

INTERNATIONAL CYBER TERRORISM: A GLOBAL APOCALYPTIC ‘TIME-BOMB’

Prof. Anthony Afe Asekhauno, Ph.D

*Department of Philosophy
University of Benin, Nigeria*

And

Theophilus Arebamen Okojie, Ph.D

*Department of Political Science
Faculty of Social Sciences
University of Benin, Nigeria*

Abstract

Given the devastation of the two World Wars, the reluctance of world powers to fashion the part of peace against that which ignited those wars, another World War could be imminent, and such could be cyber-base or cyber-ignited. Given that man did not institute violence, but as a subsistent agent, humanity was replete with interpersonal rivalry; and as a social actor man has been enmeshed in the gauge of tensions, conflations, confrontations and wars—each platform advances over the other in intensity and complexity, in scope and devastation. Apparently and even though the intensity of ideological (including religious) rivalry has never waned, the strategies deployed have become scintillating, provocative, sharper, more precise and exact—with further devolution and progress in internet/cyber technology, which though has introduced better modes in communication and transportation; effectiveness and efficiency. Nevertheless, this technology has become handy for malevolence. Thus, adopting some phenomenological and analytical tool to review existing theoretical amid evident factual material, this work espouses need for cyber-technology and discovers that its abuse (criminality and terrorism) is fast outweighing its relevance in the necessity for posterity of humanity. It thus concludes that, given its trajectory and unless reversed, a third world war would be largely cyberwarfare and annihilating. It however recommends restraint and caution on the part of international actors both on adversarial missions and the development/deployment of cyber-intelligence.

Keyterms: Apocalypse, law/international law, politics, terrorism/cyber terrorism, time-bomb.

Introduction and Background to the Study

Recent human history indicates that cyber-terrorism and its threat has almost wholly surpassed “direct” military combat in application of violence in contemporary world affairs. In *how philosophy caused the First World War and beyond*, Asekhauno (2017) points out, *inter alia*, that

...From Galilean world view, Newtonian physics, to Wright Brothers airplane; and from the computer, atomic/nuclear/oxygen bomb, to the boundless social media of the contemporary, the world (by its own product (philosophy) has had untold progress..., with its devastating evil other-side—the acme of which is a highly technologically united world that can be extinguished in few minutes...; the much blood *has* flowed in every parts of the world as a result of the tensions *arising from* incompatible philosophical ideologies and the men and women who espoused them, culminating in a polarized world and the World Wars and others around the world.

Apt and truly beyond those wars described, others are ranging, and yet others more well threatened in present century heightened in the midst of adversary ideologies, nations are primarily committed to development and possession weapons of mass annihilation.

Since those Wars down to the late sixties and now into the 21st century, the world press has been carrying more and more and more of startling news about airline hijacked, embassies blown up or set on fire, diplomats kidnapped, acts of provocation and upright raids staged against government and non-governmental missions, plastic parcel-bombs going off amid other variety. Here are some of the most sensational episodes of such based on (an example each) whether individual, local, organizational, or state terror—with two of the most intense episodes in the decade.

(i) *The 1960s and 1970s* The decades of this period marked untold era of terrorism. For instance, on December 3, 1969, a group of 40 Zionists raided the Syrian Delegation headquarters at the UN. On March 3 1971, a petrol bottle was thrown into the Iraqi Mission at the UN. On October 20, a member of the Zionist Jewish Defense League shot with a large-bore rifle at the headquarters of the Soviet Delegation at the UN from the roof of an adjacent house in New York. He fired at the window of a room with four children at the moment. However, official government representative were not the only target of terrorism.

