Artigo recebido em fevereiro de 2017 e aceite para publicação em maio de 2017

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

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

Dardano do Nascimento Mota
Major de Comunicações
Escola de Comando e Estado-Maior do Exército
22290-270 Rio de Janeiro, Brasil
dardanomota@yahoo.com.br

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.

Como citar este artigo: Mota, D., 2017. Uma conceção da relação entre o terrorismo e a guerra cibernética no contexto da guerra de informação. *Revista de Ciências Militares*, maio de 2017 V (1), pp. 65-89.
Disponível em: http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes.

Abstract

The present article intends to present an analysis on the possible relation between Terrorism and the Cyber War in the context of the War of Information. In order to reach the proposed objective, the development of the present work is subdivided into the following sections: preliminary considerations; The Information War with its main concepts; The Cyber War where the aspects related to the GI will be detailed; An overview of modern Terrorism; Integral considerations of the article (state of the art); And, finally, a proposal on how the relationship between terrorism and Cyber War would be structured in the context of the Information War. The article presents basic concepts related to Terrorism, Cyberwarfare and Information Warfare, in order to facilitate the understanding of the analysis developed. For this, it uses bibliographical and documentary research, prioritizing the studies related to the subject matter. From the verification of the relationship between Terrorism and Cyberwar, the concreteness of Cyberterrorism is analyzed as an important aspect of this relationship, employing Deductive Reasoning as a tool. Finally, the present article sought to find conclusions about this, pointing out, among them, for the future structuring of an Information Warfare Command.

Keywords: *Information Warfare, Terrorism, Cyberwarfare, Cyberterrorism.*

1. Introdução

"A força, para opor-se à força oponente, mune-se de invenções da arte e da ciência". *Clausewitz*, ao apresentar a referida assertiva em sua obra "Da Guerra", visualizou a importância da tecnologia para o êxito em combate.

Atualmente, o trâmite de dados, por seu volume e variedade de fontes, está baseado, maioritariamente, em estruturas de Tecnologia da Informação[1] (TI). Isso tem feito crescer a nossa dependência nas tecnologias digitais.

Nesse cenário, estamos a presenciar o aumento de conflitos assimétricos[2] e da Guerra Irregular[3], os quais estão a ocupar espaços cada vez mais relevantes no concerto internacional. Nesse contexto, o terrorismo está a se constituir na solução de grupos que discordam do *status quo*. Isso também tem contribuído para aumentar as incertezas e o medo em várias partes do mundo.

[1] Conjunto de dispositivos individuais, como hardware, software, telecomunicações ou qualquer outra tecnologia que, faça parte ou gere tratamento da informação ou, ainda, que a contenha. Disponível em: http://www.convibra.com.br/upload/paper/adm/adm_3123.pdf.

[2] Todo e qualquer tipo de conflito bélico em que, - pelo menos em algum momento -, a superioridade militar (e, particularmente, tecnológica) de um dos contendores resta evidente no Campo de Batalha. Disponível em: http://www.scielo.br/pdf/his/v29n2/v29n2a09.pdf.

[3] Conflito conduzido por uma força que não dispõe de organização militar formal e, sobretudo, de legitimidade jurídica institucional. Disponível em: http://www.eceme.ensino.eb.br/images/IMM/producao_cientifica/dissertacoes/marcelo-bastos-de-souza.pdf.

Essa realidade, complexa e difusa, nos remete à chamada "Guerra de 4.ª Geração" que, segundo Wunderlich (2012, p. 7), consiste em "um conflito multidimensional, a envolver ações terrestres, fluviais, marítimas, aéreas, espaciais, ou ainda no espectro eletromagnético e no ciberespaço".

O mesmo autor acrescenta que "nessa atual e desafiadora conjuntura estratégica, o inimigo pode ser tanto um Estado independente, uma coligação de Estados, como também um grupo terrorista ou uma organização criminosa qualquer".

Nessa realidade de transformações políticas e sociais, também podemos observar uma constante mudança de valores. Esse processo, motivado pela tecnologia e variados interesses, tem demonstrado a volatilidade de estruturas econômicas e políticas. Tomando por base essa tendência, a velocidade de transmissão da Informação e o alcance global que os dados têm alcançado tem possibilitado um maior estreitamento das relações humanas. A principal plataforma por onde isso ocorre é a *Internet*.

A *Internet* influenciou nos últimos anos o nosso modo de viver. Segundo Nunes (2010, p. 10) "os grandes sistemas que gerenciam os dados estão, de algum modo, ao alcance de todos por meio da *Internet*. Dados de todos os tipos passam a trafegar pela grande rede, incluindo os sigilosos".

Somado a isso, a facilidade de manuseio da Internet, materializada em diferentes meios, como os *tablets* e *smartphones* lhe proporcionaram uma portabilidade e alcance sem precedentes. Isso contribuiu para o fortalecimento da chamada "Sociedade da Informação". Relativamente a esse conceito, o Livro Verde de Defesa brasileiro (2010, p. 14) afirma que "na nova conformação dessa Sociedade, vale destacar o aumento das ameaças e das vulnerabilidades de segurança cibernética e os ambientes cada vez mais complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças".

A citação acima apresentada, ratifica a perceção de que estamos inseridos em uma realidade marcada por complexidade, rapidez e grande quantidade de dados. Isso tem demandado capacidades cada vez mais específicas para a operação dos meios de TI.

Paralelamente, as disputas por poder e influência estão a se acirrar. Isso tem intensificado o emprego das redes sociais, da imprensa digital e dos diversos meios de comunicações para a difusão de ideias dos mais variados grupos, inclusive armados.

Nesse universo, existem organizações terroristas que se utilizam amplamente do uso dos meios de TI para a consecução de seus objetivos. Dentre elas, temos o Estado Islâmico (DAESH), no qual "a propaganda ideológica é uma atividade que envolve alta tecnologia, administrada por profissionais qualificados, incluindo alguns ocidentais com alto nível de instrução" (Napoleoni, 2015, p. 57). Como exemplo disso, "quando as redes sociais tiraram o vídeo do DAESH contendo a decapitação de *James Foley*, em poucas horas a equipe de propaganda do grupo terrorista havia restaurado o acesso ao vídeo através de *sites* de aliados mantidos no exterior" (Napoleoni, 2015, p. 57).

Existem grupos de *hackers*, como o Exército Eletrônico Sírio[4] (SEA, sigla em inglês) que estão a mostrar suas capacidades pelos ataques cibernéticos contra veículos das media ou a agências estatais, em defesa do governo de Bashar Al Assad. Isso tem reforçado a ideia de que os Estados e a iniciativa privada precisarão estar cada vez mais aptos a conduzir conflitos cibernéticos.

Assumindo o cenário acima apresentado, o Livro Branco de Defesa Nacional do Brasil afirma que "outros desafios que se apresentam ao país se referem à sua capacidade lidar com os chamados 'conflitos do futuro'. Dentre eles podemos destacar as **guerras de Informação** e os conflitos de pequena escala caracterizados por sua origem indeterminada e estruturas de comando e controlo difusas **que operam com o emprego de redes sociais**". (Brasil, 2012, p. 28) (negrito nosso).

A Guerra de Informação envolve não apenas países com histórico recente de conflitos. Ela está presente em um mundo cada vez mais interconectado e com indicadores sociais, econômicos e políticos dinâmicos.

Esse artigo tem por objetivo principal apresentar uma conceção de como o Terrorismo e a Guerra Cibernética podem se relacionar no contexto da Guerra de Informação, destacando suas consequências e enfatizando, particularmente, o ciberterrorismo.

A metodologia utilizada se constituiu em uma abordagem qualitativa que passou por uma fase de pesquisa bibliográfica e documental com o objetivo de atestar, de forma clara, uma conceção do relacionamento entre o Terrorismo e a Guerra Cibernética. Desse mote, considerando ser esse um assunto relativamente recente e amplo, buscamos relacionar terrorismo e guerra cibernética com os conceitos de Guerra de Informação.

