UMA PROPOSTA DO RELACIONAMENTO ENTRE A GUERRA CIBERNÉTICA E O TERRORISMO NO CONTEXTO INFORMACIONAL E SEUS REFLEXOS PARA AS INFRAESTRUTURAS CRÍTICAS

Dardano do Nascimento Mota*
Fernanda Antônia Barbosa da Mota**

RESUMO
O presente artigo pretende apresentar uma análise sobre a possível relação entre o Terrorismo e a Guerra Cibernética no contexto informacional. Para atingir o objetivo proposto, o desenvolvimento do presente trabalho encontra-se subdividido nas seguintes seções: considerações preliminares; a Informação; a Guerra Cibernética (GC) onde serão detalhados os aspectos que a relacionam com a Informação; um *overview* do Novo Terrorismo; e, por fim, uma proposta de como estaria estruturada a relação do Terrorismo com a GC. O artigo apresenta conceitos básicos relacionados ao Terrorismo, à Guerra Cibernética e à Informação, visando facilitar o entendimento da análise desenvolvida. Para isso, emprega pesquisa bibliográfica e documental, priorizando os estudos relacionados ao assunto em tela. Por fim, o presente artigo buscou encontrar conclusões quanto à análise proposta sugerindo a criação de um órgão nacional voltado para a proteção de infraestruturas críticas.
Palavras-Chave: Informação. Terrorismo. Guerra Cibernética. Tecnologia da Informação. Opinião Pública.

A PROPOSAL OF THE RELATIONSHIP BETWEEN CYBER WAR AND TERRORISM IN THE INFORMAL CONTEXT AND ITS REFLECTIONS FOR CRITICAL INFRASTRUCTURES

ABSTRACT
The present article intends to present an analysis on the possible relation between Terrorism and the Cybernetic War in the informational context. In

* Bacharel em Ciências Militares (AMAN-2000), Curso Básico de Guerra Eletrônica – Especialização (Centro de Instrução de Guerra Eletrônica – 2004), Especialização em Bases Geo-Históricas para formulação Estratégica (2013), Comando e Estado-Maior (ECEME – 2015/2016). Atualmente, exerce as funções de instrutor como Comandante do Curso de Comunicações da Escola de Aperfeiçoamento de Oficiais. E-mail: dardanomota@yahoo.com.br. Currículo Lattes: http://lattes.cnpq.br/3668446482364459.

** Doutora em Educação (2014), Mestre em Educação (2007) e Licenciada em Pedagogia (2000) pela Universidade Federal do Piauí (UFPI). Especialista em Psicopedagogia (2001) pela União Cearense de Ensino Superior (UNICE). Professora Adjunta da Universidade Federal do Piauí (UFPI). Atua principalmente nos seguintes temas: Formação de Professores, Prática Pedagógica, Formação Humana, Filosofia da Educação e Infância, Educação e Filosofia, com ênfase nos estudos de Foucault e Deleuze. E-mail: fabmota13@yahoo.com.br. Currículo Lattes: http://lattes.cnpq.br/0208919237949818.

order to reach the proposed objective, the development of the present work is subdivided into the following sections: preliminary considerations; Information; the Cyber War (CW) where the aspects related to information will be detailed; an overview of New Terrorism; and, finally, a proposal on how the relationship between Terrorism and Cyber War would be structured. The article presents basic concepts related to Terrorism, Cyberwarfare and Information, in order to facilitate the understanding of the analysis developed. For this, it uses bibliographical and documentary research, giving priority to studies related to the subject matter. Finally, the present article sought to find conclusions regarding the proposed analysis recommended the creation of a national body focused on the protection of critical infrastructures.
Keywords: Information. Terrorism. Cyberwarfare. Information Technology. Public opinion.