Late in 1972, the Scotland Yard had to introduce special control at the London post office for the first time since World War II because of a spate of plastic bombs, posted as letters or parcels. In October 1977, the Japanese

International Cyber Terrorism: A Global Apocalyptic 'Time-Bomb'

Government had to meet the demand of terrorist from the Japanese Sekigun organization who had seized a JAL airliner with passengers on board, bound for Paris from Tokyo. The terrorist demanded a ransom of 6 Million Dollars and the release of their former nine associates from Japanese jails. They threatened to kill off the passengers and their crew if their demand was not met. This terrorism is practiced not merely by gangs of killers, but by the state machinery by some countries around the world.

We could cite more of such examples but those and similar episodes were just the beginnings of worse ahead. However, half of all the acts of terrorism committed in the 1970s occurred in Europe, 21 percent in Latin America, 14% in North America and 11 percent in the Middle East and North Africa. In 1970, there were twice as many terrorist acts in Latin America as in Europe. In 1978, they were in reversed proportion. Direct damage caused by terrorist action and overhead expenses they involved, as those for security and insurance in 1970-1978 ran into billions of dollars (Blishchenko&Zhdanov 1984). Remarkably, those initial forms of terrorism were largely pockets of individual, internal/local, organizational, or state sponsored.

(ii) *The 1980s and 1990s* marked more terrorist activities than the previous decades. More presidents/national leaders were killed and governments toppled (for instance, Samora Michel of Mozambique, and Thomas Sankara of Burkina Faso); espionage activity heightened leading to the disintegration/dissolution of the USSR and emergence of many independent states from the former Union, and to the re-unification of Germany. Yet individual, local, organizational, or state also thrived.

(iii) *The 21st Century* If the World Wars of the 20th represented conventional confrontations among nations, the emergent terrorism represent sharp turn in the nature of organized international violence before its close of the century. And the 21st century perfects and marks the acme of international terrorism—individual, organizational, and state sponsored. As I sit here in the ancient city of Benin, Nigeria, facing the Cable breaking news item on the brutal assassination in his home of the Haitian President—with internal, state, international in planning, financing or personnel?

Whether national or international, terrorism endangers or takes (innocent) human lives, jeopardizes human rights and fundamental freedoms, irrespective of ideological plane and place. The risk remains hypothetical but the antagonist has degenerated from hostile states to include extremist groups like Al Qaeda and Taliban (with headquarters in Pakistan and Afghanistan respectively); ISIS (with

headquarters in Syria/Iraq); then Boko-Haram and Ipwap (with headquarters in Nigeria and Mali respectively). Al Qaeda wrecked physical havoc on New York on September 11, 2001(9/11), and Isis on American Libyan Embassy in 2012; Malaysian Airliner has been missing for nearly a decade; there have been Shootings, kidnappings, and other attacks some declared or undeclared reasons—to mention a few.

Hence, today, the world has become more terrified and hellish as never. From the atomic bomb on Hiroshima and Nagasaki (marking the end of the second world war), to the reality of the highly volatile remote-controllable nuclear weapon, another but emergent major threat to world/human existence is the accessibility of this ignition to the internet—a ploy which has become fashionable to adversary individuals, organizations, and states to herald their political interests or deploy for their terrorist activity.

What Terrorism is

Terrorism is not war; yet it may have its features and may lead to actual war. Terrorism is usually goal-directed at some target—persons, property, or institutions. Terrorism inflicts terror and violence. State versus tribe war, of secessionism is termed rebellion. Terrorism could ignite shock, neurosis and trauma amid other a kinds of psychological violence. Terrorism is aggression—the energetic activity of the mind or body, by proper assertion of forceful act or morbidly expressed in bullying, masochism, destructiveness (Watson 1978/84). It is a political tactic, policy of using acts inspiring terror, or great fear, as a method of ruling or of conducting political opposition. The state as well as the individual can terrorize; it is an aspect of violence (Blishchenko & Zhdanov 1984).

