Article received in February 2017 and accepted for publication in May 2017

A CONCEPTION OF THE RELATIONSHIP BETWEEN TERRORISM AND CYBER WAR IN THE CONTEXT OF INFORMATION WARFARE

UMA CONCEÇÃO DA RELAÇÃO ENTRE O TERRORISMO E A GUERRA CIBERNÉTICA NO CONTEXTO DA GUERRA DE INFORMAÇÃO

Dardano do Nascimento Mota
Major of Communications
Army Command and General Staff College
22290-270 Rio de Janeiro, Brazil
dardanomota@yahoo.com.br

Abstract

The present paper aims to present an analysis of the potential relationship between Terrorism and Cyber Warfare in the context of Information Warfare. In order to achieve the proposed objective, the work has been divided into the following sections: preliminary considerations; Information Warfare and its main concepts; Cyber Warfare, where the aspects related to IW will be detailed; an overview of modern Terrorism; some considerations that will frame the analysis (state of the art); and, finally, a proposal on how the relationship between Terrorism and Cyber Warfare may be structured in the context of Information Warfare. The paper presents basic concepts related to Terrorism, Cyberwarfare, and Information Warfare that will be useful to understand the analysis conducted. To that end, a literature and documentary review has been conducted focusing on studies related to the issue. Once the relationship between Terrorism and Cyberwarfare had been verified, the materiality of Cyberterrorism as an important aspect of this relationship was analysed using Deductive Reasoning. Finally, the present paper aimed to reach some conclusions, among which is a future Information Warfare Command.

Keywords: Information Warfare, Terrorism, Cyberwarfare, Cyberterrorism.

How to cite this paper: Neves, N., 2017. A conception of the relationship between terrorism and cyber war in the context of information warfare. *Revista de Ciências Militares*, May 2017 V (1), pp. 91-114.
Avalable at: http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes.

Resumo

O presente artigo pretende apresentar uma análise sobre a possível relação entre o Terrorismo e a Guerra Cibernética no contexto da Guerra de Informação. Para atingir o objetivo proposto, o desenvolvimento do presente trabalho encontra-se subdividido nas seguintes secções: considerações preliminares; a Guerra de Informação (GI) com seus principais conceitos; a Guerra Cibernética (GC) onde serão detalhados os aspetos que a relacionam com a GI; um *overview* do Terrorismo moderno; considerações integradoras do artigo (estado da arte); e, por fim, uma proposta de como estaria estruturada a relação do Terrorismo com a GC no contexto da GI. O artigo apresenta conceitos básicos relacionados ao Terrorismo, à Guerra Cibernética e à Guerra de Informação, objetivando facilitar o entendimento da análise desenvolvida. Isso posto, empregam-se a pesquisa bibliográfica e documental, priorizando os estudos relacionados ao assunto proposto. A partir da constatação do relacionamento entre o Terrorismo e a Guerra Cibernética, é analisada a materialidade do Ciberterrorismo como um importante aspeto desse relacionamento, utilizando-se do Raciocínio Dedutivo como ferramenta. Por fim, o presente artigo buscou encontrar conclusões quanto a isso, apontando, dentre elas, para a futura estruturação de um Comando de Guerra de Informação.

Palavras-Chave: Guerra de Informação, Terrorismo, Guerra Cibernética, Ciberterrorismo.

1. Introduction

"Violence arms itself with the inventions of Art and Science in order to contend against violence". When Clausewitz made this assertion in his work *On War*, he predicted the importance of technology for combat success.

Today, because of its volume and variety of sources, data processing is mostly based on Information Technology[1] (IT) structures. This has increased our dependence on digital technology.

Thus, we have witnessed an increase in asymmetric conflicts[2] and Irregular Warfare[3], which have been occupying an increasingly relevant space in international affairs. In this context, terrorism is becoming the answer for any groups that disagree with the status quo. It has also contributed to growing uncertainty and fear in various parts of the world.

This complex and diffuse reality refers to what has been called "4th Generation War" which, according to Wunderlich (2012, p. 7), consists of "a multidimensional conflict involving

[1] A set of individual devices, such as hardware, software, telecommunications, or any other type of technology that participates in, or creates, information processing, in addition to storing it. Retrieved from: http://www.convibra.com.br/upload/paper/adm/adm_3123.pdf.

[2] Any type of military conflict in which - at least at some point - one of the contenders has clear military (and especially technological) superiority on the ground. Retrieved from: http://www.scielo.br/pdf/his/v29n2/v29n2a09.pdf.

[3] Conflict conducted by a force that does not belong to a formal military organisation and, especially, that does not have institutional legal legitimacy. Retrieved from: http://www.eceme.ensino.eb.br/images/IMM/producao_cientifica/dissertacoes/marcelo-bastos-de-souza.pdf.

ground, fluvial, maritime, air, and space actions, as well as actions in the electromagnetic spectrum and cyberspace".

The author adds that "in the current challenging strategic environment, the enemy could be an independent state, a coalition of states, a terrorist group, or any criminal organisation".

This context of political and social transformations is also one of constantly changing values. This process, which is driven by technology and by a variety of interests, has demonstrated the volatility of economic and political structures. In keeping with this trend, the speed of information transmission and the global reach of data have played a role in narrowing human relationships. The main platform through which this occurs is the internet.

The Internet has influenced our way of life in recent years. For Nunes (2010, p. 10) "large data management systems are accessible to everyone through the internet to some extent. All kinds of data, including classified data, now travel through this vast network".

Furthermore, the ease of use of the Internet, which can be accessed through different devices such as tablets and smartphones, lends it unprecedented portability and reach. This has contributed to strengthen the "Information Society". With regard to the concept of information society, the Brazilian Green Paper on Defence (2010, p. 14) states that "the new configuration of this society includes increasing cyber security threats and vulnerabilities, and increasingly complex environments with multiple actors, a variety of interests, and constant and rapid changes".

This confirms the realisation that we inhabit a reality marked by complexity, speed, and large amounts of data. This has required increasingly specific capabilities to operate IT assets.

At the same time, disputes for power and influence have aggravated. This has intensified the use of social networks, of the digital press, and of the various media for the dissemination of ideas by a wide range of groups, including armed groups.

Some terrorist organisations make extensive use of IT assets to achieve their goals. One such organisation is the self-proclaimed Islamic State (DAESH), for which "ideological propaganda is an activity that involves advanced technology operated by qualified professionals, including westerners with high levels of education" (Napoleoni, 2015, p. 57). For example, "when social networks took down the video of James Foley's beheading by DAESH, within a few hours the terrorist group's propaganda team had restored access to it through allied websites hosted abroad" (Napoleoni, 2015, p. 57).

Hacker groups, such as the Syrian Electronic Army (SEA)[4], have showcased their capabilities through cyber attacks on media vehicles or state agencies in support of the Bashar Al Assad government. This has reinforced the idea that states and private enterprises will need to be increasingly capable of conducting cyber warfare.