UNA PROPUESTA DE LA RELACIÓN ENTRE LAS GUERRA CIBERNÉTICA Y EL TERRORRISMO EN EL CONTEXTO DE INFORMACIÓN Y SUS REFLEJOS EN LAS INFRAESTRUCTURAS CRÍTICAS

RESUMEN
Este artículo tiene por objetivo hacer un análisis de una posible relación entre el Terrorismo y la Guerra Cibernética en el contexto de información. Para ello, el desarrollo del presente trabajo se encuentra subdividido en las siguientes partes: consideraciones preliminares; la información; la Guerra Cibernética (GC) donde se detallarán los aspectos que la relacionan con la información; un *overview* del nuevo terrorismo; y, por último, una propuesta de cómo sería la estructura de la relación del Terrorismo con la GC. El artículo presenta conceptos básicos relacionados al Terrorismo, a la Guerra Cibernética (GC) y a la información, con la finalidad de facilitar la comprensión del análisis desarrollado. Para eso, se utiliza de investigación bibliográfica y documental, dando prioridad a los estudios relacionados a este presente tema. Por fin, este artículo buscó encontrar conclusiones cuanto al análisis propuesto, proponiendo que se creen un organismo nacional con el fin de proteger las infraestructuras críticas.
Palabras Clave: Información. Terrorismo. Guerra Cibernética. Tecnología de la Información. Opinión Pública.

1 INTRODUÇÃO

O fluxo informacional, ao ser analisado em suas muitas nuances, pode se configurar, em alguns momentos, como algo complexo. Os caminhos que a informação percorre, do agente emissor ao destinatário, nem sempre são tão claros. Nesse contexto, os Sistemas de Tecnologia da Informação têm sido importantes,

uma vez que estes atuam como agentes facilitadores não só para o armazenamento, como também para o fluxo dos dados informacionais.

Não há um limite temporal preciso no passado para o surgimento da Informação como a conhecemos. Sabe-se que ela está presente em todos os campos do poder, influenciando pessoas, grupos e instituições.

Em que pese este fato, a presente análise enfocará, particularmente, o período compreendido entre os séculos XX e XXI, considerando o Terrorismo e a Guerra Cibernética como os espaços em que a Informação estará sendo trabalhada.

A Informação pode transitar por diversos meios. Dentre eles, podemos destacar o Rádio, a Televisão e, mais recentemente, a *Internet*.

O Rádio, desde a sua invenção, fortaleceu-se como um poderoso instrumento para a disseminação informacional. A título de exemplo, temos o impacto causado pela *Columbia Broadcasting System* (CBS) que, em 1938, transmitiu a invasão da Terra por marcianos (FERREIRA, 2013, p. 2).

Mais moderna que o Rádio, a Televisão também é uma ferramenta de grande alcance para transmitir informações. Como assevera Martinelli (2010, p. 76), "pode-se dizer que a televisão é o principal meio de informação, pois consegue unir o universo da linguagem escrita ao audiovisual. A TV define-se pela imagem, mas incorpora com muita propriedade o som e a escrita".

Além disso, a Televisão, caracterizada por sua simplicidade de operação e portabilidade, tem influenciado as massas populares pela rapidez com que transmite ideias, muitas vezes em tempo real. Nesse contexto (de amplo e rápido alcance) temos a divulgação das ações terroristas e a Guerra Cibernética.

Em complemento a esse aspecto, nos últimos anos, esse processo de "espalhamento de dados" em tempo real tem contado com a contribuição da *Internet*.

Paralelamente, as ações terroristas têm ocorrido em várias partes do globo. Seja em países ricos ou pobres, cristãos ou islâmicos, o Terrorismo pode se manifestar por motivações diversificadas. Nesse cenário, a Surpresa tem-se constituído em de seus principais pilares:

> A grande preocupação atualmente reside nas pequenas células, descentralizadas e, muitas vezes, agindo por conta própria. Os alvos são selecionados por acaso dentro do princípio da oportunidade, fatores que dificultam o monitoramento e a detecção antes da ação terrorista. (WOLOSZYN, p. 24, 2010).

Da mesma forma, a Guerra Cibernética constitui-se como um fenômeno de alcance internacional. Para muitos especialistas nesse tema, a pergunta a ser feita não é "se seremos atacados ciberneticamente", mas sim "quando seremos atacados". Uma vez conectados em redes de computadores, podemos ser alvos de hackers, seja por razões políticas, ideológicas e econômicas, entre outras.