O desenvolvimento desse estudo (além desta introdução e da conclusão) está dividido em seis secções: a primeira apresentará as considerações preliminares; a segunda objetivará a Guerra de Informação (GI) com seus principais conceitos; a terceira tratará da Guerra Cibernética (GC), onde serão detalhados os aspetos que a relacionam com a GI; a quarta abordará, em linhas gerais, o Terrorismo moderno; a quinta tem por objetivo apresentar as considerações integradoras (estado da arte) do artigo; e a última buscará apresentar uma proposta de como estaria estruturada a relação do Terrorismo com a GC no contexto da GI.

2. A Guerra de Informação, a Guerra Cibernética e o Terrorismo

A Guerra é um tema transversal à evolução da Humanidade. Ela vem ganhando em complexidade. Compreender a sua dinâmica demanda conhecimentos adjacentes a ela e, ao mesmo tempo, interligados entre si.

[4] O governo sírio para se opor aos seus adversários na Guerra Civil que assola a Síria desde 2012, instituiu o Exército Eletrônico Sírio que não apenas exerce suas atividades de defesa e segurança cibernética, mas também exerce atividades midiáticas que tentam demonstrar a ilegitimidade e a radicalização dos opositores. Disponível em: 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

Esses conhecimentos envolvem campos do poder como o econômico, o militar e o político. Nesse escopo, a 2.ª Guerra Mundial (1939-1945) e a Guerra Fria (1949-1989) não só entraram para a História, mas também influenciaram o curso das relações internacionais no século XX.

No século XXI, alguns conflitos apresentaram não somente o escopo supracitado, mas também uma particularidade comum: o terrorismo como uma de suas justificativas. Walzer (2010, p. 336) assinala que "na guerra, o terrorismo é um modo de evitar o combate direto com o exército inimigo. Ele representa uma forma extrema da estratégia da 'abordagem indireta'"[5].

O terrorismo de hoje está associado a conflitos em larga escala. Como exemplo, os atentados de 11 de setembro de 2001 contribuíram para que os Estados Unidos da América (EUA) invadissem o Afeganistão em 2002. Da mesma forma, empregando a retórica de "Eixo do Mal"[6] e de armas de destruição em massa, o governo Bush (2001- 2009) criou um pretexto para invadir o Iraque em 2003.

Como se pode observar, o terrorismo tornou-se uma das principais justificativas para guerras que envolveram muitos recursos e vitimaram milhares de vidas. Essa afirmativa ratifica a importância do tema proposto, dada a sua capacidade de catalisar esforços em âmbito internacional.

Paralelamente a isso, o mundo tem testemunhado os ataques cibernéticos, os quais estão a se constituir numa realidade na qual a Tecnologia da Informação pode ser usada como uma arma de grande poder, inclusive em possíveis conflitos assimétricos.

Um caso que ilustra essa ideia está na relação entre China e EUA quando observamos a sua disputa de poder no ciberespaço[7]. Quanto a isso, Clarcke e Knake (2015, p. 45) afirmam que "no final dos anos 1990, os estrategistas chineses convergiram para a ideia de que a Guerra Cibernética poderia ser usada pela China para compensar suas deficiências qualitativas militares em relação aos Estados Unidos".

Ao considerarmos uma conjuntura de ameaças, na qual o terrorismo vem se expandindo e a Guerra Cibernética tem ganhado importância, é lícito que busquemos entender quais relações existem entre esses temas. Partindo dessa ideia podemos formular alguns questionamentos que nortearão o presente trabalho:

1. Quais são os principais pontos de intersecção entre a Guerra Cibernética e o Terrorismo?
2. Qual seria a materialidade do ciberterrorismo?
3. Existem defesas eficazes contra essa ameaça?
4. Os terroristas e os "cibercriminosos" podem atuar conjuntamente?

[5] A Estratégia de ação indireta (concebida por Lidell Hart) procura tirar o máximo proveito da mobilidade, da velocidade e da surpresa oferecidas pela tecnologia militar moderna para desequilibrar a estrutura do dispositivo inimigo. Disponível: http://www.esg.br/images/Revista_e_Cadernos/Cadernos/CEE-012.pdf.

[6] Grupo compreendido por Irã, Iraque e Coréia do Norte. Esses países eram acusados pelos Estados Unidos da América de serem os principais financiadores do terrorismo internacional

[7] Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde a informação digital transita, é processada e/ou armazenada (BRASIL, 2014a, p. 18/36,).

5. Como as relações entre a Guerra Cibernética e o Terrorismo estariam inseridas no contexto da Guerra de Informação? E quais seriam as suas prováveis consequências?

A resposta ao último questionamento se constitui na ideia chave da presente reflexão integradora. É necessário, portanto, que sejam apresentados os principais aspectos referentes à Guerra de Informação, à Guerra Cibernética e ao Terrorismo, antes de detalhar os pontos que respondem ao último questionamento.

Dada a amplitude do assunto ora proposto, as linhas de pensamento para a presente análise estarão baseadas em três vetores: econômico, político e militar.

2.1. A Guerra de Informação (GI)

A GI se constitui no núcleo do presente trabalho. Contudo, antes de abordá-la, é importante apresentar três conceitos que a estruturam e estão interligados entre si.

O primeiro deles consiste no que vem a ser Informação. Ela corresponde "à representação inteligível de objetos, estados e acontecimentos nos domínios real, virtual e subjetivo, integrando processos para a construção do conhecimento, o que promove a compreensão do ambiente operacional" (Brasil, 2014, pp. 4-17).

A Dimensão Informacional, o nosso segundo conceito, diz respeito "ao conjunto de indivíduos, organizações e sistemas no qual os tomadores de decisão são utilizados para obter, produzir, difundir e atuar sobre a informação" (Brasil, 2014, pp. 2-3).

E, como último conceito, temos a chamada Superioridade de Informações que é traduzida como:

> "Uma **vantagem operativa** advinda da habilidade de reunir, processar, difundir, explorar e preservar um **fluxo ininterrupto de informações** aos comandantes em todos os escalões, ao mesmo tempo em que se busca tirar vantagem das informações do oponente e/ou negar-lhe essas habilidades. É possuir mais e melhores informações do que o adversário sobre o ambiente operacional. **Permite o domínio da dimensão informacional** (espectros eletromagnético, cibernético e outros) **por determinado tempo e lugar**" (Brasil, 2014, p. 3-2).

Dadas essas definições, podemos afirmar que os meios de TI são necessários para o manuseio e armazenamento da Informação. Eles contribuem para que esta seja oportuna e de relevância na dimensão informacional. Somado a isso, a gestão da informação é fundamental para que possa ser assegurada a Superioridade de Informação.

Conjuntamente a esses aspetos e, considerando a expansão quantitativa e qualitativa dos meios de TI, com números crescentes de pessoas com acesso à *Internet* (Figura 1) e dotadas de perfis em redes sociais (Figura 2), podemos afirmar que vivemos em uma realidade cada vez mais "informacional e digitalizada".

	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

Figura 1 – Quadro de domínios de Internet por regiões do mundo

Fonte: Relatório da União Internacional de Telecomunicações[8].

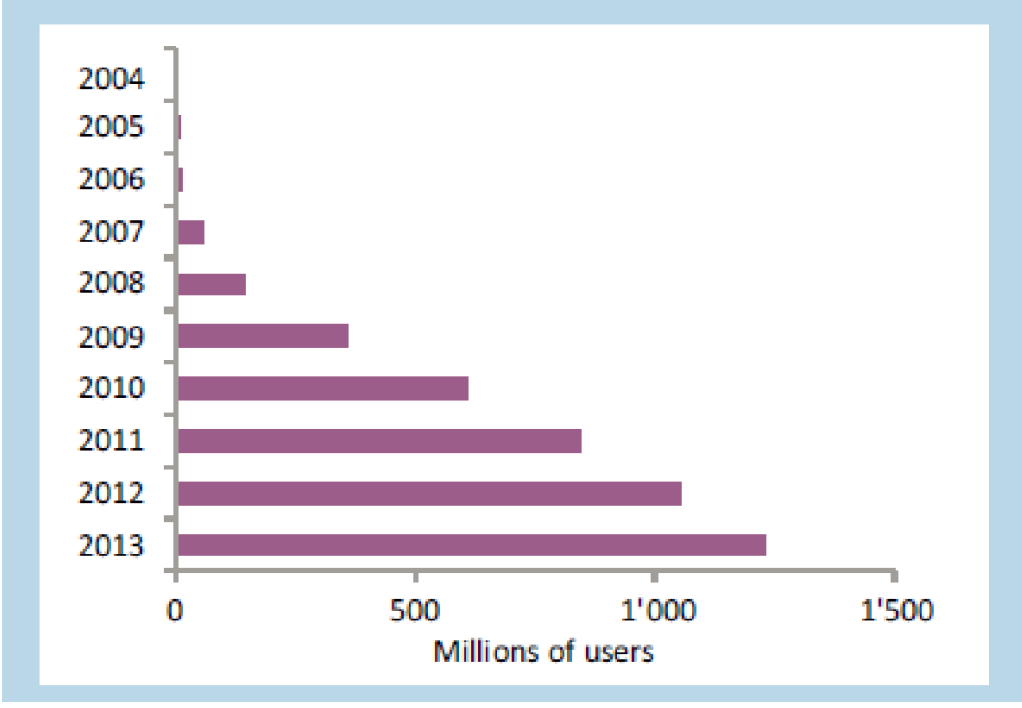

Figura 2 – Gráfico de crescimento dos usuários do Facebook (2004 – 2013)

Fonte: Relatório da União Internacional de Telecomunicações[9].