[4] In order o fight its adversaries in the civil war that has been ravaging Syria since 2012, the Syrian government has created the Syrian Electronic Army, which is not only responsible for cyber security and defence activities but also carries out media activities with the aim of exposing the illegitimacy and radicalisation of their opponents. Retrieved from:http://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/XIII_cadn/guerra_hibrida_e_ciberconflitos_uma_analise_das_ferramentas_ciberneticas_nos_casos_da_siria_e_conflito_russia-ucrania

In light of the above, Brazil's White Paper on National Defence states that "other challenges facing the country relate to the ability to deal with the so-called 'conflicts of the future'". Among them are **Information Warfare,** as well as small-scale conflicts with indeterminate origin and diffuse command and control structures **that operate through the use of social networks**" (Brasil, 2012, p. 28) (emphasis added).

Information Warfare does not only involve countries with a recent history of conflict. It is present in a world that is increasingly interconnected and that has dynamic social, economic and political indicators.

This paper's main objective is to present a conception of how Terrorism and Cyber Warfare relate in the context of Information Warfare, as well as to highlight its consequences, with special emphasis on cyberterrorism.

The paper used a qualitative methodology which included a literature review and documentary research phase in order to establish a clear conception of the relationship between Terrorism and Cyber Warfare. Thus, as this is a relatively recent and broad topic, we have endeavoured to relate terrorism and cyber warfare to Information Warfare concepts.

The analysis is divided into six sections (in addition to the introduction and the conclusions): the first section will present the preliminary considerations; the second will focus on Information Warfare (IW) and its principal concepts; the third will deal with Cyber Warfare (CW) and will further examine the aspects related to IW; the fourth will consist of a general analysis of modern Terrorism; the fifth will present the paper's conceptual framework (state of the art); and the last section will advance a proposal on the relationship between Terrorism and CW in the context of IW.

2. Information Warfare, Cyber Warfare and Terrorism

War is a recurring theme in human evolution. It has become increasingly complex. Understanding its dynamics requires knowledge of subjects related to warfare, and these subjects are themselves interconnected.

This knowledge involves power sectors such as the economic, the military and the political sector. Thus, World War II (1939-1945) and the Cold War (1949-1989) have not only entered into history, they also influenced the course of international relations in the twentieth century.

In the twenty-first century, some conflicts were not only fought within the above context, but also had something in common: terrorism as one of their justifications. Walzer (2010, p. 336) states that "in war, terrorism is a way of avoiding direct combat with the enemy army. It represents an extreme form of the strategy of 'indirect approach'"[5].

Today, terrorism is associated with large-scale conflicts. For example, the attacks of 11 September 2001 contributed to the US invasion of Afghanistan in 2002. Similarly, the "Axis of

[5] The Strategy of Indirect Approach (conceived by Liddell Hart) aims to take full advantage of the mobility, speed and surprise offered by modern military technology to unbalance the structure of the enemy apparatus. Retrieved from: http://www.esg.br/images/Revista_e_Cadernos/Cadernos/CEE-012.pdf.

Evil"[6] and weapons of mass destruction rhetoric gave the Bush administration (2001-2009) a pretext to invade Iraq in 2003.

As we can see, terrorism has become one of the main justifications for wars that have engaged numerous resources and taken thousands of lives. This reinforces the relevance of the topic at hand, given its ability to mobilise international efforts.

At the same time, the world has witnessed cyber attacks, which are becoming part of a reality where Information Technology could be used as a powerful weapon in asymmetric conflicts.

One case that illustrates this idea is the relationship between China and the US, especially with regard to these countries' power struggle in cyberspace[7]. Clarcke and Knake (2015, p. 45) argue that "by the end of the 1990s, China's strategists had converged on the idea that cyber warfare could be used by China to make up for its qualitative military deficiencies when compared to the United States".

In an environment of threats that include the expansion of terrorism and the growing relevance of Cyber Warfare, it seems pertinent that we attempt to understand what relationships exist between these issues. This idea has allowed us to formulate some questions to guide the present work:

1. What are the main points of intersection between Cyber Warfare and Terrorism?
2. What is the materiality of cyberterrorism?
3. Is there any effective defence against this threat?
4. Can terrorists and "cyber criminals" act together?
5. How does the relationship between Cyber Warfare and Terrorism fit into the context of Information Warfare? And what are its likely consequences?

The answer to the last question is the core idea of this integrative reflection. It is, therefore, necessary to present the main aspects of Information Warfare, Cyber Warfare, and Terrorism before further exploring the answers to the last question.

Given the scope of the topic proposed, the lines of thought followed in the present analysis will be based on three factors: economic, political and military.

2.1. Information Warfare (IW)

IW is the focus of the present work. However, before we begin to address it, we will present three interconnected concepts that frame it. The first is Information. Information is the "intelligible representation of objects, states, and events in real, virtual, and subjective

[6] A group of countries comprising Iran, Iraq and North Korea; these countries were accused by the US of being the leading funders of international terrorism.

[7] Virtual space consisting of computer devices, networked or otherwise, where digital information travels, is processed, and/or is stored (Brasil, 2014a, pp. 18;36).

domains, which includes processes for the construction of knowledge, enabling the understanding of the operational environment" (Brasil, 2014, pp. 4-17).

The second concept, that of Information Dimension, concerns "the set of individuals, organisations, and systems that rely on decision makers to obtain, produce, disseminate, and act on information" (Brasil, 2014, pp. 2-3).

The third concept is that of Information Superiority, which is defined as:

> "An **operational advantage** derived from the ability to collect, process, disseminate, exploit, and preserve an **uninterrupted flow of information** that is available to commanders at all levels, while seeking to exploit the opponent's information and/or deny them access to it. It means possessing more and better information than the adversary on the operational environment. **It enables control over the information dimension** (electromagnetic and cybernetic spectra, among others) within a given time-span and location" (Brasil, 2014, pp. 3-2).

In light of these definitions, it can be said that IT assets are required for handling and storing Information. They provide timely and relevant information in the information dimension. Furthermore, information management is crucial to guarantee Information Superiority.

Moreover, and considering the quantitative and qualitative expansion of IT assets, since an increasing number of people have access to the internet (Figure 1) and a social network profile (Figure 2), it can be said that we live in an increasingly "informational and digitised" reality.

	2003		2008		2013	
	Millions	%	Millions	%	Millions	%
World	**59.7**	**100.0**	**173.4**	**100.0**	**245.2**	**100.0**
Developed	49.6	82.9	135.9	78.4	197.4	80.5
Developing	7.1	11.8	34.7	20.0	45.0	18.4
Other/Unknown	3.1	5.2	2.8	1.6	2.7	1.1
Africa	0.3	0.5	1.0	0.6	2.3	0.9
Americas	23.9	40.1	71.8	41.4	98.9	40.4
Asia	5.3	8.9	29.8	17.2	36.9	15.0
Europe	25.8	43.3	63.7	36.8	98.0	40.0
Oceania	1.2	2.1	4.2	2.4	6.4	2.6

Figure 1 - Internet domains by world region

Source: International Telecommunication Union report[8].