Diante disso e, do ponto de vista geopolítico, um ataque cibernético pode ser considerado como um ato de guerra?

Esse questionamento tem influenciado a estruturação de órgãos governamentais voltados para o combate cibernético, seja em ações de defesa, ataque ou somente de exploração cibernética. Países como Estados Unidos da América, Rússia, China e Coreia do Norte são bons exemplos de nações que têm investido na criação e fomento aos referidos órgãos para garantir o próprio funcionamento como país:

> 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; KNAKE, 2015, p. 85).

A seguir, será analisado o papel da Informação, destacando a Guerra Cibernética e o Terrorismo.

2 UM CENÁRIO DIFUSO DE AMEAÇAS

A Guerra está intimamente relacionada à evolução da Humanidade. Compreendê-la envolve todos os campos do poder. Nesse sentido, longas disputas como a Guerra Fria (1949-1989) não só entraram para a História, mas também influenciaram as relações internacionais no século XX e mantêm esse status no XXI.

No século XX, os conflitos envolviam adversários conhecidos (normalmente entre Estados oponentes); o Terrorismo era um fenômeno conduzido por organizações como o Setembro Negro, as Brigadas Vermelhas, o Grupo *Baader-Meinhof* e o *Euskadi Ta Askatasuna* (basco para "Pátria Basca e Liberdade"), ETA com objetivos mais políticos que motivados por outras questões, como a religiosa; e a Guerra Cibernética ainda dava seus "primeiros passos".

Diferentemente do anterior, no século XXI, alguns conflitos têm apresentado uma particularidade comum: o Terrorismo religioso. Associado a isso, Walzer (2010, p. 336) afirma que "na guerra, o terrorismo representa uma forma extrema da estratégia da 'abordagem indireta"[1].

1 Expressão utilizada inicialmente por Lidell Hart para designar, dentre outros pontos, a Guerra Assimétrica.

Em paralelo a esse aspecto, a sociedade tem convivido com os ataques cibernéticos. Um dos casos que configura essa assertiva está na relação entre China e Estados Unidos da América do Norte (EUA), particularmente quando observamos a sua disputa de poder no ciberespaço (MOTA, 2017).

Quanto a isso, Clarcke e Knake (2015, p. 45) destacam 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".

Assim, ao considerarmos uma conjuntura de ameaças, na qual o Terrorismo e a Guerra Cibernética vêm ganhando relevância é necessário que entendamos quais relações existem entre eles. Nesse entorno, podemos formular os seguintes questionamentos:

Quais são os principais pontos de intersecção entre a Guerra Cibernética e o Terrorismo?

E qual é o papel da Informação nesse contexto?

É necessário, portanto, que sejam apresentados os principais aspectos referentes à Informação, à Guerra Cibernética e ao Terrorismo antes de detalhar os pontos que poderiam justificar a supracitada relação.

3 A IMPORTÂNCIA DA INFORMAÇÃO AO LONGO DA HISTÓRIA

O pensador chinês Sun Tzu em sua Obra *A arte da guerra* (1997) afirmou que "deve-se procurar obter todas as informações sobre o inimigo. Informar-se exatamente de todas as suas relações, suas ligações e interesses recíprocos".

Como se pode observar, a Informação não se constitui em algo recente. Ao longo da História da Humanidade, os exemplos quanto a isso são variados, tanto os relacionados à sua valorização quanto à sua negligência.

Nesse sentido, a Bíblia (2008) apresenta, no Capítulo 2 do Livro de Josué, o envio de espias para buscar informações sobre a cidade de Jericó, que culminariam com o cerco e conquista desta pelos hebreus.