Whether by individuals or as groups, ‘terrorism’ is usually planned violence targeted at the state. Popular view holds that to be violent is to be furious, which tends to pervert the eclectic meaning. Violence means to ‘violate’—the intention is to inflict injury or damage on the bearer. It is the violation of the rights, physique and/or property of others or another. Sometimes, it could be inflicted on the self or against nature. Ordinarily, the idea of ‘violence’ is equated with the use of force. Thus, terrorism could violate persons (even kill them) or principles, nature things, or objects, by either inflicting bodily harm or infringe on their rights or freedom. Sometimes, it could be inflicted on the self or against nature. Terrorism is politically/ideologically motivated violence.

Let us proceed by specifying the concept and definition and act of terrorism. The term, terrorism and ‘an act of terror’ are ad derivative of the term

International Cyber Terrorism: A Global Apocalyptic 'Time-Bomb'

terror—which has a Latin root but has become widespread in world discourse. Its use and spread followed the description of the deleteriousness that followed public executions in especially post-revolution France of late 1880s; and, similarly for that latent consequence, the ecclesiastic authorities required popular attendance at scenes of executions (Blishchenko&Zhdanov 1984). At those points, terror was already state official policy, perhaps as deterrent. On the other hand, individual terrorism is action capable of breeding social danger, great loss of life and property. Both represent an encroachment designed with a view to violent destruction of all or aspects of political and legal/administrative organizations of society. Such informed the ideological spar between the east and west in the course of the decades culminating in the establishment of the UN as arbiter. Still later, hijackers, guerrillas, and mercenaries followed. In this way, acts of terrorism can be committed by combatants in the context of international or national conflict. Terrorism could involve in liberation struggles. Thus there could be war terror, repressive error, revolutionary terror, and sub-revolutionary terror (Wilkinson 1973,293-308). It might be a faulty weapon which could misfire, for accomplishing different objectives. Alexander et al (1979) defines terrorism as “the threat or actual use of force or violence to attain a political goal through fear, coercion, or intimidation.” In all, terrorist elements include the decision, the threat or use, and the effect of violence plus international (UN) opinion on it as such—implying no specific definition of it. Yet a difference exists between struggle and violence against domestic autocracy, foreign conquerors exterminating a people, and domestic institutions. According to Felix Gross (1969, 422/432), terrorism could be tactical (retributive and damaging to government), random-focused, mass terror, or dynastic assassination.

Terrorism could occur in times of war as well as times of peace. In the latter sense, terrorism comes “within the framework of *jus in bello* and denotes the practices which appear to be uselessly cruel or odious, and are eventually interpreted as war crimes...or infringements of humanitarian law; but in peacetime, terrorism is goal-directed action against some target state” (Blishchenko&Zhdanov, 27).

Terrorist spans a wide ranging scale, traversing age gender—with ideological trend (religious and political) most common. By and large, we could define terrorism as “the product of fanatical violence perpetuated generally in order to realize some political end to which all humanitarian or ethical beliefs are sacrificed” (Wilkinson 1973, 292). Terror certainly is a method of violence; terrorism is the application of such method through individual terrorist act. Accordingly, Brian M. Jenkins wrote,

Terrorism appeared to have increased markedly in the past few years. Political and criminal extremist in various part of the world have attacked passengers in airline terminals and railway station; planted bombs in government building. The office of the multinational corporations, pubs, and theatres; he jacked airliners and ships, even ferryboat in Singapore; held hundreds of passengers hostage; seized embassies; and kidnapped government officials, diplomats, and business executives. We read of new incidents almost daily...terrorism has become a new element in international relations (1975, 13).

There have been certain instances of international law breaking been mixed up with terrorism, which objectively hampers a concentrated effort to check this type of international crime; a case in point is the work of Louis Rene Beres, *Terrorism and Global Security*(1979). He articulates the nuclear threats which accompany the possession of the nuclear arms and the eventuality of their being used for acts of terrorism. Because of the divergence positions of various states with regard to terrorism and the loose wording of item 92 of the agenda, neither the twenty seventh, nor the subsequent twenty-eighth session of the UN General Assembly could work out any specific measures to check acts of terrorism jeopardizing the normal course of international relations.