[8] Retrieved from: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.

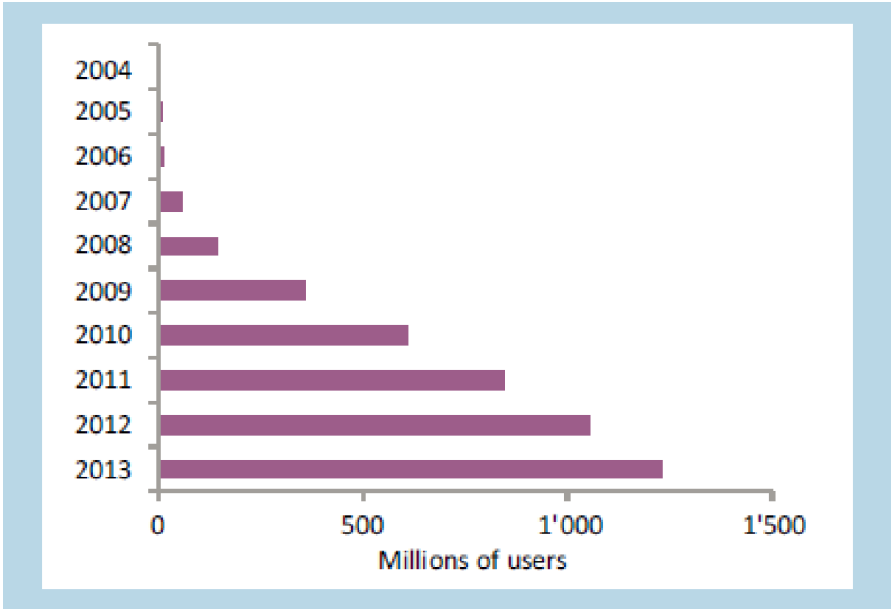

Figure 2 - Chart depicting the growth of Facebook users (2004-2013)

Source: Report of the International Telecommunication Union[9]

This leads us to Information Warfare (IW). This topic has been widely covered in a variety of literature, which contributes to a number of different definitions. The issue has been increasingly addressed since the end of the First Gulf War (1991).

First, Information Warfare can be said to consist of "actions to deny, exploit or destroy an adversary's information structures, as well as taking action to counter such actions when they are taken by the adversary, expanding one's own information management capabilities" (Militão, 2014, p. 9). Haeni (1997, p. 3) offers a complementary perspective, defining it as:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks, while defending one's own information, information-based processes, information systems, and computer-based networks.

This demonstrates that the main objective of IW is to achieve a state of Information Superiority, as defined by the Brazilian Ministry of Defence:

> Information Warfare – **Set of actions devised to obtain information superiority** by affecting an opponent's communication networks and the information that underlies adversary decision processes, while

[9] Retrieved from: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.

guaranteeing friendly information and processes (Brasil, 2007, pp. 124;274) (emphasis added).

This is an important concept, since Information Superiority is a sine qua non condition for success in Information Warfare. Figure 3 depicts one of the most accepted models of Information Superiority, as advanced by Alberts in his work NCW.

Figure 3 identifies two contenders: "the dominant competitor" and the "dominated competitor". It should be noted that in this model, Information Superiority is not indefinitely guaranteed over time. This means that the "dominant group" can become the "dominated group" and vice versa.

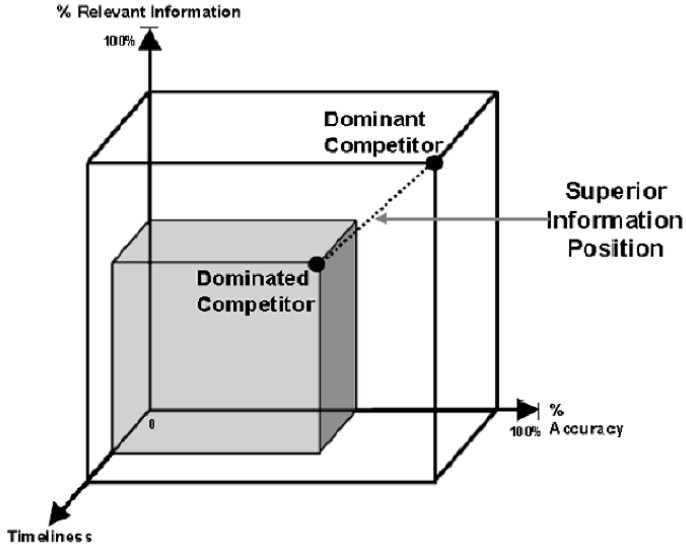

Figure 3 - Conceptual Model of Information Superiority

Source: (Alberts, Garstka, & Stein, 1999, p. 34)

This reversal will depend, among other factors, on the assets employed in the collection and processing of information, particularly the human factor, especially with regard to technical ability and motivation to act. This may provide "control of the narrative".

In addition to the dichotomy illustrated by the clash between the "dominant group" and the "dominated group", IW can be classified, among other subdivisions, according to two forms: Offensive and Defensive. This division shows that, in the first form, information is acquired through the unauthorised exploitation of systems. The focus of the second form (defensive) is prevention by monitoring and accessing available third party information (Militão, 2014, p. 40).

According to the line of thought we have been following, IW largely involves IT structures. These structures provide the "pathways" through which information will feed information systems, both in their Offensive and Defensive forms.

Likewise, IT structures will be the platform where Cyber War is conducted, an issue that will be discussed further on. However, it should be stressed that Information Warfare is not limited to IT assets. According to Stein[10] (1995):

> Information warfare in this sense can be seen as societal-level or nation-to-nation conflict waged, in part, through the worldwide internetted and interconnected means of information and communication (…) Information warfare, then, may define future warfare or, to put it another way, be the central focus for thinking about conflict in the future.

Stein (1995) further stresses that "although information warfare would be waged largely, but not entirely, through the communication nets of a society or its armed forces, it is fundamentally not about satellites, wires and computers. It is about influencing human beings and the decisions they make".

Thus, framing the main threats in the context of IW, Stein (1995) highlights the proliferation of non-state actors as "terrorists with easy access to worldwide computer and communications networks **to influence**, to exchange information, or to coordinate political action on a global basis" (emphasis added). This confirms the importance of maintaining control of the narrative. Without it, there is no legitimacy[11], even if Information Superiority has guaranteed it.

For this reason, controlling the dominant narrative can be considered a decisive factor for current military operations, since losing it can even limit freedom of action on the ground and influence actions in cyberspace.

Given the scope of IW and the threats it poses, it is fair to conclude, albeit partially, that issues such as Cyber Warfare and Terrorism can be contextualised within IW. However, before we establish how the relationship between them develops, we will endeavour to explore them separately.