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

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

Isso posto, chegamos à Guerra de Informação (GI). Esse assunto é vasto em suas literaturas, o que contribui para variadas definições sobre ele. A sua abordagem veio a se expandir após a 1.ª Guerra do Golfo (1991).

Em um primeiro momento, podemos afirmar que a Guerra de Informação consiste "em ações de negação, exploração ou destruição das estruturas de informação do adversário, também adotando condutas para contrariar essas ações quando provenientes do adversário, e expandindo as próprias capacidades de gestão de informação" (Militão, 2014, p. 9). Apresentando uma visão complementar, Haeni (1997, p. 3) a define como:

> *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.*[10]

Baseado nisso, pode-se visualizar que a GI tem como objetivo principal, alcançar um estado de Superioridade de Informação, conforme define o Ministério da Defesa brasileiro:

> Guerra de Informação – **Conjunto de ações destinadas a obter a superioridade das informações**, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos. (Brasil, 2007, pp. 124; 274) (Negrito nosso)

Trata-se de um importante conceito, pois a Superioridade de Informação se constitui em condição *sine qua non* para o êxito na Guerra de Informação. Um dos modelos mais aceites para a Superioridade de Informação é apresentado por Alberts, em sua obra NCW, e está representada na Figura 3.

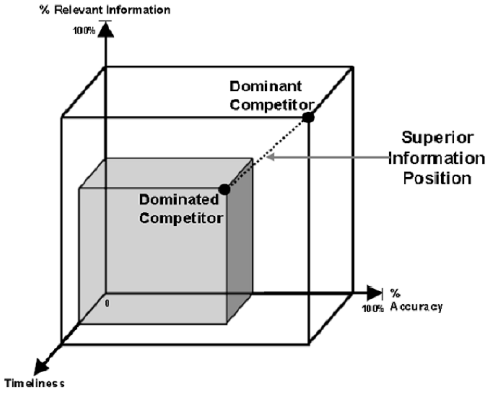

Figura 3 – Modelo Conceitual de Superioridade de Informação
Fonte: (Alberts, Garstka e Stein, 1999, p. 34).

[10] Ações tomadas para alcançar a superioridade da informação ao afetar a informação adversa, os processos baseados na informação, os sistemas de informação e as redes baseadas em computador, ao mesmo tempo em que se defendem as próprias informações, processos baseados na informação, sistemas de informação e redes computacionais.

Na Figura 3, identifica-se a presença de dois contendores: "o competidor dominante" e o "competidor dominado". Nesse modelo, é importante destacar que a Superioridade de Informação não está indefinidamente assegurada no tempo. Isso quer dizer que o "grupo dominador" pode passar à situação de "grupo dominado" e vice-versa.

Essa inversão dependerá, dentre outros fatores, dos meios empregados na coleta e tratamento da Informação, particularmente do fator humano, principalmente no que se refere à sua capacidade técnica e motivação para prosseguir em suas ações. Isso poderá proporcionar o "controlo da narrativa".

Além dessa dicotomia, ilustrada pelo embate entre o "grupo dominador" e o "grupo dominado", a GI, dentre as suas subdivisões, está fracionada em duas formas: Ofensiva e Defensiva. Dada essa divisão, pode-se observar que, em sua primeira forma, busca-se a informação através da exploração não autorizada de sistemas. Na segunda (defensiva) o foco está na prevenção, através da monitorização e acesso à informação disponível de terceiros (Militão, 2014, p. 40).

A linha de pensamento adotada até aqui nos possibilita afirmar que a GI envolve, em grande medida, estruturas de TI. Elas proverão os "caminhos" por onde passará as informações que alimentarão os sistemas de informação, tanto na sua forma Ofensiva quanto na Defensiva.

Igualmente, as estruturas de TI comporão as bases por onde se desenvolve a Guerra Cibernética, um dos temas que será abordado à frente. Contudo, é importante ressaltar que a Guerra de Informação não está circunscrita somente aos meios de TI. Segundo Stein[11] (1995):

> A guerra de informação pode ser vista como um conflito de nível social, ou de nação contra nação, conduzido em parte através de meios de informação e de comunicação em rede de interconexão mundial (...) A guerra de informação, por conseguinte, pode definir a guerra futura ou, dito de outro modo, ser o foco central do pensamento sobre o conflito no futuro.

O mesmo Stein (1995) complementa a sua ideia ressaltando que "ainda que a guerra de informação venha a ser conduzida em larga medida, mas não integralmente, através das redes de comunicação de uma sociedade ou de suas forças armadas, ela não se resume a satélites, fiação e computadores. Ela objetiva influenciar os seres humanos e as suas decisões".

Assim, ao enquadrar as principais ameaças no contexto da GI, Stein (1995) destaca a proliferação de atores não estatais como os "terroristas com acesso a redes de computador e de comunicações de âmbito mundial, **a ponto de influenciarem**, trocarem informação ou coordenarem ações políticas em bases globais" (negrito nosso). Isso corrobora a importância do controlo da narrativa. Sem ele, não haverá legitimidade[12], ainda que esteja assegurada pela Superioridade de Informação.

---

[11] Dr George J. Stein (Bacharelato, Assumption College; Mestrado em Artes, Pennsylvania State University; Doutorado, Indiana University). Disponível em: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-p/1995/3tri95/pstein.html.

[12] Caracterizada pela necessidade de atuar conforme diplomas legais, mandatos e compromissos assumidos pelo Estado (Brasil, 2014a, p. 5-5)

Por esta razão, deter a narrativa dominante pode ser considerado um ponto decisivo nas operações militares atuais, já que perdê-la pode até mesmo restringir a liberdade de ação no campo de batalha, vindo a influenciar, inclusive, as ações no ciberespaço.

Dada a abrangência da GI e suas ameaças, é lícito concluir, ainda que parcialmente, que temas como a Guerra Cibernética e o Terrorismo podem estar inseridos em seu contexto. Porém, antes de estabelecermos como ocorre o relacionamento entre esses assuntos, é necessário explorá-los isoladamente.

2.2. Guerra Cibernética

O ciberespaço não está limitado por fronteiras geopolíticas. Nesse campo, as operações cibernéticas implicarão em grande flexibilidade e rapidez sendo que as decisões, por esta razão, poderão perder a oportunidade. Corroborando essas ideias, Clarcke e Knake (2015, p. 41) afirmam que "a necessidade de tomar a iniciativa, em parte é determinada pelo facto de que as ações tomadas no ciberespaço se movem em um ritmo nunca antes visto em guerras".

É nas entrelinhas da supracitada citação que está inserida a Guerra Cibernética. De acordo com o Livro Verde de Defesa Nacional brasileiro (2010, p. 23), ela consiste em "um conjunto de ações ofensivas e defensivas de informações e sistemas de informação para negar, explorar ou destruir os sistemas de informação inimigos. Visa vantagens tanto militares quanto civis".

Para que as referidas vantagens possam ser obtidas, o principal meio utilizado pela GC tem sido a *Internet*. Por esse meio, transitarão os *botnets*[13] e os *worms*[14] com o objetivo de angariar superioridade no ciberespaço, o que poderá refletir-se nos campos político, econômico e militar.