Ainda na Idade Antiga, antes da Batalha das Termópilas (Portões Quentes)[2], o Rei persa Xerxes recebeu informações quanto ao poder de combate dos gregos. Contudo, ele negligenciou aquelas que poderiam, de alguma forma, causar uma grande quantidade de baixas ao seu Exército e que lhe impossibilitaram

2 A Batalha das Termópilas foi travada no contexto da Segunda Guerra Médica entre uma aliança de pólis gregas liderados pelo rei de Esparta Leônidas I e o Império Aquemênida de Xerxes I. A batalha durou três dias e se desenrolou no desfiladeiro das Termópilas ('Portões Quentes') em agosto ou setembro de 480 a.C. Disponível em:www.ebooksbrasil.org/adobeebook/historiaherodoto.pdf. Acesso em: 25 jul. 2018.

conquistar a Grécia ao final das Guerras Médicas[3]. Isso se encontra citado a seguir:

> Xerxes mandou chamar Demarato, filho de Aríston, que se achava no acampamento, e quando este chegou interrogou-o sobre a conduta dos lacedemônios em tão perigosa situação. "Senhor — respondeu Demarato —, quando encetámos a marcha contra a Grécia eu vos falei sobre esse povo, dizendo-vos da atitude que ele assumiria ante o perigo de um ataque, e nenhuma atenção destes às minhas palavras. Embora incorra no risco de desagradar-vos, quero que saibais a verdade e peço-vos que me escuteis. Aqueles homens que ali se encontram estão dispostos a vedar-vos a passagem, e para isso se preparam, pois os Lacedemônios têm o costume de tratar dos cabelos quando em vésperas de arriscar a vida numa empreitada. Se conseguirdes subjugar esses homens e os que se encontram em Esparta, podeis estar certo, senhor, que nenhuma outra nação ousará mais erguer-se contra vós, já que os Espartanos, contra os quais agora marchais, são o povo mais valoroso da Grécia, e o seu reino e a sua cidade os mais florescentes e belos de todo o país". Xerxes, não podendo dar fé a essas palavras, perguntou, ainda uma vez, de que maneira os gregos, sendo em número tão reduzido, poderiam fazer frente ao seu poderoso exército. "Senhor — volveu Demarato —, podeis considerar-me um impostor se não acontecer tal como vos digo". O soberano, todavia, não se deu por convencido, e deixou passar quatro dias, esperando que os gregos se pusessem em fuga. (HERODOTO, 1950, p. 598).

Como os gregos, a China sofreu invasões em seu território. Isso ocorreu no século XIX, em virtude de uma desvantagem bélica resultante da negligência chinesa em buscar informações sobre os demais Estados, particularmente os Ocidentais:

> A China sabia, é claro, da existência de diferentes sociedades em torno de suas fronteiras na Coreia, no Vietnã, na Tailândia, em Burma; mas, na percepção chinesa, a China era considerada o centro do mundo, o "Império do Meio", e as demais sociedades eram auferidas segundo gradações a partir daí. No modo de ver dos chineses, um punhado de Estados menores que absorvesse a cultura chinesa e prestasse tributo à grandeza da China constituía a ordem natural do Universo. (KISSINGER, 2011, p. 28)

3 Guerras Médicas, Guerras Greco-Persas, Guerras Persas ou Guerras Medas são designações dadas aos conflitos bélicos entre os antigos gregos e o Império Aquemênida durante o século V a.C. Ocorrera entre os povos gregos (aqueus, jônios, dórios e eólios) e os medo-persas, pela disputa sobre a Jônia na Ásia Menor, quando as colônias gregas da região, principalmente Mileto, tentaram livrar-se do domínio persa. Disponível em: www.ebooksbrasil.org/adobeebook/historiaherodoto.pdf. Acesso em: 25 jul.2018.

Outro momento histórico que destacou a importância da Informação ocorreu durante os preparativos para o Desembarque Aliado na Normandia, durante a Segunda Guerra Mundial (1939 – 1945).

Por ocasião do levantamento de dados para o deslocamento de tropas aliadas na praia de *Omaha*, o Major *Scott-Bowden* e o Sargento *Ogden Smith* do Comando Supremo Aliado, colheram amostras do terreno onde iriam desembarcar os aliados nas praias do norte francês, que até aquele momento estavam fortemente defendidas pelo Exército alemão.