2.2. Cyber Warfare

Cyberspace is not limited by geopolitical boundaries. In that context, cyber operations imply great flexibility and speed; hence decisions can miss their window of opportunity. Clarcke and Knake (2015, p. 41) confirm this, arguing that "the need to take the initiative […] is dictated in part by the fact that actions taken in cyberspace move at a pace never before experienced in war".

---

[10] Dr George J. Stein (Bachelor, Assumption College, Master of Arts, Pennsylvania State University, PhD, Indiana University). Retrieved from: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-p/1995/3tri95/pstein.html.

[11] Characterised by the need to act according to legal diplomas, mandates and commitments issued by the State (Brasil, 2014a; pp. 5-5)

It is between the lines of the above quote that Cyber Warfare is embedded. According to the Brazilian Green Paper on National Defence (2010, p. 23), it consists of "a set of offensive and defensive information actions and information systems actions devised to deny, exploit or destroy enemy information systems. The aim is to obtain both military and civilian advantages".

The main media used in CW to obtain these advantages has been the internet. Botnets[12] and worms[13] travel that media to acquire cyberspace superiority, with potential political, economic and military repercussions.

That being said, in recent years the importance of CW has been growing thanks to its ability to attack banking, government and defence systems, among others. This has been the motivation behind the creation of state bodies to act in the cybernetic environment.

To illustrate this, we will present the example of three nations that have invested considerable resources (financial, human and technological) in their Cyber Warfare structures: Russia, China and North Korea. For different reasons, these countries have demonstrated some of their capabilities by launching cyber attacks for political, economic, and military purposes.

From the policy point of view, Russia has used its cybernetic tools as instruments to project power and influence. This was demonstrated in the cybernetic DDoS[14] attacks on Estonia (one of the most wired nations in the world) in 2007. A significant portion of the country's computer systems was taken down when the servers that hosted the country's most accessed pages were flooded with access requests, to the point "that some of the servers collapsed under the load and (…)" became "inaccessible. Estonians could not use their online banking, their newspapers' websites, or their government's electronic services" (Clarcke and Knake, 2015, p. 16).

In the economic sector, Chinese hackers have attempted to acquire the source codes of multinational companies. Clarcke and Knake (2015, p. 53) state that this has driven the development of new technologies in China:

> When Google's scientists figured out what was going on (…), they traced back the hacking to a server in Taiwan, where they found copies of their proprietary information and those of at least twenty other companies, including Adobe, Dow Chemical, and the defense contractor Northrop Grumman.

[12] "A network of computers that have been forced to operate on the commands of an unauthorized remote user, usually without the knowledge of their owners or operators" (CLARCKE and KNAKE, 2015, p. 224).

[13] "Malicious software that causes computers or networks to do things that their owners or users would not want done" (Clarcke and Knake, 2015, p. 224).

[14] "Distributed Denial of Service (DDoS): basic cyber war technique often used by criminals and other nonstate actors in which an Internet site, a server, or a router is flooded with more requests for data than the site can respond to or process" (Clarcke and Knack, 2015, p. 223) .

Unlike Russia and China, North Korea only provides internet services to a small portion of its population. Paradoxically, this reality has not prevented this country from investing in its Cyber Warfare infrastructure as a tool for projecting its military power. This can be seen in the following statement:

> The Enemy Secret Department Cyber Psychological Warfare Unit 204 **has 100 hackers and specializes in cyber elements of information warfare.** (…) Unit 121 (…) specializes in disabling South Korea's military command, control, and communications networks. (Clarcke and Knake, 2015, p. 27) (Emphasis added)

The above leads us to conclude that the handling of Information in the context of CW is a common point among the three nations. This is confirmed by the fact that Cyber Warfare is related to Information Warfare in the sense that both aim to create an environment of information superiority through the use of computer networks.

However, this requires exploiting cyberspace weaknesses. One such weakness, which facilitates the action of hackers, is something that has not yet been properly sized: the internet's vulnerabilities.

Against this background, Clarcke and Knake (2015, p. 72) state that "There are bound to be vulnerabilities in anything so large. Today, it has grown so extensive that the Internet is running out of addresses". Thus, given the reach of the internet, it is imperative that we characterise some of its weaknesses.

The first is that the majority of data traffic occurs "openly", that is, without encryption[15]. "Many (but not most) websites now use a secure, encrypted connection when you log on", however, "due to cost and speed, most then drop the connection back into an unsecure mode after the password transmission is made" (Clarcke and Knake, 2015, p. 69).

The second vulnerability is how easy it is to propagate malicious traffic designed to attack computers. This software can travel the internet virtually unsupervised. "Most ISPs do not take even the most basic steps (…), in part because it is expensive and can slow down the traffic, and also because of privacy concerns" (Clark and Knake, 2015, p. 70).

Equally important, the third vulnerability is the decentralised architecture of the internet. This is due to the fact that its designers "placed a higher priority on decentralization than on security" (Clarcke and Knake, 2015, p. 70).

In spite of all this, the means employed in Cyber Warfare are not limited to the exploitation of internet gaps. Viruses, logic bombs[16], and hackers can also act towards non-state ends. This is evidenced as follows:

> The same way that a hand can reach out from cyberspace and destroy an electric transmission line or generator, computer commands can derail

[15] "The scrambling of information so that it is unreadable to those who do not have the code to unscramble it" (Clarcke and Knake, 2015, p. 224).

[16] Malicious code.

> a train or send freight cars to the wrong place, or cause a gas pipeline to burst. Computer commands to a weapon system may cause it to malfunction or shut off. What a cyber warrior can do, then, is to reach out from cyberspace, causing things to shut down or blow up, things like the power grid, or a thousand other critical systems, things like an opponent's weapons (Clarcke and Knake, 2015, p. 85).

Thus, when we consider what we call critical infrastructures[17], we can see that they are important targets for Cyber Warfare. This is due, for example, to the socio-economic impact that a shutdown of energy supply structures could have on industrial parks in cities such as Chicago or Beijing.

In the face of this, two points emerge that could be related in the context of CW: public opinion and authorship attribution of cyber attacks. With this in mind, we can posit that cyber attacks with impact on critical infrastructures would also influence public opinion. However, to what extend would that influence occur?

Clarcke and Knake (2015, p. 173) state that "when it comes to figuring out who attacked you, unless you are sitting on the network the attacker uses and you see it coming (and sometimes not even then), you may not know right away". The difficulty in identifying the origin of a cyber attack can create multiple "public opinions" as to its authors. This is subject to change if the attacker claims the attack, which would generate a different, probably more homogeneous public opinion.

In addition to this, and bearing in mind this scenario of uncertainty, it should be noted that, unlike Conventional and Non-Conventional Warfare[18], CW also involves issues related to private enterprise. This includes companies that do not wish to comply with the regulations that states wish to impose.