Isso posto, nos últimos anos, a importância da GC vem crescendo, dada a sua capacidade de atacar sistemas bancários, governamentais e de defesa, dentre outros. Isso tem motivado a criação de órgãos estatais com o objetivo de atuar no ambiente cibernético.

Para ilustrar essa realidade, serão apresentados os exemplos de três nações que estão a investir grandes recursos (financeiros, humanos e tecnológicos) em suas estruturas de Guerra Cibernética: Rússia, China e Coreia do Norte. Esses países, por razões distintas, têm demonstrado parte de suas capacidades, através da execução de ataques cibernéticos com fins políticos, econômicos e militares.

Do ponto de vista político, a Rússia está a fazer uso de suas ferramentas cibernéticas como instrumentos de imposição de poder e influência. Isso ficou evidenciado nos ataques cibernéticos DDoS[15] sobre a Estónia (um dos países mais conectados à *Internet* no mundo)

[13] Rede de computadores forçada a operar sob comandos de um usuário remoto não autorizado, geralmente sem o conhecimento de seu dono ou operador (Clarcke e Knake, 2015, p. 224).

[14] *Software* malicioso que força computadores ou redes a fazer coisas que seus donos ou usuários não fariam (Clarcke e Knake, 2015, p. 224).

[15] Ataque Distribuído de Negação de Serviço: técnica básica de guerra cibernética utilizada por criminosos e outros personagens não estatais em que um site da Internet, um servidor ou um roteador é inundado com mais solicitações de pacotes que o site pode responder ou processar (Clarcke e Knake, 2015, p. 223).

em 2007. Esse país teve uma significativa parcela de seus sistemas informáticos postos abaixo, quando os servidores que hospedavam as suas páginas mais utilizadas foram sobrecarregados com pedidos de acesso. "Isso fez com que estes entrassem em colapso a ponto de deixarem de funcionar e ficarem inacessíveis. Os estonianos não podiam acessar seus bancos *on line*, os *sites* de seus jornais ou os serviços eletrónicos do governo". (Clarcke e Knake, 2015, p. 16).

No campo econômico, *hackers* chineses têm buscado adquirir os códigos-fonte de empresas multinacionais. Clarcke e Knake (2015, p. 53) afirmam, conforme a citação a seguir, que essa aquisição tem impulsionado o desenvolvimento de novas tecnologias na China:

> Quando os cientistas do Google descobriram o que estava acontecendo (...) conseguiram rastrear a invasão até um servidor em Taiwan, onde encontraram cópias de suas informações proprietárias e de pelo menos mais vinte outras empresas, incluindo Adobe, Dow Chemical e a empresa de defesa Northorp Grumman.

Diferentemente da Rússia e da China, a Coreia do Norte disponibiliza serviços de *Internet* apenas para uma pequena parcela de sua população. Paradoxalmente, essa realidade não tem impedido que este país investisse em sua infraestrutura de Guerra Cibernética como uma ferramenta de projeção de seu poder militar. Isso pode ser constatado a seguir:

> O Departamento Secreto para Guerra Psicológica e Cibernética Inimiga, Unidade 204, **possui cem *hackers* e é especializada em elementos cibernéticos para guerra de informação**. (...) A Unidade 121 é especializada em desabilitar as redes de comunicação, comando e controlo militares da Coréia do Sul. (Clarcke e Knack, 2015, p. 27) (negrito nosso)

Pelo exposto, pode-se depreender que o manuseio da Informação em um contexto de GC se constitui em um ponto comum entre as três nações citadas. Isso se confirma pelo facto de a Guerra Cibernética estar relacionada à Guerra de Informação pela busca em se construir um ambiente de superioridade informacional através do emprego de redes de computadores.

Entretanto, para que isso se realize, é necessário que o ciberespaço apresente suas fragilidades. Uma delas, e que facilita as ações dos hackers, se deve a algo que ainda não foi apropriadamente dimensionado: as vulnerabilidades da *Internet*.

Dentro desse cenário, Clarcke e Knake (2015, p. 72) afirmam que "era esperado que existissem vulnerabilidades em algo tão grande. Hoje, a *Internet* tem crescido tão extensivamente que começa a ficar 'sem endereços'". Dessa maneira, dada a amplitude da *Internet*, é necessário caracterizar algumas de suas fragilidades.

A primeira está no facto de grande parte do tráfego de dados ocorrerem "abertamente", ou seja, sem criptografia[16]. "Atualmente muitos *sites* (mas não a maioria) usam a conexão segura quando se faz o *logon*. Entretanto, devido ao custo e à velocidade, depois que a

[16] Codificação de uma informação de modo a torná-la ilegível para quem não possuir a chave de decodificação (Clarcke e Knake, 2015, p. 224).

senha foi transmitida, muitos deles retornam à conexão em seu modo inseguro" (Clarcke e Knake, 2015, p. 69).

A segunda vulnerabilidade está na facilidade de propagação de tráfego malicioso para atacar computadores. Eles podem transitar pela *Internet* com pouca fiscalização. "A maioria dos provedores de serviço sequer tomam os cuidados básicos, em parte pelos custos e pela lentidão do sistema e igualmente por questões de privacidade" (Clarcke e Knake, 2015, p. 70).

Igualmente importante, a terceira vulnerabilidade é a arquitetura descentralizada da *Internet*. Isso se deve ao facto de os seus desenvolvedores, quando a projetaram, "terem priorizado a descentralização e não a segurança do sistema" (Clarcke e Knake, 2015, p. 70).

Em que pese tudo isso, os meios empregados na Guerra Cibernética não se restringem somente à exploração dos gaps da *Internet*. Os vírus, bombas lógicas[17] e *hackers* também podem atuar para fins de caráter não estatal. Essa outra possibilidade pode ser observada a seguir:

> Da mesma forma que alguém pode chegar pelo ciberespaço e destruir uma linha de transmissão elétrica ou um gerador, comandos por computadores podem descarrilar um trem, enviar vagões de carga para um lugar errado ou fazer com que um gasoduto exploda. Enviar comandos computacionais para um sistema de armas pode fazer com que ele funcione incorretamente ou que seja desligado. Então, um guerreiro cibernético pode, a partir do ciberespaço, provocar ações para desligar ou explodir coisas, como uma rede elétrica ou um milhão de outros sistemas críticos, como o armamento de um oponente. (Clarcke e Knake, 2015, p. 85).

Dessa maneira, ao considerarmos as chamadas infraestruturas críticas[18], podemos afirmar que elas se constituem em importantes alvos da Guerra Cibernética. Isso se deve, por exemplo, ao impacto sócio econômico que uma eventual paralisação de estruturas de abastecimento de energia, poderia ocasionar a parques industriais de cidades como Chicago ou Pequim.

Diante disso, emergem dois pontos que na GC podem estar ligados: a opinião pública e a atribuição de autoria do ataque cibernético. Partindo dessa ideia, podemos considerar que ataques cibernéticos que impactam infraestruturas críticas também influenciariam a opinião pública. Entretanto, em que medida tal influência poderia ocorrer?

Clarcke e Knake (2015, p. 173) afirmam que "quando se trata de descobrir quem atacou você, a menos que você esteja situado na rede que o atacante está utilizando e esteja visualizando o ataque, é difícil saber quem é o atacante". Essa dificuldade de identificação da procedência do ataque cibernético pode criar "opiniões públicas" variadas quanto a quem corresponderia

[17] Códigos maliciosos

[18] Instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (Brasil, 2014a, p. 19/36).

a sua autoria. Isso poderia mudar se o atacante assumisse a responsabilidade pelo ataque, o que geraria uma nova opinião pública, provavelmente mais homogênea.

Somando-se a isso e, a observar esse cenário de incerteza, é importante ressaltar que, diferentemente das Guerras Convencional e Não-Convencional[19], a GC também envolve questões ligadas à iniciativa privada. Isso engloba empresas que são avessas às regulações que os Estados desejam impor.