Generally, terrorist acts could be understood and classified based on two broad general motivating criteria: one whether the act is individual, organizational or state; and two, whether the act is internal/local (insurrection) or international (ideological and political). From these two general categories, we could isolate the following five typology of terrorism: (1) Individual-state; (2) organizational-state; (3) individual international; (4) organizational-international; and (5) state-state. Let us describe these trends or forms along some sensational examples of each episode seriatim.

Individual-State Terrorism is a necessity by one individual or group which discerns despair and political doom for political struggle against existing system. This common trend is usually internal to a state. But individual political terrorism is conscious struggle against a government; yet individual terrorist acts may be genuine politico-ideological struggle but mostly inexpedient and therefore reject-able.

Organizational-State Terrorism is usually the leftist terrorism which often turns out to be a specific manifestation of protest against racism, colonialism/political domination, foreign occupation, poverty, and despair. It could degenerate to revolution, as were the Arab Springs of 2011 and beyond. This trend mostly cuts across ideological divides, but depending on the perception of the organization, targets may extend to the international as was the

attack on the US Embassy in Benghazi, Libya 2012 by members of the Islamic militant group, Ansar al Sharia. This also occurs where a state is a victim in its own territory of subversive and/or terrorist acts by irregular, volunteer, or armed bandits.

Individual International Terrorism involves a wide range of instances essentially unconnected with any state whatsoever. What can be said to be connection of state with this strength place of planning of the act like individual national terrorism. This can be study reacting terror inform of violence antagonism in a foreign land however most time the planning execution is done in stage by a foreign national who must have come to residence in guise of either tourist, education/research or asylum.

Organizational-International Terrorism is the terror of the class in power; terror of the class struggling for power; or revolutionary-terror and counter-terror. Whether international or against the state, individual terrorism appears as intellectuals perceive the necessity of struggle against perceived or real undesirable system.

State-State Terrorism obtains where there is a commission of acts of terrorism against a State b groups formed of servicemen of another State, whether directly undertaking, tolerating or encouraging such also count as aggression. Attacking causing injury and death to civilian population of opponent State is a case in point as different from similar acts by a citizen but not representing the will of his State which must but bring such culprit to book to establish its goodwill against the act and its *corpus delicti* (circumstances and body of the crime). The premise of cyber terrorism is that as nations and critical infrastructure became more dependent on computer networks for their operation, new vulnerabilities are created: "a massive electronic Achilles' heel." A hostile nation or group could exploit these vulnerabilities to penetrate a poorly secured computer network and disrupt or even shut down critical functions (Lewis 2002). Before the 21st century, a rival nation would sponsor individual/agency spying on the technology and developments of some other country (or its aligning one); today, cyber-espionage and systematic cyber-sabotage has almost wholly but dangerously taking-over that tact. And the more industrial/technological nations are both the likely attackers and more vulnerable to attacks.

An act of terrorism is to draw attention to a particular political cause or situation, though the objective may be longer term—raising money to enhance political struggle, obtaining the release of political prisoners, spreading general terror, removing/replacing a 'strong political personality', or even to provoke reprisals

and aggression. These could raise international tensions; exacerbate existing armed conflicts and strike at enduring political and social structures/development. The typical features of an act of terrorism include: violent action capable of attracting the attention of the general public; a political motive underlying the commission of a terrorist act, plus the fact that the act itself targets person(s) or a group or state or representatives of their interests; absence of reliable alternative(s) to achieve such goals. The underling goal is to intimidate and compel some source to fulfil the objectives and demands underlying the commission of the terrorist act(s). According to Karpets (1979, 98), terrorism is usually "...organized to commit murder, use violence, take people hostage for ransom or other demands, and forcibly deprive freedom, to inflict torture and blackmail. By and large, the eminent trends of terrorism include 'right-wing' (using as its theoretical foundation the ideological divide—aimed on either ends against communist/working-class movements and capitalist scheme of progress as in US forceful overthrow of 'obnoxious' regimes in Africa), and the inherently cruel 'organizational' (especially often founded on radical religious extremist/fundamentalist convictions directed against rival ones as in the activities of Al Qaeda and the Taliban)—where, the international law may be somewhat helpless.