Against this background, it should be noted that state regulations are related to Cyber Defence[19] and, in some cases, are contrary to private interests, as they could restrict the freedoms or reduce the profits of large IT corporations. At this point, it is necessary to control the state's narrative with the big corporations in order to influence society regarding the urgency of enhancing digital security in exchange for some of the amenities[20] offered by the private sector to the consumer market. Thus, the influence of Economy and Policy on Cyber

[17] If the performance of these facilities, services, goods and system is degraded, or if they are interrupted or destroyed, this will have serious social, economic, political, international repercussions, or repercussions for the security of the state and of society (Brasil, 2014a, pp. 19;36).

[18] A broad spectrum of usually long-term military and paramilitary operations predominantly carried out through, with or by native or subversive forces organised, trained, equipped, supported, and directed to varying degrees by foreign sources. It includes, but is not limited to, guerilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery. Retrieved from: http://educaleaks.dominiotemporario.com/doc/Conceitos_Relacionados_a_Guerrilha.pdf

[19] Offensive, defensive and exploratory actions carried out in Cyberspace, in the context of strategic national planning, coordinated and integrated by the Ministry of Defence, devised to protect information systems of interest to National Defence, to obtain data for the production of Intelligence knowledge, and to compromise the information systems of the opponent. (Brasil, 2014a, pp. 18;36).

[20] Transmission speeds and the reach of data packets offered by IT companies to their users.

Warfare shows the complexity of the instruments that shield critical infrastructures from cyber attacks.

In addition to this, greater economic and social development is currently associated with an abundance of IT assets. This has increased the technological dependency of all instruments of power and created a corresponding need to develop Cyber Defence structures.

For example, in their analysis of the current US status regarding Cyber Warfare Clarcke and Knake (2015, p. 119) state that "**on this fundamental issue of whose job it is to defend America's infrastructure in a cyber war**, the government and industry are talking past each other" (emphasis added). "As a result, no one is defending the likely targets in a cyber war, at least not in the U.S".

The American example proves that "it is easier to mount cyber attacks than to defend against them, possibly encouraging an offensive bias in the construction of new capabilities" (Kissinger, 2014, p. 346). This statement has clearly had an impact on the US, since some American military analysts have proposed the creation of a Cyber Force separate from the other four branches of the armed forces. According to Graham (2016, p. 74):

> Establishing the Cyber Force, complete with its own member of the Joint Chiefs of Staff, would allow military leaders with experiential depth in cyberspace to effectively communicate the challenges of cyberwarfare to political decision makers. In turn, the Cyber Force leaders could efficiently employ the guidance and resources ascribed to military operations in cyberspace.

Thus, we can conclude in part that the current CW environment is varied and complex. It spans areas that deeply connect the governmental and private spheres. The proof of this is that many of what we call critical infrastructures operate on the internet via private providers. However, there can be no guarantee of protection without the presence of robust Cyber Defence structures. Although these structures do not ensure full protection, they can contribute to supply basic services such as electricity and transportation to society.

As we have seen, the permeability promoted by the internet also has impact on the political and military sectors. These sectors are inhabited by two relevant actors for the development of Cyber Defence, the government and the armed forces.

Despite what has been discussed so far, we must also briefly examine terrorism in order to establish, in a consistent manner, its relationship with Cyber Warfare in the context of Information Warfare.

2.3. An overview of modern terrorism

Terrorism is not a recent phenomenon. According to Teixeira da Silva, it is historically divided into "waves". The "first wave" (1880-1914) sought popular support and was markedly anarchist; the "second wave" (1945-1974) aimed to obtain independence for the colonies and could be found in countries such as Algeria and Indonesia (which were colonies at the time);

the third wave (1975-1985) was characterised by terrorism supported by nation states such as Libya and had a strong political bias.

Following this line of thought, we are now in the "fourth wave", which is characterised by "actions of global and unlimited proportions, **using unconventional assets** that characterise those actions as a form of **Asymmetric Warfare**" (Simioni, 2008, p. 24).

Although terrorism is not a recent phenomenon, the ideas that define it are still controversial. In light of this, we will present some of those ideas in order to find the ones that best suit this reflection.

For Walzer (2003, p. 335), the aim of terrorism is "to destroy the morality of a nation or a class, to undermine its solidarity. Its methodology is the random murder of innocent people".

In another perspective, Marighella (1968, p. 1) highlights the relationship between violence and terrorism, emphasising that the latter "does not divide, on the contrary, it represents the centre of attraction. Today, being 'violent' or a 'terrorist' is a quality that ennobles any honest person". Whittaker (2005, p. 21), for his part, states more broadly that:

> Terrorism, in the most widely accepted contemporary usage of the term, is fundamentally and inherently political. It is also ineluctably about power: the pursuit of power, the acquisition of power, and the use of power to achieve political change. **Terrorism is thus violence - or, equally important, the threat of violence** – used and directed in pursuit of, or in service of, a political aim. (Emphasis added)

That being said, analysing the above definitions leads us to ask a counter question: does terrorism only involve the murder of people for political aims? We must examine the matter further to discover, as Whittaker argues, that terrorism can also be the threat of violence, which generates social intimidation.

Visacro (2009, p. 283) states that "terrorism comprises a wide range of activities that transcend common sense. It is often associated with demagogic proselytism that aims to achieve certain psychological goals".

The above allows us to identify two ideas. The first is that: terrorism's main tool to achieve success is violence; and the second is that: terrorism includes variants which, due to their ability to promote intimidation, are ultimately designed to achieve political aims. Thus, with these two ideas as our starting point, we will analyse some of the peculiarities of terrorism.

With regard to the first idea, terrorism in recent years has been marked by indiscriminate violence. According to a report of the Institute for Economics and Peace, approximately 5,000 people were killed in terrorist attacks in 2000. In 2014, that number was just over 30,000.

Walzer (2005, p. 347) confirms this, pointing out that terror "is the totalitarian version of war and politics. It takes the conventions of war and the political code and reduces them to dust. It disregards moral limits beyond which any other limit seems impossible". In keeping

with this idea, one of its manifestations was the Beslan Massacre that took place in Russia in 2004. According to Giel (2014, p. 21):

> The Beslan tragedy distinguishes itself from other terrorist attacks that have occurred in the history of the Russian Federation due to its magnitude and complexity. I acknowledge that, in terms of hostage – taking tragedies, the terrorist attacks of Budennovsk (1995), Kizlyar (1996) and Dubrovka (2002) were also momentous acts that threatened the security of the Russian. However, the main reasons for considering Beslan a potential turning point are the extremely high level of hostages (1300), fatalities (372) and injuries (747), the cruel acts of the terrorists towards children and women, the long duration of the siege (3 days), the well - preparedness of the perpetrators that led to severe issues among the responsible security services at the time of the siege as well as the fact that Beslan was a global media event which led to questions about the capability of Russia to prevent and to manage terrorist attacks.