Nesse campo, é oportuno destacar que as regulações estatais estão relacionadas à Defesa Cibernética[20] e, em algumas ocasiões, vão de encontro aos interesses privados, já que podem restringir liberdades ou diminuir lucros de grandes corporações de TI.Neste ponto, torna-se necessário o controlo da narrativa do Estado frente às grandes empresas, no sentido de influenciar a sociedade quanto à premência da segurança digital em detrimento de algumas comodidades[21] oferecidas pela iniciativa privada ao mercado consumidor. Dessa maneira, observando a influência da Economia e da Política sobre a Guerra Cibernética, notam-se quão complexos são os instrumentos para garantir que as infraestruturas críticas não sejam atacadas ciberneticamente.

Em adição a isso, atualmente, um maior desenvolvimento econômico e social tem estado associado à abundância de meios de TI. Isso tem aumentado a dependência tecnológica em todas as expressões do poder e, na mesma proporção, à necessidade de desenvolver estruturas de Defesa Cibernética.

Como exemplo, Clarcke e Knake (2015, p. 119), ao analisarem o atual status norte-americano em Guerra Cibernética afirmam que "**sobre essa questão fundamental de quem é o trabalho de defender a infraestrutura dos EUA diante de uma guerra cibernética**, o governo e a indústria estão passando a bola uns para os outros" (negrito nosso). Como resultado, ninguém está a defender os principais alvos de uma guerra cibernética, pelo menos não nos Estados Unidos.

O exemplo estadunidense atesta que "é mais fácil articular ataques informáticos do que se defender deles, o que encoraja possivelmente uma postura ofensiva na construção de novas capacidades" (Kissinger, 2014, p. 346). O poder dessa citação é notório nos EUA, já que na expressão militar norte-americana, alguns analistas têm proposto a criação de uma Força Cibernética separada das outras quatro Forças Armadas. Segundo Graham (2016, p. 74):

---

[19] Um amplo espectro de operações militares e paramilitares, normalmente de longa duração, predominantemente conduzida através, com ou por forças nativas ou subversivas, organizadas, treinadas, equipadas, apoiadas, e direcionadas em vários graus por fonte externa. Inclui, mas não se limita, a guerra de guerrilhas, subversão, sabotagem, atividades de inteligência, e recuperação assistida não-convencional. Disponível em: http://educaleaks.dominiotemporario.com/doc/Conceitos_Relacionados_a_Guerrilha.pdf

[20] Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planeamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (Brasil, 2014a, p. 18/36).

[21] Se referem à velocidade de transmissão e alcance dos pacotes de dados oferecidos pelas empresas de TI aos usuários.

> O estabelecimento da Força Cibernética, inclusive com o seu próprio membro na Junta de Chefes de Estado-Maior, permitiria que comandantes com profunda experiência no ciberespaço comuniquem efetivamente os desafios da guerra cibernética aos formuladores de políticas. Por sua vez, os chefes da Força Cibernética podem empregar eficientemente a orientação e os recursos destinados às operações militares no ciberespaço.

Assim, conclui-se parcialmente que a atual conjuntura de GC é variada e complexa. Ela perpassa pontos que ligam de forma profunda as esferas governamental e privada. Isso pode ser comprovado, ao observarmos que muitas das chamadas infraestruturas críticas funcionam baseadas na *Internet,* com provedores privados. Entretanto, não há como garantir a sua proteção sem que existam estruturas de Defesa Cibernética robustas. Ainda que elas não garantam total proteção, poderão contribuir para conferir à sociedade o fornecimento de serviços básicos, como o de energia elétrica e de transportes.

Como se pôde observar, essa permeabilidade, promovida pela *Internet*, também impacta os campos político e militar. Neles estão dois atores relevantes na estruturação da Defesa Cibernética, o Governo e as Forças Armadas.

Em que pese o exposto até aqui, é importante abordar o Terrorismo para que possa ser estabelecido, de forma consistente, o teor de sua relação com a Guerra Cibernética em um contexto de Guerra de Informação.

2.3. Um *overview* sobre o Terrorismo moderno

O Terrorismo não é um fenômeno recente. Segundo Teixeira da Silva, historicamente, ele está dividido em "ondas".A "primeira onda" (1880-1914) buscava o apoio popular e era marcadamente anarquista; a "segunda onda" (1945-1974) visava a independência colonial e esteve presente em países como a Argélia e Indonésia (colônias naquela época); a terceira (1975-1985) caracterizou-se por um terrorismo apoiado por Estados-Nação, com um forte viés político, como a Líbia.

Prosseguindo nessa linha de pensamento, encontramo-nos na "quarta onda", que se caracteriza por suas "ações de proporções globais e ilimitadas, com **o emprego de meios não convencionais** que apontam para uma caracterização de suas ações como uma forma de **Guerra Assimétrica**" (Simioni, 2008, p.24).

Ainda que o Terrorismo não seja um fenômeno recente, as ideias que o definem ainda são controversas. Isso nos motiva a apresentar algumas delas com o objetivo de encontrarmos as mais apropriadas a esta reflexão.

Para Walzer (2003, p. 335) o objetivo do Terrorismo consiste "na destruição do moral de uma nação ou de uma classe, em solapar sua solidariedade. Seu método é o assassínio aleatório de pessoas inocentes".

Sob outro ponto de vista, Marighella (1968, p. 1) enaltece a relação entre a violência e o terrorismo, destacando que o último "não divide, pelo contrário, ele representa o centro

da atração. Hoje, ser 'violento' ou um 'terrorista' é uma qualidade que enobrece qualquer pessoa honrada". Whittaker (2005, p. 21), por sua vez e, de forma mais ampla, afirma que:

> O terrorismo, no mais comumente aceite uso contemporâneo do termo, é fundamental e inerentemente político. E está vinculado de forma inextrincável ao poder: a busca, a conquista e o uso do poder para conseguir mudança política. **O terrorismo é, assim, violência – ou, igualmente importante, ameaça de violência** –, usada e direcionada na perseguição de objetivo político ou a seu serviço. (negrito nosso)

Isso posto, ao analisarmos as definições acima, observamos um contraponto: o terrorismo implicaria somente no assassinato de pessoas com fins políticos? É necessário aprofundar mais o assunto para constatarmos, como afirma Whittaker (2005), que o terrorismo também pode estar na ameaça de violência, que causaria intimidação social.

Visacro (2009, p. 283) afirma que "o terrorismo compreende um vasto repertório de atividades que transcende o senso comum. Ele está associado, frequentemente, a um proselitismo demagógico com o intuito de atingir determinados objetivos psicológicos".

Pelo exposto, identificamos duas ideias. A primeira: o terrorismo tem na violência a sua principal ferramenta para ser bem-sucedido; e a segunda: o terrorismo abrange variantes que, por sua capacidade de promover intimidação, visam atingir, em última instância, objetivos políticos. Assim, partindo das duas ideias levantadas, passaremos a analisar algumas das peculiaridades do terrorismo.

No que tange à primeira ideia, o terrorismo, nos últimos anos, tem sido pautado pela violência indiscriminada. De acordo com o relatório do *Institute for Economics and Peace*[22], no ano 2000 aproximadamente 5.000 pessoas morreram vítimas de atentados terroristas. Em 2014, pouco mais de 30.000.

Walzer (2005, p. 347) corrobora essa afirmação ao destacar que o terror "é a forma totalitária da guerra e da política. Ele reduz a pó as convenções de guerra e o código político. Desrespeita limites morais além dos quais parece ser impossível qualquer outra limitação". Comprovando essa ideia, uma de suas manifestações foi o Massacre de Beslan, ocorrido em 2004 na Rússia. De acordo com 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*

[22] Tradução: Instituto para a Paz e Economia

> *led to questions about the capability of Russia to prevent and to manage terrorist attacks*[23]

Outra peculiaridade, também baseada na violência, se refere ao seu potencial de alterar configurações geopolíticas. O caso mais conhecido é o praticado pelo Estado Islâmico. Para Napoleoni (2015, p. 52):

> O caráter contemporâneo e o pragmatismo do Estado Islâmico resultam de uma **mistura de estratégias, tecnologia e capacidade de comunicações modernas**, propaganda psicológica, técnicas de guerra à moda antiga e costumes tribais, tais como casamentos arranjados entre mulheres de tribos sunitas e os jihadistas. Visto sob essa perspectiva, está claro que o Estado Islâmico supera em muito os feitos de todos os Estados-fantasmas do passado ou do presente **na construção de nações** e que talvez ele consiga ser bem-sucedido onde todas as organizações armadas do pós-guerra fracassaram: **na criação, dos escombros resultantes de ações de pura violência, de um novo tipo de Estado**, bastante grande, forte e, estrategicamente, suficientemente importante para merecer a atenção do mundo. (negrito nosso)

Ainda abordando a primeira ideia, podemos observar que as organizações terroristas estão a adotar métodos baseados em TI para as suas ações. Isso foi constatado nas medidas de coordenação e controlo empregadas nos atentados terroristas em Mumbai, no ano de 2008. Nessa ocasião, um pequeno grupo, utilizando telemóveis, logrou êxito na execução de atentados que culminaram com a morte de mais de 180 pessoas.