Segundo Ambrose (2009):

> O major *Scott-Bowden* e o sargento *Ogden-Smith* nadaram para a praia, conduzindo pistolas, facas, bússolas de pulso, lâmpadas elétricas portáteis à prova d'água, e uma dúzia de tubos de doze polegadas.
> Eles entraram com a maré subindo na aldeia costeira de *Luc-sur-Mer* na praia que recebeu posteriormente o codinome de *Sword* (Espada). Eles podiam ouvir canções entoadas pela guarnição alemã. Os dois homens nadaram cautelosamente para a praia, caminharam um pouco para o interior, deitaram-se no chão quando o raio de luz do farol varria a extensão da praia, caminharam um pouco mais. Tiveram o cuidado de permanecer abaixo da marca de preamar, de modo que seus rastros fossem apagados pela maré antes que amanhecesse. Enterraram seus tubos na areia, colhendo amostras e anotando a localização de cada uma em pranchetas à prova d'água que usavam nos braços. (AMBROSE, 2009, p. 87).

Pelo exposto, ao analisarmos como a Informação se apresenta, podemos afirmar que ela se constitui em algo multifacetado. Diante de tal assertiva, emerge o questionamento de como se processaria essa característica. Vamos tentar respondê-lo.

De forma preliminar, ao considerarmos essa característica, a Informação apresenta diversas definições dentro da estrutura do Conhecimento. Conforme Gleick (2013), a Informação é "aquilo que alimenta o funcionamento do nosso mundo: o sangue e o combustível, o princípio vital. Ela permeia a ciência de cima a baixo, transformando todos os ramos do conhecimento".

De acordo com Messias (2005), do ponto de vista da Biologia, "para a existência e funcionamento de um organismo é fundamental a existência da Informação. Além das informações cerebrais, próprias do ser vivo, também existem as informações genéticas".

Ainda, conforme Messias (2005), no ambiente administrativo tem-se a informação como sendo:

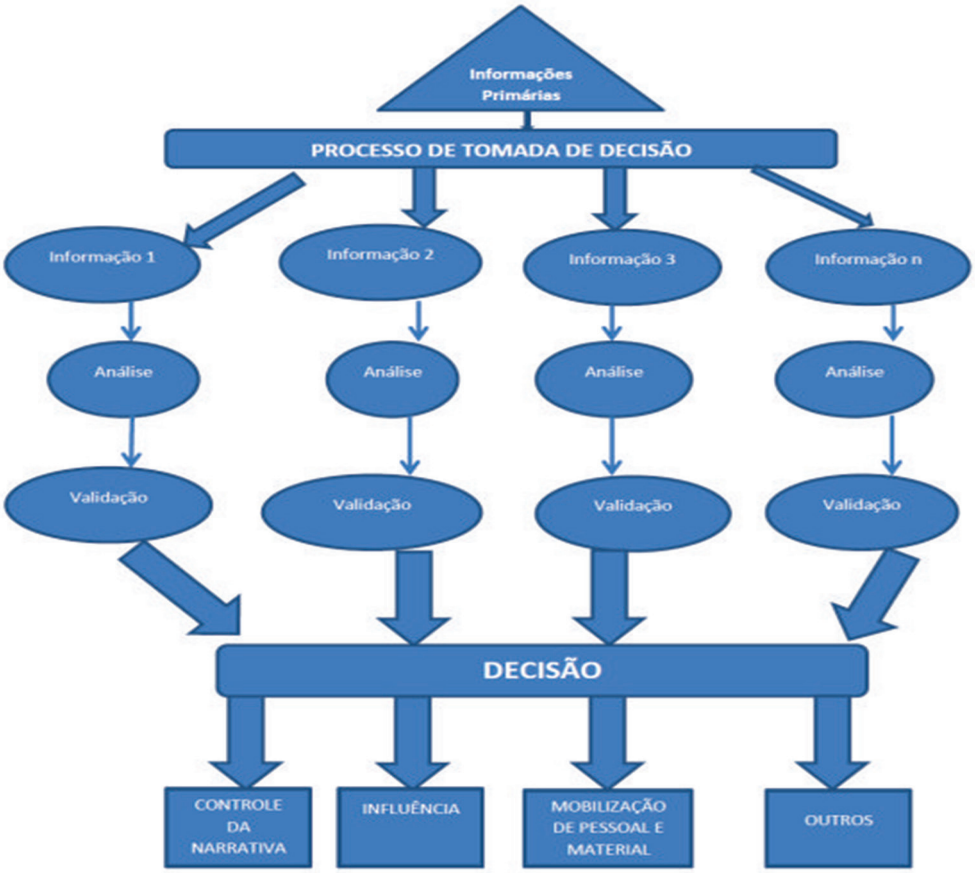
> Um recurso estratégico para a tomada de decisões, resultando sempre numa ação planejada. Os administradores, se detentores da informação, tem a possibilidade de se antecipar a problemas e garantir