Another peculiarity, also related to violence, is the potential to change geopolitical configurations. The most widely-known case is that of the self-proclaimed Islamic State. For Napoleoni (2015, p. 52):

> The contemporary character and the pragmatism of the Islamic State come from a **blend of modern strategy, technology and communications capabilities**, psychological propaganda, old-fashioned warfare techniques, and tribal customs such as arranged marriages between Sunni tribal women and jihadists. Seen from this perspective, it is clear that the Islamic State has far outdone the feats of all past and present ghost states when it comes to **nation-building**, and that it will perhaps succeed where all postwar armed organisations have failed: **in creating, from the rubble of acts of sheer violence, a new type of state**, considerably large, strong, and strategically important enough to merit the attention of the world. (Emphasis added)

Still regarding the first idea, it is clear that terrorist organisations are adopting IT-based methods in their actions. This could be seen in the coordination and control measures employed in the terrorist attacks in Mumbai in 2008. On that occasion, a small group of terrorists using mobile phones was successful in carrying out attacks that resulted in the death of more than 180 people.

The Mumbai bombings demonstrated the importance not only of technological assets, but also of individuals capable of exploiting their potential. This ensured a state of Information Superiority that the Indian authorities were not prepared to fight.

DAESH has used technological means, especially the internet, to recruit individuals. On that subject, Napoleoni (2015, p. 49) states that "the growing number of people who adhere to the practice of violence through DAESH propaganda confirms the fascination of their message: that the virtual world in which we live can also produce new acts of irrational and barbaric violence".

Now that the first idea has been addressed, we will analyse the second idea, highlighting two other peculiarities of terrorism. The first is its financial power, which has had repercussions for state policies.

Although each nation deals with the issue in a different way, its financial implications are indisputable as it implies costs with security. These costs derive not only from managing the consequences of a terrorist attack, but also from preventing one from happening. For example, Brazil invested approximately € 900 million[21] in counter-terrorism measures to guarantee security during the Rio 2016 Olympics.

The second peculiarity is associated with what Visacro (2009, p. 293) believes drives the planning of terrorist actions: the media, public opinion and decision-makers. This triad of the interconnected world which we inhabit is also based on IT assets, especially the internet.

Visacro (2009, p. 293) further states that "the study of the media and public opinion allows us to set suitable goals. **The analysis of decision-makers is required to define how the state will react to media pressure and pressure from public opinion**" (emphasis added). This will entail states taking back control of the narrative from terrorist organizations.

Therefore, we can partly conclude: that terrorism has acquired relevant variants associated with technology; that successful terrorist actions can no longer follow the same pattern; and that the structure of terrorist organisations has evolved, including with regard to human resources. Furthermore, according to Akpan (2008, p. 47):

- Terrorism has become more bloody;
- Terrorists are less dependent on state sponsors;
- Terrorists have evolved, developing new models of organisation capable of waging global campaigns;
- The world will see an increase in cyberterrorism and suicide attacks.

The aspects presented allow us to infer that Terrorism, Cyber Warfare and Information Warfare are related and that that relationship is becoming narrower.

The Mumbai bombings showed that terrorism, even if it involves violent action, has used technology to multiply its combat power, enhanced by Information Superiority, the main objective of Information Warfare, to carry out successful actions in the Information environment. This is another idea that will support the present reflection.

Furthermore, Cyber Warfare and Information Warfare can manifest themselves in a variety of power sectors. This can be seen in the international confrontations between world powers, such as the US, China, and Russia, for financial resources, geopolitical influence, and military power, which are supported by computer networks.

[21] Source: https://www.google.com.br/search?q=gastos+contra+antiterror+olimp%C3%ADada&biw=1252&bih=574&source=lnms&tbm=isch&sa=X&ved=0ahUKEwisppbE9IrQAhWIlZAKHXrcCB0Q_AUIBygC#imgrc=l43ZWgInH_dSBM%3A

Similarly, modern Terrorism in its various manifestations has sought to influence public opinion, with impact on the political, economic and military sectors. Today, DAESH is its ultimate manifestation, also embedded in the context of IW.

That being said, we have identified, among others, two points of intersection between Cyber Warfare and Terrorism. The first is how it affects public opinion and the second is how it uses Information Technology and Communications tools to amplify its effects. With regard to the above, Kissinger (2014, p. 346) states that:

> A laptop can produce global consequences. A solitary actor with enough computing power is able to access the cyber domain to disable and potentially destroy critical infrastructure from a position of near-complete anonymity. Electric grids could be surged and power plants disabled through actions undertaken exclusively outside a nation's physical territory (…). Already, an underground hacker syndicate has proved capable of penetrating government networks and disseminating classified information on a scale sufficient to affect diplomatic conduct.

Thus, the above points of intersection can aid us in constructing a conception of the relationship between Terrorism and Cyber Warfare in the context of Information Warfare. To further explore this idea within the information environment, each point of intersection will be addressed in the next topic.

2.4. The relationship between Terrorism and Cyber Warfare

When attempting to ascertain how Terrorism and Cyber Warfare are related in the Information domain, the two points of intersection referred to in the previous topic will be analysed. This analysis will allow us to verify the materiality of the relationship between the two issues.

The method chosen to verify this relationship will be based on a qualitative approach, focusing on a literature and documentary review and on observation as a data collection tool. Additionally, deductive reasoning will be used to structure a product of critical thinking on cyberterrorism. All this will enable us to put together arguments that support the relationship between CW and Terrorism in the context of IW.

Therefore, we will present some considerations regarding the "Information Dimension" referred to previously. It can be said that it is composed of "three interrelated perspectives that constantly interact with each other and with individuals, organisations and systems. Those perspectives are: logic, physics and cognition" (Brasil, 2014, pp. 2-3).

The logic perspective (which will not be addressed) corresponds to "where and how information is obtained, produced, stored, protected and disseminated. It refers to military command and control" (Brasil, 2014, pp. 2-4).

The physical perspective concerns "the physical platforms and the communications networks connecting them. It has a multinational character" (Brasil, 2014, pp. 2-4,).

For its part, the cognitive perspective includes the minds of decision-makers. "They can be influenced by individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, traditions, education, mental health, identities and ideologies" (Brasil, 2014, pp. 2-4). These considerations, combined with the above points of intersection between Terrorism and Cyber War, allowed us to elaborate Table 1.

Table 1 - Framework of relationships between Terrorism and Cyber Warfare

Dimension	Points of Intersection	Terrorism	Cyber War
Information	Public Opinion (cognitive perspective)	• It aims to shock and enact change through the use of violence or simple intimidation. • It is a Centre of Gravity[a] for terrorist actions.	• It seeks to influence society by exposing the vulnerabilities of the internet. • It can result in "multiple public opinions".
	Ample use of IT (physical perspective)	• It is used to coordinate and control terrorist agents worldwide (for example: through social networks).	• It is interconnected, since IT platforms are the main pathways through which worms travel. • It has global ties.

a) An essential component of a state, of a military force, or of a number of systems, that is essential for the survival of the whole. CoG are not limited to military forces and serve as an energy source that provides moral or physical strength, freedom of action, or will to act (Brasil, 2014).

Source: prepared by author.