Os atentados de Mumbai demonstraram não só a importância dos meios tecnológicos, mas também de indivíduos com capacidade para explorar suas possibilidades. Isso assegurou um estado de Superioridade de Informação para o qual as autoridades indianas não estavam preparadas para combater.

O DAESH está a empregar meios tecnológicos, especialmente a *Internet*, para recrutar indivíduos. Quanto a isso, Napoleoni (2015, p. 49) afirma que "o crescente número de pessoas que aderem à prática da violência pela propaganda do DAESH confirma o fascínio de sua mensagem: a de que o mundo virtual em que vivemos pode produzir também novos atos de violência irracionais e bárbaros".

Finda a primeira ideia, iniciamos a segunda, destacando outras duas peculiaridades do terrorismo. A primeira delas está no seu poder financeiro, o que tem se refletido na política dos Estados.

---

[23] Tradução: a tragédia de Beslan distingue-se de outros ataques terroristas que ocorreram na história da Federação Russa devido à sua magnitude e complexidade. Em termos de tragédias de tomada de reféns, os ataques terroristas de Budennovsk (1995), Kizlyar (1996) e Dubrovka (2002) também foram atos importantes que ameaçaram a segurança dos russos. No entanto, as principais razões para considerar Beslan um ponto de viragem potencial são o nível extremamente elevado de reféns (1300), mortes (372) e lesões (747), os atos cruéis dos terroristas para crianças e mulheres, a longa duração do cerco (3 dias), a boa preparação dos autores que levaram a graves problemas entre os serviços de segurança responsáveis no momento do cerco, bem como o facto de que Beslan foi um evento de media global que levantou questões sobre a capacidade da Rússia de prevenir e enfrentar ataques terroristas.

Ainda que cada nação lide com essa questão de forma distinta, é indiscutível a sua implicação financeira, o que impõe gastos com segurança. Isso ocorre não só para administrar as consequências de um atentado terrorista, mas também para preveni-lo. A título de exemplo, o Brasil investiu aproximadamente novecentos milhões de euros24 em medidas de antiterrorismo para garantir a segurança dos Jogos Olímpicos Rio 2016.

A segunda peculiaridade está associada àquilo que Visacro (2009, p. 293) afirma que orienta o planeamento das ações terroristas: os media, a opinião pública e os tomadores de decisão. Esse tripé no mundo interconectado em que nos encontramos também está baseado em meios de TI, particularmente na *Internet*.

Complementando essa ideia, Visacro (2009, p. 293) destaca que "o estudo da media e da opinião pública permite estabelecer metas apropriadas. **A análise dos tomadores de decisão é necessária para a definição de como o Estado reagirá à pressão da media e também da opinião pública**" (negrito nosso). Isso implicará no controlo da narrativa que o Estado deverá buscar frente às organizações terroristas.

Pelo exposto, conclui-se parcialmente que: o Terrorismo está a ganhar variantes importantes, associadas à tecnologia; que não existem mais formas de operar o terrorismo de forma exitosa seguindo o mesmo padrão; e que a estrutura que conforma uma organização terrorista evoluiu, inclusive no que se refere aos seus recursos humanos. Além disso, segundo Akpan (2008, p. 47):

- O Terrorismo ficou mais sangrento;
- Os Terroristas estão menos dependentes de patrocinadores dos Estados;
- Os Terroristas evoluíram para novos modelos de organização, capazes de lutar em campanhas globais;
- O mundo vai presenciar mais ciberterrorismo e suicida.

Pelos aspetos apresentados, infere-se que o Terrorismo, a Guerra Cibernética e a Guerra de Informação estão relacionados e essa relação está a se estreitar.

Pelos atentados de Mumbai, se observou que o terrorismo, ainda que pressuponha ação violenta, tem na tecnologia um multiplicador de seu poder de combate potencializado pela Superioridade de Informação, principal objetivo da Guerra de Informação, e que possibilita o sucesso de ações no ambiente da Informação. Essa se constitui em mais uma ideia que sustentará a presente reflexão.

Além disso, a Guerra Cibernética e a Guerra de Informação podem se manifestar nos mais variados campos do Poder. Pode-se observar essa afirmação na confrontação internacional entre potências mundiais como EUA, China e Rússia por recursos financeiros, influência geopolítica e poder militar, tendo por suporte, as redes de computadores.

[24] Fonte: 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

Da mesma forma, o Terrorismo moderno, em suas diversas manifestações, tem buscado atuar sobre a opinião pública, também sendo transversal aos campos político, econômico e militar. Nesse contexto, o DAESH é, hoje, sua manifestação máxima, também inserida na GI.

Isso posto, identificamos, dentre outros, dois pontos de intersecção entre a Guerra Cibernética e o Terrorismo. O primeiro está na atuação sobre a opinião pública e o segundo está no uso de Tecnologias da Informação e Comunicações como ferramentas para expandir seus efeitos. Quanto a esses pontos, Kissinger (2014, p. 346) afirma que:

> Um portátil pode produzir um facto de consequências globais. Um agente solitário dotado de poder informático pode ter acesso ao ciberespaço para desativar ou potencialmente destruir infraestruturas vitais, agindo a partir de uma posição de quase completo anonimato. Redes elétricas podem ser levadas a sofrer pane e usinas de energia desligadas por meio de ações a partir de fora do território físico de uma nação. Um grupo clandestino de hackers já se mostrou capaz de penetrar em redes governamentais e difundir informações sigilosas numa escala grande o bastante para afetar a conduta diplomática.

Pelo exposto, os supracitados pontos de intersecção podem contribuir para que seja construída uma conceção da relação entre o Terrorismo e a Guerra Cibernética, inserida no contexto da Guerra de Informação. Para detalhar essa ideia, no ambiente de informação, cada ponto de intersecção será abordado no tópico a seguir.

1.4. A relação entre o Terrorismo e a Guerra Cibernética

Ao tentarmos visualizar como se relacionam o Terrorismo e a Guerra Cibernética no domínio da Informação, serão analisados os dois pontos de intersecção levantados no tópico anterior. A partir dessa análise será possível constatar a materialidade do relacionamento entre os dois assuntos.

Como visão metodológica para verificar a relação em estudo, esta se baseará em uma abordagem qualitativa focada na pesquisa bibliográfica, documental e na observação, como instrumento de coleta de dados. Além disso, o raciocínio dedutivo será empregado para estruturar um produto do pensamento crítico quanto ao ciberterrorismo. Tudo isso irá possibilitar a construção de argumentos que sustentarão as razões que tornam factível a relação entre a GC e o Terrorismo no contexto da GI.

Dessa forma, é importante apresentarmos algumas considerações relativas à já mencionada "Dimensão Informacional". Podemos afirmar que ela é composta de "três perspetivas inter-relacionadas que interagem continuamente entre si e com indivíduos, organizações e sistemas. Essas perspetivas são: a lógica, a física e a cognitiva". (Brasil, 2014, pp. 2-3).

A perspetiva lógica (não será abordada) corresponde a "onde e como as informações são obtidas, produzidas, armazenadas, protegidas e difundidas. Ela se refere ao exercício do Comando e Controlo das forças militares." (Brasil, 2014, pp. 2-4).

A perspetiva física diz respeito "às plataformas físicas e às redes de comunicações que as conectam. O seu caráter é multinacional." (Brasil, 2014, pp. 2-4).