> o sucesso na tomada de decisões. Em contrapartida, o resultado de uma decisão tardia, devido à falta de informações, compromete no desempenho da organização. (MESSIAS, 2005, p. 28).

Sendo assim, e considerando os supracitados conceitos, a necessidade por Informações vem-se intensificando, em virtude, em alguns casos, da crescente complexidade das relações sociais e ferramentas à disposição para isso, como os meios tecnológicos.

Isso nos impele a apresentar um sintético estudo de caso, que terá como escopo a Segunda Guerra do Golfo (2003 – 2012). Para isso, veremos um Fluxograma que apresenta, de forma sumária, a relação do Processo de Tomada de Decisão com o papel das Informações.

Figura 1 - Fluxograma do Processo Decisório e as Informações



Fonte: Os Autores, 2018

Analisando a Figura 1, podemos observar que a chamada Informação Primária inicia o Processo de Tomada de Decisão.

No contexto informacional, constata-se que a Decisão e seus produtos (Controle da Narrativa, Influência e Mobilização de Pessoal e Material) estão envolvidos com a qualidade e validade das Informações levantadas, o que embasará os próximos passos que serão dados.

Ao trazermos essa linha de pensamento para a Segunda Guerra do Golfo, podemos depreender os seguintes pontos:

I. Informações Primárias: ataques terroristas (principalmente o de Nova York – 11 Setembro 2001); Guerra do Afeganistão (havia iniciado em 2002).
II. Informações: informações de inteligência norte-americanas sobre a atuação de grupos terroristas apoiados pelo regime de *Saddam Hussein*; provável presença de armas de destruição em massa no Iraque (discurso sustentado pelos Estados Unidos); parecer desfavorável da Organização das Nações Unidas (ONU) quanto à presença de armas de destruição em massa no Iraque.
III. Análise: Atuação de grupos da ONU para verificar a existência de armas de destruição em massa no Iraque; Estudo por parte de órgãos norte-americanos.
IV. Validação: emitida somente pelo governo norte-americano.
V. Decisão: Invadir o Iraque e destruir o Regime de Saddam Hussein.
VI. Controle da Narrativa: A comunidade internacional deverá acreditar que o Iraque possui armas de destruição em massa e, por isso, o governo de *Hussein* deverá cair.
VII. Influência: os Estados Unidos buscaram, continuamente, influenciar outras nações para a necessidade de derrubar *Saddam Hussein*, além de sua própria sociedade civil.
VIII. Mobilização de Pessoal e Material: Os Estados Unidos atacarão empregando os seus próprios meios.
IX. Outros aspectos: impactos da Decisão de invadir o Iraque sobre a Sociedade Civil norte-americana, em médio e longo prazo (caso houvesse um prolongamento do conflito).

Analisando o exposto, podemos observar que, ainda que tenha sido respeitado todo o fluxograma, as informações que contrariavam a invasão ao Iraque não foram consideradas e a Decisão tomada atendeu a interesses políticos unilaterais.

Dessa forma, ainda que o Iraque tenha sido invadido e o Regime de Hussein tenha caído, os Estados Unidos não conseguiram sustentar o controle de sua narrativa, em virtude de dados incompletos e de decisões unilaterais.

4 INFLUÊNCIA INFORMACIONAL DAS MÍDIAS SOCIAIS

Quando refletimos sobre redes sociais, mídias sociais e comunidades virtuais, lembramo-nos do seu emprego por grande parte das pessoas em todo o mundo. Corroborando esse pensamento, *Singer*; *Friedman* (2017) afirmam que:

> Podemos nos queixar disso, porém *Facebook*, *Twiter*, *Google* e todo o restante são a exata definição da vida moderna no Ocidente Democrático. Para muitos, uma Internet funcionando com liberdade de discurso e uma boa conexão com as redes sociais de nossa escolha é um sinal não apenas da modernidade, mas de uma própria civilização. (SINGER; FRIEDMAN, 2017, p. 25).