That said, we now come to the aspects (highlighted in yellow) that demonstrate the relationship between Terrorism and Cyber Warfare in the context of IW. Combining them could enhance the effects intended by terrorist organisations.

In order to construct a conception of the relationship between Terrorism and Cyber War from an informational perspective, we must elaborate some comments on cyberterrorism, as the subject can tie together the points presented above.

Cyberterrorism is a recent issue that is still controversial as to its manifestations. Some authorities strongly disagree that it exists. However, they do not deny the possibility that the phenomenon will become a reality in the near future.

Clarcke and Knake (2015, p. 112) first state that "cyber terrorism is largely a red herring and, in general, the two words 'cyber' and 'terrorism' should not be used in conjunction because they conjure up images of bin Laden waging cyber war from his cave". However,

the same experts also point out that "a well-funded terrorist group might find a highly skilled hacker club that would do a cyber attack in return for a lot of money, but that has not happened to date" (Clarcke and Knake, 2015, p. 127).

Furthermore, Liang and Xiangsui (1999) point out that "just as there are all kinds of people in society, so hackers come in all shapes and colors. All types of hackers, with varying backgrounds and values, are hiding in the camouflage provided by networks: curious middle school students; on-line gold diggers; corporate staff members nursing a grudge; **dyed-in--the-wool network terrorists**; and network mercenaries" (emphasis added).

With due respect to the above statements, we must stress that the purpose of this paper is not to say that we are living in a world of cyber-terrorist attacks. However, the extant literature allows us to analyse it as a potential (and important) link between terrorism and cyber warfare. Thus, we will establish four premises:

1. Cyber attacks have been occurring in regions with IT facilities;
2. Cyberterrorism is a form of cyber attack;

Therefore, we can conclude that cyberterrorism can occur in any regions where there are IT facilities.

3. Terrorism disregards human rights;
4. Cyberterrorism is a form of terrorism.

Therefore, we can conclude that cyberterrorism disregards Human Rights.

Considering these premises and conclusions, we are now able to frame a few arguments. It can be seen that Premise 1, in combination with Premise 2, allows us to confirm that: cyber attacks are far-reaching and use IT tools (currently scattered over much of the world). Would that alone constitute a real threat of cyberterrorism? No.

However, by extending the two premises to asymmetric warfare, it can be seen that a terrorist organisation that seeks maximum effect and that possesses "means of persuasion" (be they ideological, religious or even financial) to co-opt hackers will be able to carry out cyberterrorism actions.

Another relationship that we can address is the direct link between premises 3 and 4. This link can be verified by considering the "Achilles' Heel" of a given public or private organisation.

Let us consider that the internet, because of its vulnerabilities and its ability to act on so-called critical infrastructures, would be the above "Achilles Heel". A terrorist group unconcerned with human rights and in possession of the cybernetic knowhow to exploit internet weaknesses may, for example, carry out cyber attacks on airspace control stations or on the command and control centres of hydroelectric plants such as the one in Itaipu[22].

[22] An important hydroelectric power plant in Brazil and Paraguay. Responsible for the supply of energy to the main Brazilian industrial centres.

Attacks of this nature could spread chaos and claim victims on a large scale. Clarcke and Knake (2015) present two complementary considerations in this respect:

> Hacking into the flight controls of an aircraft in flight is probably also becoming more feasible. The Federal Aviation Agency raised concerns with Boeing that plans for the new 787 Dreamliner called for the flight control system and the elaborate interactive passenger-entertainment system to use the same computer network. The FAA was concerned that a passenger could hack into the flight control system from his seat, or that live Internet connectivity for passengers could mean that someone on the ground could hack into the system (p. 165).
>
> The international laws of war prohibit targeting hospitals and civilian targets in general, but **it is impossible to target a power grid without hitting civilian facilities**. (…)While being careful with bombs, the U.S. and other nations have developed cyber war weapons that have the potential to be indiscriminate in their attacks (p. 163) (Emphasis added)

Thus, terrorist actions in cyberspace using malicious code on state or private infrastructures could cause cyberterrorism to violate human rights. This fact alone demonstrates its relevance.

Given this, can we say that we are experiencing cyberterrorism? No. However, the above links can be established, allowing us to argue that the threat may become clearer in the future due to the assets, individuals, and values that currently form the main terrorist organisations. However, how could this be achieved?

From a practical point of view, analysing Table 2 allows us to propose a solution to this question. This analysis requires looking, in particular, at the preparatory phase and at the consequences phase.

Table 2 – Timeline of a terrorist attack

Preparatory phase (before)	Crisis/Attack (during)	Consequences phase (after)
Terrorist activities: Capability building Recruitment Training Funds collection Research and development Acquisition of materials Intelligence gathering Planning Strategic displacement/bases Establishing a network Reconnaissance Counter-information Information Operations	Final displacement Rendezvous Equipment assembly Final reconnaissance Execution Extraction	Exfiltration[b)] Capability regeneration Assessment of consequences Analysis of operations Information Operations

b) Operation to retrieve the person responsible for an incursion into enemy territory.

Source: VISACRO (2009, p. 286).

An analysis of Table 2 also reveals the presence of Information Operations before and after a terrorist attack. This demonstrates its relevance in an IW scenario. In addition to this, a cyber-terrorist attack, if framed within the phases listed above, requires less time and activities in its timeline. This is demonstrated by the fact that the "Capability development" activity can be omitted as a group of individuals with the expertise to carry out cyber attacks is available.

Furthermore, another aspect that deserves mention is that the costs of a cyber-terrorist attack are lower than those of a "conventional" attack. The reason for this is that there are fewer requirements for Research and Development and strategic displacement/bases (included in the preparatory phase), which are provided by hackers in terrorist organisations.

Therefore, hackers in the service of terrorist organisations make it possible to conduct attacks in cyberspace, with serious consequences for society. Thus, bearing in mind the economic and military dimensions, Clarcke and Knake (2015, p. 182) state that:

> Insurgents in Iraq had used twenty-six-dollar software to monitor the video feeds of U.S. Predator drones through an unencrypted communications link. While not directly threatening to American troops, the discovery raises questions about the Pentagon's beloved new weapon. What if the unencrypted signal could be jammed, thus causing the drone to return home? American forces would be denied one of their most valuable tools and an off-the-shelf program would defeat the product of millions of dollars of research and development.

The above allows us to partly conclude that cyberterrorism is a concrete possibility, given the feasibility of a relationship between Cyber Warfare and Terrorism. For this to happen, however, some factors must play an important role. Among them are the time factor and the human factor.

As for the first, it is clear that any terrorist attack takes time to prepare. This will affect whether or not the attack is successful.

Closely related to the time factor, the human factor is crucial. It includes control of the narrative, which will ensure that the best suited individuals will be co-opted to execute a cyber-terrorist attack.

Conclusion

The above allows us to state that the analysis indicated the possibility of a clear and potential relationship between Terrorism and Cyber Warfare in the context of IW. This was essentially demonstrated by the points of intersection between public opinion and the use of IT assets.