Insecurity, Terrorism and International Law

Most texts on international law rarely discuss the subject beyond its nature, sources and actors; treaties, conventions and agreements; boundaries, rights and dispute resolution procedures. Although the issue of insecurity pops-up often, that of terrorism/cyber-terrorism seldom. Yet the verity of terrorism and especially cyber-terrorism (C-BT) is not only a current but typically torrent. International law, otherwise hitherto referred to as the 'law of nations', "refers to those rules and norms which regulate the conduct of states within the international sphere...relations of states...recognized" as such (Bazuaye and Enabulele 2006, 1). In fact the law regulates relations by international actors which include states, persons and organizations/agencies. Whether public or private, international law contains the principles, customs and standards of such relations (Williams & Menstra 1987, 1). Unlike municipal law, international law is founded on formal (those legal procedures and methods for creation of legally binding rules) and material (where the law may be found/applicable) sources. Most vividly, the statutes of the ICJ is the most authoritative statement on the sources of International Law—international conventions/customs, judicial decisions and general rules—without a specific hierarchy.

Yet, as custodians of the international law, the UN and the ICJ is committed to world security, stable society and peace—by security is meant “the freedom from all forms of encumbrances that can hinder man from satisfactorily meeting needs of life” (Olajide&Omoyibo 2017, 15); to a situation where man enjoys freedom and protection from attacks and dangers. Although each and all of those standards criminalizes all forms of unwarranted violence, there is no aspect of state or international custom which tolerates terrorism—which currently dominates acts of violence on national and the international stage; hence the astronomical rise in international terrorism and counter-terrorism. To wit, counter-terrorism is commonly reactionary, a reprisal effort to repay an earlier perceived or actual terrorist act. Sadly, international terrorism and cyber-terrorism has become typical feature of recent terrorism and the real problem of international relations, a new formidable challenge to law.

International law has set certain standards to measure whether an act is one of terror during wartime or peace time—for instance, the International Military Tribunal, several Articles of the various Geneva Conventions (1949) and the Hague Convention (1954) amongst others. Acts of terrorism could also be committed by authorities of a state against her citizens with a view to intimidating them or suppressing opposition or part of a policy of systemic discrimination on race, inequality and justice or outright acts of genocide (as was in Nazi Germany and apartheid South Africa). However, international law has appropriate provisions against such as in Article 6(c) of the International Military Tribunal, the UDHR (1948), and the various international Conventions: 1966 Covenant on Civil and Political Rights; International Convention on Non-Applicability of Statutes of Limitation to War Crimes and Crimes Against Humanity, 1968; and 1973 International Convention on the Suppression and Punishment of the Crime of Apartheid; and the 1937 Convention for the Prevention and Punishment of Terrorism; the 1970 Convention for the Suppression and Unlawful Interference with the Operation of Air Services, for instance.

Terrorism or the internationalization of terrorism as a phenomenon has engaged international relations for decades. While the terror wave is global, the major context is between the west and eastern ideologies, and among the major world powers—notably the US, Russia, and China, with Iran and North Korea as emerging cyber aggressors and conveners of newer alignments.

Cyber-terrorism: Its Nature, Typology and Threat

Section two identified the nature of terrorism. Accordingly, all the forms of terrorism described are of relevance here, especially cyber-base terror. Cyber-terrorism posits a new approach in international terrorism which thrives on the use internet; that is, the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. Cyber-terrorism is “the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.” Mark Pollitt (FBI 1997) defines cyber terrorism as: “The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents.”