Nesse sentido, para ilustrar essa questão do ponto de vista prático e, buscando um exemplo do Oriente, temos a Primavera Árabe. Nesse fenômeno, que ocorreu em uma parte do mundo muçulmano, foram observadas transformações provocadas por manifestos nas redes sociais que culminaram com o movimento de milhares de pessoas (principalmente jovens), que derrubaram regimes como de o *Kaddaffi*[1] (1942-2011) na Líbia e de *Mubarak*[2] no Egito.

Aprofundando essa análise, cabem os seguintes questionamentos: quais foram os resultados concretos dos idealizadores desse Movimento que começou na Tunísia? Hoje, aquelas regiões estão sendo democraticamente geridas? Ou foi somente um fenômeno passageiro que trocou ditadores por líderes defensores de minorias mais poderosas e influentes? Os Estados envolvidos estavam prontos para controlar a narrativa de modo a se contrapor às informações que circulavam nas mídias sociais?

Essa realidade traz à tona a seguinte ideia: as mídias sociais podem ter resultados transformadores, mas se não forem devidamente geridos, ficarão sem resultados concretos que tragam melhorias substanciais para a sociedade.

O fluxo informacional, obviamente, sempre terá objetivos. Contudo, caso estes não estejam bem definidos, os resultados poderão ser poucos e acanhados. É necessário, portanto, saber manuseá-los. Para isso é preciso conhecer o Processo Decisório envolvido bem como os pontos que precisarão ser alcançados.

Encerrando o tópico específico da importância da Informação para o presente trabalho, será apresentada uma visão da Árvore Informacional (Figura 2). Nela podemos destacar as raízes alimentando, por intermédio da *Internet*, os "frutos" apresentados na ilustração, particularmente o Terrorismo e a Guerra Cibernética.

---

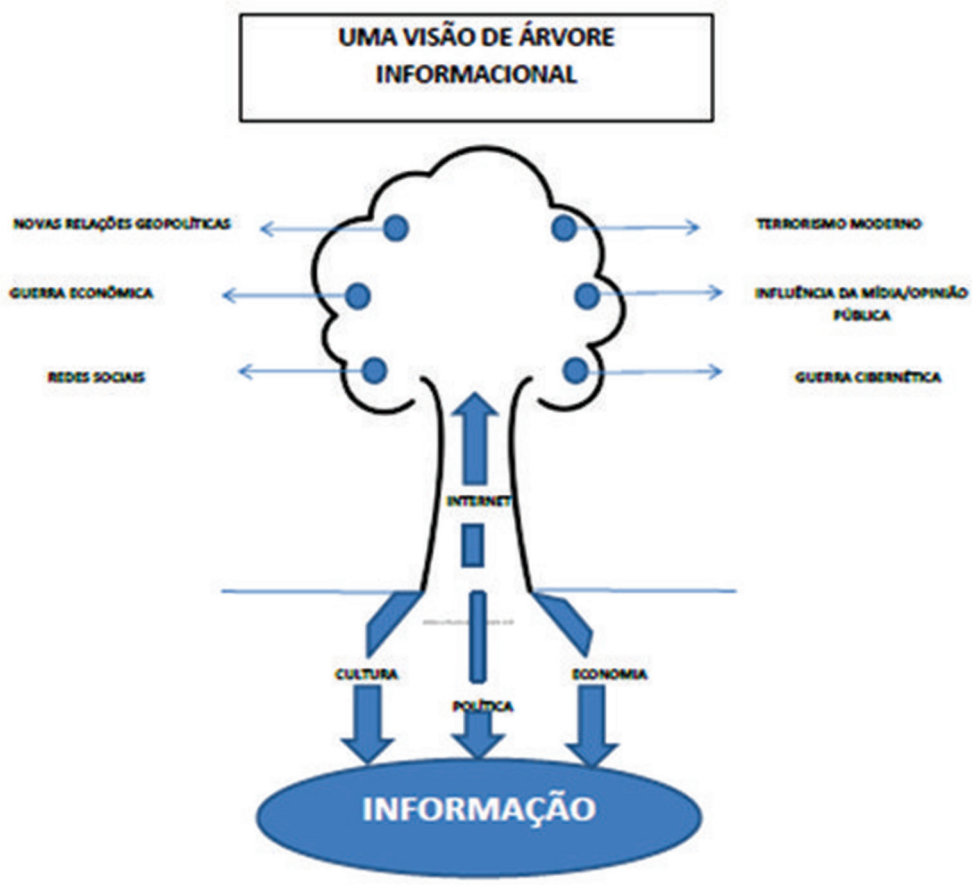
1 Muammar Mohammed Abu Minyar al-Gaddafi foi um militar, político, ideólogo e ditador líbio, sendo de facto chefe de estado do seu país entre 1969 e 2011 (ano de seu falecimento).

