter measures to remedy the detected vulnerabilities and recommends solutions and best practices, examines available recovery tools and processes and recommend solutions. Test for compliance with security policies and procedures. May assist in the creation, implementation or management of security solutions.

ii. **Security engineer:** Performs security monitoring, security data or log analysis and forensic analysis to detect security incidents and mounts the incident response. Investigates and utilizes new technologies and process to enhance security capabilities and implement improvement, may also review code or perform other security engineering methodologies.

iii. **Security architect:** Designs a security system or major components of a security and may head a security design team building a new security system.

iv. **Security administration:** Installs and manages organization wide security systems, may also take on some of the tasks of a security analyst in smaller organizations.

v. **Information security officer (CISO):** A high level management position responsible for the entire information security division. The position may include hands-on technical work.

3.0 DISCUSSION

The threat of terrorism has made the world to devote a lot of resources to security. In this era of information revolution, it is obvious that terrorists can attack anything, anywhere, and at anytime. No country has the resources to protect everything, everywhere, and at everytime for that reason, there will always be vulnerabilities. Physical security measures cost a lot and most times their effectiveness is hard to measure.

Terrorists usually create fear and tension in the heart of the populace before their actual attack. To respond well to terrorist attacks, they should be careful measures to reduce public alarm and panic among the populace. This can be achieved by putting in place a crisis management structures and procedures. Counter measures should be put in place to negate their negative propaganda as well. Faceless social media users should be monitored closely in every country in order to track down malicious communications.

There are actually no hard and fast rules that will prevent terrorism all the time but with cyber security techniques, information can be secured as people communicate over the cyberspace. The following are some of the ways to secure information;

i. Secure systems with hardware and software protection: Install intrusion detection systems and respond immediately to any intrusion, as recommended by the computer emergency response team which deal with computer threats.

ii. Governments should affiliate with defensive organizations to track threats. Use the military as a resource to keep up with threats and defense mechanisms, make sure your system or network is secured with a strong password and effective firewall, install antivirus systems, keep them updated and run checks regularly to detect and remove any problems.

iii. Create a firm security policy: Train employees to guard against such things as opening email attachments or responding to messages from unknown sources. Institute and apply regular filters to screen out suspicious material or messages from known sources of threats such as specific countries.

iv. Test your defenses regularly: Employ a testing or security service to routinely invade your network and have it report any deficiencies. Change a system or network when a vulnerability is identified.

v. Install surveillance camera in public places (CCTV): It’s clear that surveillance plays a key role in fighting crime and protecting public places.

While on the cyber space, you can apply the following strategies. These include:

i. Use strong password, long in length and combination of alphabets, numbers and special characters.
ii. Use different password for different websites and if needed, consider using a password manager.
iii. Update your system when patches are released and vulnerability discovered.
iv. Use more secure operating systems.
v. Secure your personal network using firewalls.
vi. Do not install untrusted software on your computers.
vii. Test your personal network for vulnerabilities.
viii. Secure your data by using strong encryption where possible.

Terrorism has been associated with physical acts of violence and crime like killings, kidnapping, destruction of lives and property etc. but starting from the twentieth century the increasing number of technology and systems controlled by computer has brought a new form of criminal activity - Cyber terrorism. Cyber terrorism can be carried out by individuals, terrorist groups etc. Cyber terrorist can be prevented through different means of cyber security techniques. Most targets of cyber terrorists are large organizations, governments, utilities, infrastructure, businesses, financial institutions etc.

4.0 CONCLUSION

In this study, we have been able to show what terrorism is all about, the different types, history and ways to fight them which involves the use of cyber security techniques. We shall stop terrorists through relentless action by implementing the various techniques listed in this study as fast as possible.

In waging this war against social terrorism we will be equally resolute in maintaining our commitment to our ultimate objective. The defeat of terror is a worthy and necessary goal in its own right. We shall not only forge a powerful coalition to combat terrorism today but work with experts to build a lasting and powerful mechanism for combating social terrorism. Cyber security techniques are the best remedy to stop the spread of social terrorism and a world without terror is the world we must build today. Therefore we have to adoped these cyber security techniques in order to make the world a better place to live.

5.0 REFERENCES

Abraham M. (2008); What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy, *International Security Volume 32, Issue 4, Spring 2008 p.78-105* .

Angus Martyn (2002): The Right of Self-Defence under International Law—the Response to the Terrorist Attacks of 11 September online at https://www.aph.gov.au/binaries/library/pubs/cib/2001-02/02cib08.pdf

Fortna, V. (2015). Do Terrorists Win? Rebels' Use of Terrorism and Civil War Outcomes. *International Organization, 69*(3), 519-556. doi:10.1017/S0020818315000089

Gérard Chaliand, Arnaud Blin (2007): The History of Terrorism: From Antiquity to Al-Qaeda, online at https://www.jstor.org/stable/23616152

Hoffman B. (1998): Inside Terrorism New york times on the web online at https://archive.nytimes.com/www.nytimes.com/books/first/h/hoffman-terrorism.html?_r=2

Hudson R. A. (1999): The Sociology and Psychology of Terrorism: Who Becomes A Terrorist and Why? Online at https://www.loc.gov/rr/frd/pdf-files/Soc_Psych_of_Terrorism.pdf

Jeremy Kirk (2012): Pacemaker hack can deliver deadly 830-volt jolt. Online at https://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html

Jim Finkle (2014): Cyber attacks more of a threat to healthcare than financial sectors – FBI. Online at https://www.biznews.com/health/2014/04/24/cyber-attacks-threat-healthcare-financial-sectors-fbi/

Kang Cecila (2016): Self-Driving Cars Gain Powerful Ally: The Government. Online at https://www.nytimes.com/2016/09/20/technology/self-driving-cars-guidelines.html

Kim Campbell (2001): When is 'terrorist' a subjective term? The Christian Science Monitor. Online at https://www.csmonitor.com/2001/0927/p16s2-wogi.html

Pape, R. (2003). The Strategic Logic of Suicide Terrorism. *American Political Science Review, 97*(3), 343-361. doi:10.1017/S000305540300073X

Peter I. Rose (2003): Disciples of religious terrorism share one faith. *The christian Science Monitor online at https://www.csmonitor.com/2003/0828/p15s02-bogn.html/(page)/2*

Ruby, C. L. *(*2002*)*. The definition of terrorism*. Analyses of Social Issues and Public* Policy (ASAP), 2(1), 9-14. Online at http://dx.doi.org/10.1111/j.1530-2415.2002.00021.x.

Stevenson A. (2010): Oxford Dictionary of English (3 ed.), online at http://www.oxfordreference.com/view/10.1093/acref/9780199571123.001.0001/acref-9780199571123

Timothy Snyder (2010): A Fascist Hero in Democratic Kiev; American Review of Books, online at http://www.nybooks.com/daily/2010/02/24/a-fascist-hero-in-democratic-kiev/

Williams P. (2008): Violent non-state actors and national and international security; international relations and security network online at https://www.files.ethz.ch/isn/93880/VNSAs.pdf

Winsnewski J. J. (2008): Torture, Terrorism, and the Use of Violence Review Journal of Political Philosophy Volume 6, Part 1 online at http://www.cambridgescholars.com/download/sample/61270.pdf