There is no universally accepted definition of cyber terrorism, the lack of which is both an issue and a challenge in countering cyber-terrorism threats. Wyman 2005 (as cited in Gaines and Kappeler 2011) defines cyberterrorism as “The use of computer network tools to harm or shut down critical national infrastructures.” One type of cybercrime that would be devastating to our country would be a physical attack to our communications infrastructure. Our nation is not prepared to reconstruct the Internet from a massive disruption, nor do we have a coordinated comprehensive response to a significant breach in the Internet. Such breaches and disruptions could have significant, long-lasting, detrimental effects on our economy, defense and society in general.

Cyber terrorism includes the attacking of our cyber infrastructure, virtual information including hardware, software, data and information. Terrorist methods of attacks include physical or convention attack, primary aim is on an entire infrastructure; an electronic attack which is on a specific computer or server; and malicious code which is on a computer or network but can spread. Cyberterrorism is a cybercrime. However there are varieties of cybercrime—which are acts that are committed using in or by means of a virtual world; these include: 1. Hacking—using ‘code’ to deliberately gain unauthorized access; 2. Cyber warfare—an attack by a country on another’s central information network control; and cyber terrorism.

The premise of cyber terrorism is that as nations and critical infrastructure became more and more electronically developed—highly computer-base as against the earlier mechanistic tools (which were costlier). The electronic-based modes depend on cyber-networks and other wireless platforms. There are five main types of cyber terrorism attack which are incursion, destruction, and disinformation, denial of service and defacement of web sites. Some of these

International Cyber Terrorism: A Global Apocalyptic 'Time-Bomb'

attacks are more severe than the others and have different objectives. Their trend is wide-ranging, but as visible in religious concerns beyond Islamic fundamentalists.

To better understand why cyber-terrorism acts are committed, one needs to initially decipher cyber terrorism from motivational perspectives. Motivational forces behind cyber terrorism can be social, political, ideological, and economic. Emphasizing the transnational nature of cyber security issues, the last few years have seen the emergence of highly sophisticated criminal gangs capable of exploiting and defrauding vulnerabilities in finance and business networks, in politics and administration, and in morals, education and security, for instance. Taken more seriously, to cause terror in people's minds cyberterrorism must involve the realization of an indiscriminate attack "in" or "through" the cyberspace, with consequences in the outside world that are identified with deaths, serious injuries or other similar outcomes. In the beginning, it was mostly carried on by the atomic and nuclear powers. Yet the atomic bomb was delivered or deliverable via modes including fighter-jets, war ships and missiles. Recently pre-programmed drones proved more effective in the delivery of violence. Earlier, it carried on having to crisscross borders (to deliver bombs); today, detonations are remotely controlled hence distance is no longer a barrier; so, many digital Pearl Harbors, Hiroshimas and Nagasakis are possibilities and likely.

Cyber-terrorism uses computer network technology to expose those remote-control (automated) buttons to hackers and terrorists. State-sponsored cyber-terrorism does not just seek to destabilize and destroy computer networks, critical infrastructure and general progress in the target state/organization (as is the case of the alleged Russian interference in the 2020 US and other state elections), it inherently seeks to trigger cyber-aggression that one fears a possible cyber-based World War. Therefore, cyber-terrorism is a global time-bomb where in lies the feared apocalypse; cyber-warfare would require no mass-moving men (soldiers and snipers) and machines between distances; it is just that the control of one nation's (atomic, chemical, nuclear and other technological munitions or lines of communication) arsenal gets in the hands of an aggressor—using a nation's own technology of destruction to destroy it by superior technology; and with coronavirus pandemic ranging (for instance), such is the great but grave criminal conspiracy of humanity against itself and nature—imagine the virus was a result of hacking; it is a trajectory that needs to be reversed. And according to Lewis (2002),

Much of the early work on the 'cyber threat' depicted hackers, terrorists, foreign spies and criminal gangs who, by typing a few commands into a

computer, can take over or disrupt the critical infrastructure of entire nations. This frightening scenario is not supported by any evidence. Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations. Cyber-terrorism has attracted considerable attention, but to date, it has meant little more than propaganda, intelligence collection or the digital equivalent of graffiti, with groups defacing each other's websites. No critical infrastructures have been shut down by cyber-attacks.