A perspetiva cognitiva, por sua vez, engloba as mentes dos decisores. "Eles podem ser influenciados por crenças individuais e culturais, normas, vulnerabilidades, motivações, emoções, experiências, costumes, educação, saúde mental, identidades e ideologias" (Brasil, 2014, pp. 2-4). Essas considerações, associadas aos supracitados pontos de intersecção entre o Terrorismo e a Guerra Cibernética, nos permitem construir o Quadro 1.

Quadro 1 - Quadro de Relações entre o Terrorismo e a Guerra Cibernética

Dimensão	Pontos de Intersecção	Terrorismo	Guerra Cibernética
Informacional	Opinião Pública (perspetiva cognitiva)	• Procura chocar e transformá-la pela violência ou simples intimidação pelo uso desta. • É um dos Centros de Gravidade[a)] para as ações terroristas	• Procura influenciar a sociedade apresentando as vulnerabilidades da Internet. • Pode criar uma "multiplicidade de opiniões públicas"
	Amplo emprego de TI (perspetiva física)	• Vem sendo utilizada para coordenar e controlar os agentes terroristas em todo o mundo (Ex: redes sociais).	• Estão ligadas, já que as plataformas de TI são os principais caminhos por onde transitam os *worms* • Conexões globais.

a) Ponto essencial de um Estado, de forças militares ou de sistemas diversos, cujo funcionamento é imprescindível à sobrevivência do conjunto. Os CG não se limitam a forças militares e serve como fonte de energia que fornece força moral ou física, liberdade de ação ou vontade de agir (Brasil, 2014).

Fonte: (Autor).

Isso posto, chegamos aos aspetos (destacados em amarelo) capazes de conferir efetividade à relação entre o Terrorismo e a Guerra Cibernética no contexto da GI. A associação entre eles poderá potencializar os efeitos buscados pelas organizações terroristas.

De posse disso, para que possamos construir uma conceção, do ponto de vista informacional, da relação entre o Terrorismo e a Guerra Cibernética, é necessário apresentar alguns comentários sobre o ciberterror, uma vez que esse assunto pode reunir os aspetos acima destacados.

O ciberterrorismo é um assunto recente e ainda controverso quanto às suas manifestações. Algumas autoridades discordam taxativamente da sua existência. Contudo não negam a possibilidade desse fenômeno vir a se tornar uma realidade, em um futuro próximo.

Clarcke e Knake (2015, p. 112) afirmam, em um primeiro momento, que "o ciberterrorismo é uma pista falsa e, em geral, as duas palavras 'cibernética' e 'terrorismo' não devem ser usadas em conjunto porque elas evocam imagens de Bin Laden fazendo GC de sua caverna". Entretanto, em um segundo momento, os mesmos especialistas destacam que "um grupo terrorista bem financiado pode encontrar um clube de *hackers* altamente qualificado que faria um ataque cibernético em troca de muito dinheiro, mas isso não aconteceu até o momento" (Clarcke e Knake, 2015, p. 127).

Em adição a essas considerações, Liang e Xiangsui (1999) apontam que "da mesma maneira que existem todos os tipos de pessoas em uma sociedade, os *hackers* também existem com as mais diversas índoles e raças. Independentemente de seus valores, escondem-se nas redes, e podem ser: estudantes de nível médio; 'vasculhadores da Internet'; elementos membros frustrados e ressentidos na administração de empresas internacionais; **terroristas experientes** ou mercenários". (negrito nosso)

Respeitando o disposto nas citações acima, destacamos que não é objetivo do presente artigo afirmar que estamos vivendo uma realidade de atentados ciberterroristas. Entretanto, a literatura existente nos permite analisá-lo como uma possível (e importante) ligação entre o Terrorismo e a Guerra Cibernética. Dessa maneira, partiremos de quatro premissas:

1. Os ataques cibernéticos vêm ocorrendo em regiões onde existem meios de TI instalados;
2. O ciberterrorismo é uma forma de ataque cibernético;

Logo, conclui-se que o ciberterrorismo pode ocorrer em quaisquer regiões onde existam meios de TI instalados.

3. O Terrorismo desrespeita os Direitos Humanos;
4. O ciberterrorismo é uma modalidade do terrorismo.

Logo, conclui-se que o ciberterrorismo desrespeita os Direitos Humanos.

Ao considerarmos essas premissas e conclusões, podemos estruturar alguns argumentos. Pode-se observar que a premissa n.º 1 quando ligada à n.º 2 possibilita uma primeira constatação: os ataques cibernéticos, com seu amplo alcance, fazem uso de ferramentas de TI (atualmente espalhadas por grande parte do mundo). Somente isso, configuraria uma ameaça real de ciberterrorismo? Não.

No entanto, ao estendermos o disposto nas duas premissas para a assimetria nos conflitos, pode-se perceber que uma organização terrorista, que busca um máximo efeito e possui "meios de convencimento" (sejam eles ideológicos, religiosos ou mesmo financeiros) para cooptar *hackers*, deterá as condições para executar ações de Ciberterrorismo.

Outra análise que podemos abordar está na conexão direta entre as premissas n.º 3 e 4. Isso pode ser verificado ao considerarmos o "Calcanhar de Aquiles" de determinada organização, seja ela pública ou privada.

Vamos considerar que a *Internet*, por suas vulnerabilidades e por possibilitar a atuação sobre as chamadas infraestruturas críticas seria o supracitado "Calcanhar de Aquiles". Um grupo terrorista desprovido de qualquer preocupação com Direitos Humanos e dotado de *knowhow* cibernético para explorar as referidas fraquezas da *Internet*, poderá executar, por exemplo, ataques cibernéticos sobre estações de controlo de espaço aéreo ou de centros de comando e controlo de usinas hidrelétricas como a de Itaipu[25].

Atentados dessa natureza poderiam gerar caos e vítimas em larga escala. Quanto a isso, Clarcke e Knake (2015) apresentam duas considerações complementares entre si:

> A invasão de controlos de voo de uma aeronave em cruzeiro está provavelmente se tornado mais factível. A FAA[26] levantou questionamentos com a Boeing sobre o sistema de controlo de voo do novo 787 Dreamliner, que utiliza a mesma rede de computadores do sistema interativo de entretenimento do passageiro. A FAA está preocupada com a possibilidade de um passageiro invadir o sistema de controlo de voo a partir de seu assento, ou que a conectividade com a Internet para passageiros possa permitir que alguém de fora do avião invada o sistema (p.165).
>
> As leis internacionais de guerra proíbem atingir hospitais e alvos civis em geral, **mas é impossível atingir uma rede elétrica sem afetar instalações civis**. Enquanto todos somos cuidadosos com bombas, os Estados Unidos e outras nações desenvolveram armas de guerra cibernética que têm o potencial de atacar indiscriminadamente (p. 163). (negrito nosso)

Dessa forma, ações terroristas, ocorrendo no ciberespaço e empregando códigos maliciosos sobre infraestruturas estatais ou privadas poderá configurar ciberterrorismo, a atentar contra os Direitos Humanos. Esse é um dado que confirma a sua relevância.

Diante disso, poderíamos afirmar que vivemos uma realidade de ciberterrorismo? Não. Contudo, as supracitadas conexões são possíveis e nos permitem afirmar que essa ameaça poderá ganhar contornos mais claros no futuro, em virtude dos meios, indivíduos e valores que atualmente constituem as principais organizações terroristas. Entretanto, como isso poderia se proceder?

Do ponto de vista prático, ao analisarmos o Quadro 2, podemos propor uma solução para a supracitada pergunta. Na análise, é importante que sejam observadas, particularmente, as fases preparatória e de consequências.

[25] Importante Usina Hidrelétrica do Brasil e do Paraguai. Responsável pelo fornecimento de energia para os principais centros industriais brasileiros.

[26] Agência Federal de Aviação dos Estados Unidos da América.

Quadro 2 - Cronologia de um ataque terrorista

Fase preparatória (antes)	Crise/Ataque (durante)	Fase de consequências (depois)
Atividades terroristas: Desenvolvimento de capacidades Recrutamento Treinamento Arrecadação de verbas Pesquisa e desenvolvimento Aquisição de materiais Coleta de inteligência Planeamento Deslocamento estratégico/bases Estabelecimento de uma rede Reconhecimento Contrainformação Operações de Informação	Deslocamento final Reunião Montagem do equipamento Reconhecimento final Execução Extração	Exfiltração[b)] Regeneração das capacidades Avaliação das consequências Análise das operações Operações de Informação

b) Operação de retirada do efetivo responsável por incursão em território inimigo.