In conclusion, and within the context of the above points, some aspects that support the relationship analysed in the present work can be highlighted, namely the Information Warfare environment. Terrorism is increasingly employing social networks

and IT to achieve its aims. Cyber Warfare, on the other hand, has taken advantage of the vulnerabilities of the internet to become a new form of conflict.

Terrorist groups are becoming more violent, more financially independent, and now hold a number of capabilities that enable them to operate over long distances. It is against this background that cyberterrorism is emerging.

Cyber Warfare is moving beyond the boundaries of public and private stakeholders. This has repercussions for all power sectors, in particular the political and the military sectors. This includes the government and the armed forces, and some countries, such as the US and China, have been restructuring their cyber infrastructures.

Moreover, the above relationship (Terrorism and CW) hinges on the importance of "control of the narrative". This does not only refer to "communicating first", in the case of a conflict between state and non-state actors. It is also necessary to support the narrative.

This could be achieved through firm action by the state (while respecting the different nuances of each nation) to regulate the internet, particularly with regard to Network Security, a topic that is broadly embedded in Information Warfare.

Furthermore, the above shows the possibility that we are in the presence of a "fifth wave" of Terrorism related to CW. This new "wave" would be a combination of the two previous phases, in which militarily weaker nation-states have sought to use cyber-attacks to assert their wills over stronger states, attributing the "responsibility" of those attacks to groups of hackers in their countries.

Given this scenario, we could return, in a holistic view, to the idea of "control of the narrative", both domestically and abroad, as a strategic necessity. A possible answer to this may lie in the creation of an Information Warfare Command, which would include, among others, Counter-Terrorism and Cyber Warfare agencies.

Finally, it can be concluded that knowing and deepening our understanding of the relationship between Terrorism and Cyber Warfare may be necessary in a world where political, economic and military ties are becoming increasingly complex. It is just as important to understand how IW develops, bearing in mind the above relationship. This way, we can improve our control of the narrative and avoid strengthening groups that resort to violence and disregard Human Rights.

Works cited

Akpan, I. U, 2007. *Terrorismo: a nova guerra*. Senior research paper. Rio de Janeiro. ECEME:

Alberts, D. Garstka, J. Stein, F, 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington DC: CCRP. [Online]. Retrieved from: http://www.au.af.mil/au/awc/awcgate/ccrp/ncw.pdf. [Accessed 15 Nov 16].

Brasil, 2007. Ministério da Defesa. MD35-G-01 - Glossário das Forças Armadas. Brasília.

Brasil, 2010. Presidência da República. Gabinete de Segurança Institucional. *Livro Verde: Segurança Cibernética no Brasil*. Brasília.

Brasil, 2012. Ministério da Defesa. *Livro Branco de Defesa Nacional*. Brasília.

Brasil, 2014. *Estado-Maior do Exército. EB 20-MC-10.213, Operações de Informação*. 1st Ed. Brasília.

Brasil, 2014a. *Estado-Maior do Exército. EB 20-MF-10.102. Doutrina Militar Terrestre. 1st Ed*. Brasília.

Clarcke, R; Knake, R K, 2015. *Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito*. Rio de Janeiro: Brasport.

Clausewitz, C. V, 1979. *Da Guerra*. São Paulo. Ed: Martins Fontes.

Fontenele, M. P, 2008. *Proposta de Taxionomia da Guerra de Informação e das Operações de Informação*. Centro de Instrução de Guerra Eletrônica, Brasília, DF. [Online]. Retrieved from: http://www.ccomgex.eb.mil.br/cige/sent_colina/9_edicao_abr_10/index/Art_Maj_Fontenele.pdf [Accessed 02 Nov 16].

Giel, D. J, 2014. *The tragedy of Beslan 2004:Was this event a turning point in Russia's approach to counter – terrorism?* The Netherlands, The Universiteit Leiden. [Online]. Retrieved from: https://openaccess.leidenuniv.nl/bitstream/handle/1887/33671/Beslan%20Thesis%20DJG.pdf?sequence=1. [Accessed 02 Dec 16].

Graham, M. A, 2016. *Força Cibernética dos EUA*. Military Review. [Online]. Retrieved from: https://www.joomag.com/magazine/military-review-edi%C3%A7%C3%A3o-Brasileira-julho-setembro-016/0209296001465490873. [Accessed 30 Nov 2016].

Haeni, R. E, 1997. *Information Warfare an Introduction*. The George Washington University, Cyberspace Policy Institute. [Online]. Retrieved from: http://www.trinity.edu/rjensen/infowar.pdf . [Accessed 18 Nov 16].

Kissinger, H, 2015. *Ordem Mundial*. Rio de Janeiro: Objetiva.

Liang, Q; Xiangsui, W, 1999. *A Guerra Além dos Limites: Conjecturas sobre a Guerra e a Tática na Era da Globalização*. Beijing: PLA Literature and Arts Publishing house.

Marighella, C, 1967. *Mini-manual do Guerrilheiro Urbano*. [Online]. Retrieved from: http://Brasil.indymedia.org/media/2008/06/422822.pdf. [Accessed 30 Nov 16].

Militão, O. P, 2014. *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional*. Master's dissertation in Political Science and International Relations, specialisation in International Relations Lisbon: Universidade Nova de Lisboa. [Online]. Retrieved from: https://run.unl.pt/bitstream/10362/14300/1/Dissertacao_OMilitao_35664.pdf. [Accessed 01 Dec 2016].

Napoleoni, L. *A,* 2015. *Fênix Islamista: O Estado Islâmico e a Reconfiguração do Oriente Médio*. Rio de Janeiro: Bertrand Brasil.

Nunes, L. A. R, 2010. *Guerra Cibernética: está a MB preparada para enfrentá-la?* Senior research paper. Rio de Janeiro: EGN.

Simioni, A. A. C, 2008. *O terrorismo contemporâneo: consequências para a segurança e Defesa do Brasil*. Master's dissertation in History. [Online]. Retrieved from: http://livros01.livrosgratis.com.br/cp090607.pdf. [Accessed 10 Nov 16].

Teixeira da Silva, F. C, 2001. *O Brasil na crise internacional*. Text presented at the Symposium "Análise e consequências do ato terrorista ocorrido nos EUA, em 11 de setembro de 2001". Escola de Guerra Naval.

Walzer, M, 2003. *Guerras Justas e Injustas: uma argumentação moral com exemplos históricos*. São Paulo: Martins Fontes.

Whittaker, D. J. (Org), 2005. *Terrorismo: um retrato*. Rio de Janeiro. Biblioteca do Exército.

Wunderlich, C, 2012. A. *Guerras Assimétricas e Terrorismo: adequabilidade da resposta Brasileira ao fenômeno*. Senior research paper. Rio de Janeiro: ESG.

Visacro, A, 2009. *Guerra Irregular: terrorismo, guerrilha e movimentos de resistência ao longo da história*. São Paulo. Ed. Contexto.