As of now, it is trading of indictments; it soon chronicles the tendency to initially attribute cyber events to military or terrorist efforts when their actual source is civilian recreational hackers.

There are other ethical implications of terrorism on human persons. According to Ekei (2013), individuals, as well as cultures are different. It is therefore, morally evil to engage in war or in act of terrorism against any group based on such cultural and ideological differences. People are free, and must be free to exist and to live their lives freely in whatever manner they choose to live it. In religious terms, people should be allowed without molestation to live accordingly to their religious beliefs, provided they do not harm or hinder other people who do not share their belief-claims. Positively, the ethical implication arising from the dignity and irreplaceable nature of human person is simply, "*to live and let live*". This principle supposed to remain a clarion call of every meaningful religion, politics, economic engagements, ideological groups and camps etc. "to force or coerce people to live otherwise either by physical or psychological coercion is morally unjust and morally evil. Nothing is resolved by violence; on the contrary everything is placed in jeopardy", outside human freedom.

Again, Ekei (2013) stresses that there is a saying that violence instead of providing meaningful solution, begets violence. After violence there comes a counter violence. It must be reiterated that it is morally evil to kill or maim another person because of his not belonging to one's religion or religious group. God is at the center of every religion, and indeed, the creator of every human being; it will therefore be unthinkable for him to condone his creatures being killed by others with feigned human reasons and prejudices. There is no place, however, where God who is the object of every religion commands any one to kill another person on his behalf. It is, therefore, morally evil to terminate the lives that do not belong to one. Terrorism is, therefore, self-defeating, morally and terribly evil.

Again, throughout human history no meaningful democratic culture has ever thrived in an atmosphere of insecurity, intolerance, hatred, marginalization, brutality and bloodshed. In the traditional African society, murder and wanton destruction of human lives was always considered as the most heinous and abominable crime (*aru*) and will always remain so (Ekei 2013).

Conclusion and Recommendation

In modern world affairs, the history of terrorism has been closely tied-up with the history of violence—depending on its form and method vi-a-vis the necessitating factor(s). We have shown that Cyber-attacks, network security and information pose complex problems that reach into new areas for international security and public policy. This paper looked at one set of issues – those related to cyber-terrorism and cyber-attacks on critical infrastructure and their implications for international security. Cyberterrorism uses computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population. Then at its insipient stage it was nearly a sole machination by the US; today, it is internationalized and a common possession of almost every nation—its quality and deployment depending on the strength of the nation's technology.

It is a fact that the world has borne witness repeatedly too many such acts as blowing-up airliners, killing international political actors, and blowing-up government public departments. The wave of terrorism which sweeps across contemporary world generates throng of opinions, assumptions and prescriptions for suppressing it amid universal condemnation. A basic fact is that the development is a threat and destabilization not just to international relations but a greater one to the very existence of humanity and nature. Cyber-terrorism ups this potentiality, marking a deadlier approach in individual and state terrorism; killing thousands of (mostly innocent) people and destroying untold property. Cyber threat could simply be hacking or actual terror.

All terrorism has ill-implications for international relations—since there always is the source nation (the base of the inflictor considered as indirect aggression) and the target (existent in some other nation). Attacks involving embassies also could spark-off tensions between host nation and that having the embassy. We must consider the use of cyber-weapons beyond the context of whatever the political goals and motivations of terrorists, and whether cyber-weapons are likely to achieve these goals is doubtful. It concludes, therefore, only a new, impersonal humanistic non-antagonistic philosophy could reverse the trajectory and avert

another impending apocalypse. Philosophy ought to help in bringing about moral meaning, to a better, more rational world, not war.