Fonte: VISACRO (2009, p. 286).

Ainda da observação do Quadro 2, podemos constatar a presença de Operações de Informação antes e após o atentado terrorista propriamente dito. Isso denota a sua importância em um cenário de GI. Somado a isso, podemos perceber que um atentado ciberterrorista, se inserido nas fases explicitadas acima, exige menos tempo e atividades em sua cronologia. Isso fica claro pela possibilidade de que seja dispensada a atividade de "Desenvolvimento de capacidades", já que existe um conjunto de indivíduos com *expertise* para trabalhar com ataques cibernéticos.

Ademais, outro aspeto que merece ser mencionado, se refere aos custos mais baixos que um atentado ciberterrorista demandaria se comparado a um atentado "convencional". Isso é possível pela redução nas demandas de Pesquisa e Desenvolvimento e de Deslocamento estratégico/bases (ambos inseridos na fase preparatória) proporcionada pela presença de *hackers* na organização terrorista.

Portanto, podemos perceber que com *hackers* a serviço de organizações terroristas, é possível conduzir atentados desenvolvidos no ciberespaço, com sérias consequências para a sociedade. Assim, considerando as dimensões econômica e militar, Clarcke e Knake (2015, p.182,) em sua obra narram que:

> Insurgentes no Iraque tinham usado um *software*, de 26 dólares, para monitorar os vídeos dos drones *Predator* dos Estados Unidos por meio de um enlace de comunicação não criptografado. Embora não seja uma ameaça direta às tropas americanas, a descoberta levanta questões sobre a nova arma "queridinha" do Pentágono. E se o sinal não criptografado pudesse ser corrompido, fazendo com que o drone voltasse para casa? As forças armadas americanas seriam influenciadas negativamente por uma de suas ferramentas mais valiosas e um programa de prateleira destruiria o resultado de milhões de dólares em pesquisa e desenvolvimento.

Dados os aspetos apresentados, conclui-se parcialmente que o ciberterrorismo se constitui em uma possibilidade real, tendo em vista o relacionamento factível entre a Guerra Cibernética e o Terrorismo. No entanto, alguns factores serão importantes para que isso venha a ocorrer. Dentre eles podemos destacar o factor tempo e o factor humano.

No que diz respeito ao primeiro factor, se observa que qualquer atentado terrorista demanda tempo de preparação. O seu dimensionamento influenciará no êxito da execução do ataque.

Intimamente relacionado ao tempo, o factor humano é fundamental. Dentro dele está inserido o controlo da narrativa, que irá garantir a cooptação dos indivíduos apropriados para a execução do atentado ciberterrorista.

Conclusão

Pelo exposto, podemos afirmar que a análise apontou para a possibilidade de haver uma relação clara e possível entre o Terrorismo e a Guerra Cibernética, no contexto da GI. Percebemos isso, basicamente, nos pontos de interseção norteados pela opinião pública e pelo emprego dos meios de TI.

Em síntese e, dentro do escopo dos supracitados pontos, podem ser destacados alguns aspetos que conferem sustentação à relação analisada no presente trabalho, a considerar o ambiente de Guerra de Informação. O Terrorismo está a empregar cada vez mais as redes sociais e a TI para a consecução de seus objetivos. A Guerra Cibernética, de outro modo, está a aproveitar as vulnerabilidades da *Internet* para apresentar-se como uma nova modalidade de conflito.

Os grupos Terroristas estão mais violentos, independentes financeiramente e com capacidades variadas, que lhe possibilitam atuar a grandes distâncias. Nesse cenário, está emergindo o ciberterrorismo.

A Guerra Cibernética está a ultrapassar os limites abrangidos pelos atores públicos e privados. Isso tem impactado todos os campos do poder, em particular o político e o militar. Neles temos o Governo e as Forças Armadas que, em alguns países como Estados Unidos e China, estão a buscar reestruturar-se ciberneticamente.

Além disso, dentro da referida relação (Terrorismo e GC) percebemos a importância do "controlo da narrativa". Isso não implica somente em "comunicar primeiro", se considerarmos um conflito entre agentes estatais e não estatais. É necessário sustentar a narrativa.

Isso poderá ocorrer por uma atuação firme do Estado (respeitando as variadas nuances de cada nação) regulando a *Internet*, particularmente quanto à Segurança das Redes, tema esse amplamente inserido na Guerra de Informação.

Além disso, pelo exposto, é possível que estejamos a testemunhar uma "quinta onda" do Terrorismo, onde este se relaciona com a GC. Essa nova "onda" seria uma junção do que caracterizaria as duas fases anteriores, na qual Estados-Nação militarmente mais fracos buscariam empregar ataques cibernéticos para fazer valer suas vontades sobre Estados mais fortes, imputando a "responsabilidade" desses ataques a grupos de *hackers* de seus países.

Diante desse cenário, poderíamos retornar, em uma visão holística, à ideia de "controlo da narrativa", seja em âmbito nacional ou internacional, como uma necessidade estratégica. Uma resposta a ela pode residir na instituição de um Comando de Guerra de Informação, onde estariam incluídos, dentre outros, órgãos de Combate ao Terrorismo e de Guerra Cibernética.

Por fim, pode-se concluir que conhecer e aprofundar o entendimento da relação do Terrorismo com a Guerra Cibernética pode ser necessário em um mundo cada vez mais complexo em suas ligações políticas, econômicas e militares. Tão importante quanto isso é compreender como a GI se processa, considerando a supracitada relação. Dessa forma, poderemos controlar melhor a narrativa, evitando o fortalecimento de grupos que empregam a violência e o desrespeito aos Direitos Humanos.

Referências Bibliográficas

Akpan, I. U, 2007. *Terrorismo: a nova guerra*. Trabalho de Conclusão de Curso. Rio de Janeiro. ECEME.

Alberts, D. Garstka, J. Stein, F, 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington DC: CCRP. [Online]. Disponível em: http://www.au.af.mil/au/awc/awcgate/ccrp/ncw.pdf. [Consult. 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*. 1ª Ed. Brasília.

Brasil, 2014a. *Estado-Maior do Exército. EB 20-MF-10.102. Doutrina Militar Terrestre. 1ª 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]. Disponível

em: http://www.ccomgex.eb.mil.br/cige/sent_colina/9_edicao_abr_10/index/Art_Maj_Fontenele.pdf [Consult. 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]. Disponível em: https://openaccess.leidenuniv.nl/bitstream/handle/1887/33671/Beslan%20Thesis%20DJG.pdf?sequence=1. [Consult. 02 dez 16].

Graham, M. *A,* 2016. *Força Cibernética dos EUA*. Military Review. [Online]. Disponível em: https://www.joomag.com/magazine/military-review-edi%C3%A7%C3%A3o-brasileira-julho-setembro-016/0209296001465490873. [Consult. 30 nov. 2016].

Haeni, R. E, 1997. *Information Warfare na Introduction*. The George Washington University, Cyberspace Policy Institute. [Online]. Disponível em: http://www.trinity.edu/rjensen/infowar.pdf . [Consult.: 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]. Disponível em: http://brasil.indymedia.org/media/2008/06/422822.pdf. [Consult. 30 nov 16].

Militão, O. P, 2014. *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional*. Tese de Dissertação de Mestrado em Ciência Política e Relações Internacionais, especialização em Relações Internacionais Lisboa: Universidade Nova de Lisboa. [Online]. Disponível em: https://run.unl.pt/bitstream/10362/14300/1/Dissertacao_OMilitao_35664.pdf. [Consult. 01 dez 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?* Trabalho de Conclusão de Curso. Rio de Janeiro: EGN.

Simioni, A. A. C, 2008. *O terrorismo contemporâneo: consequências para a segurança e Defesa do Brasil*. Tese de Dissertação de Mestrado em História. [Online]. Disponível em: http://livros01.livrosgratis.com.br/cp090607.pdf. [Consult. 10 nov 16].

Teixeira da Silva, F. C, 2001. *O Brasil na crise internacional*. Texto apresentado no Simpósio "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*. Trabalho de Conclusão de Curso. Rio de Janeiro: ESG.

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