Only total renunciation of interference in nations' internal affairs and violation of generally organized principles/standards of international law can make it possible to work out wide ranging measures for the suppression of terrorism. With good will in evidence, obviously, it is possible to reach agreement also on such a problem as a joint effort to suppress acts of international terrorism, all the more so since this is a matter of vital concern to everybody.

To realize this, nations and other international actors ought to take progressive steps by reaching a consensus on adopting all appropriate measures to prevent their territories from being used to prepare, organize, and conduct terrorist activities, including ones directed against other participating nations and their nationals; and erring nations should face stiff sanctions. However, nations should ban the illegal activities, on their territories—including by individuals, groups and organizations that incite, organize, or participate in acts of terrorism. Accordingly, nations should be mandated to do possible to ensure internal socio-economic and political security (including food security and justice) to forestall those issues that do gravitate to controversy on the international scene.

From a broader security perspective, nations now face a range of amorphous threats to their safety that are difficult for the traditional tools of national security to reach. The lines between domestic and foreign, private and public, or police and military are blurring, and the nature and requirements of national security are changing rapidly. The most important implications of these changes for cyber security may well be that national policies must adjust to growing interdependence among economies and emphasize the need for cooperation among nations to defeat cyber threats.

The international law should offer better, universally upheld and efficacious principles by which to govern the relations of states to reflect current but emergent relationships. In fact, national legislations and the UN General Assembly should immediately adopt a bill that would make it easier for law enforcement to wiretap computers and combat cyberterrorism. This could create formidable obstacle in the way of international terrorism and assure a concerted effort by all nations in the fight against it and in its eventual suppression—on a practical and germane commitment towards these would controllably detonate the cyber-base variant of international terrorism and avert an impending time-bomb signaling an apocalypse.

References

- Alexander, J., David, C. & Wilkinson, P. (1979). *Terrorism: Theory and Practice*, Colorado: Westview Press.
- Asekhauno, Anthony Afe. (2017). "How Philosophy caused World War I...and others." *Idea: Polish Journal of Philosophy*, Bialystok, vol. 29/2: 230-240.
- Bazuaye, B. & Enabulele, O. (2006). *International Law*, Benin: AMBIK Press.
- Beres, L. R. (1979). *Terrorism and Global Security; The Nuclear Threat*, NY: Westview press.
- Blishchenko, I. & Zhdanov, N. (1984). *Terrorism and International Law*, USSR: Progress Publishers.
- Ekei, J. C. (2013). Ethical Implications of Terrorism on Human Person. *WAJOPS: West African Journal of Philosophical Studies*, vol. 15, 2013, 17-27.
- Garver, N. (1970). "What Violence Is." In: A. K. Bierman and J. Gold, *Philosophy for a New Generation*, New York: The Macmillan Company.
- Gross, F. (1969). *Assassination and Political Violence: A Report to the NCCPV, USA*, Washington: Government Printing Office.
- Jenkins, B. N. (1975). "International Terrorism: A New Mode of Conflict." In: *International Terrorism and World Security*, Ed. David Carlton and Carlo Schaerf, London: Hills.
- Karpets, I. I. (1979). *Crimes of International Significance*, Moscow: Yuridicheskaya Literature.
- Lewis, J. A. (2002). "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". *Center for Strategic and International Studies (CSIS)*, Washington DC, December 2002.
- Olajide, O. A. and Omoyibo, K, U. (2017). *Principles and Practice of Private Security in Nigeria*, Benin City: Mindex.

Prof. Anthony Afe Asekhauno, Ph.D and Theophilus Arebamen Okojie, Ph.D

Watson, J.(1984). *Twentieth Century World Affairs*, 3rd Ed., London: John Murry Publishers LTD.

Watson, O. *Longman Modern English Dictionary*, 1978.

Wilkinson, P. (1973).“Three questions on terrorism”.*Government and Opposition*, vol. 8, no 3.

Williams, SA, &Menstra, ALC de, (1987),*An Introduction to International Law...*, Montreal: McHills.