2 Muhammad Hosni Said Mubarak (1928) é um militar e político egípcio, que ocupou o cargo de presidente da República Árabe do Egito.

Em complemento a essa abordagem, Huntington (1993) afirma que:

> A política mundial está sendo configurada seguindo linhas culturais e civilizacionais. Nesse mundo, os conflitos mais abrangentes, importantes e perigosos não se darão entre classes sociais, ricos e pobres, ou entre outros grupos definidos em termos econômicos, mas sim entre povos pertencentes a diferentes entidades culturais. **(**HUNTINGTON, 1993, p. 21.)

Figura 2 – Árvore Informacional



Fonte: Os Autores, 2018

Dado o exposto, conclui-se parcialmente quão importante e abrangente é a Informação. É tão patente que hoje vivemos um contexto de Disputas

Informacionais, que envolvem não somente agentes estatais, mas também não estatais. A comunicação será abordado nos próximos tópicos deste trabalho.

5 A GUERRA CIBERNÉTICA E ALGUNS DE SEUS ATORES

O Livro Verde de Defesa Nacional (BRASIL, 2010, p. 23,) destaca que a Guerra Cibernética consiste em um:

> Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil.

Para que as referidas vantagens possam ser obtidas, o principal eixo de dados para a Guerra Cibernética tem sido a *Internet*.

Para exemplificar essa realidade, serão apresentados dois episódios envolvendo países (atores) que estão investindo em suas estruturas de Guerra Cibernética: Rússia e China. Essas nações têm demonstrado suas capacidades, através de ataques cibernéticos com fins políticos e econômicos.

Do ponto de vista político, a Rússia vem fazendo uso de suas capacidades cibernéticas como instrumentos de imposição de poder. Segundo Mota (2017), isso ficou evidenciado nos ataques cibernéticos DDoS[3] sobre a Estônia (um dos países mais conectados à *Internet* no mundo) em 2007.

Essa nação sofreu ataques cibernéticos, que inutilizaram seus maiores servidores pelo excesso de pedidos de acesso. “Os estonianos não podiam acessar seus bancos *on line*, os *sites* de seus jornais ou os serviços eletrônicos do governo”. (CLARCKE; KNAKE, 2015, p. 16).

Outro ponto que pode ilustrar a influência russa na Guerra Cibernética está nas denúncias norte-americanas de manipulação de resultados nas últimas eleições presidenciais dos Estados Unidos, conforme o disposto a seguir:

> Os serviços de inteligência dos Estados Unidos não trazem provas concretas sobre o papel de Putin na campanha contra *Hillary Clinton*, mas afirmam que as ações da Rússia incluíram: *Hackear emails* de contas do Comitê Nacional Democrata e de membros da alta cúpula do partido;

3 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; KNAKE, p. 223, 2015).

> - Usar intermediários como *WikiLeaks*, DCLeaks. com e *Guccifer* 2.0 para publicar informações adquiridas no hackeamento; e
> - Usar propaganda financiada pelo Estado e pagar usuários de mídia sociais ou "*trolls*" para fazer comentários desagradáveis sobre *Hillary*.[4]

Do ponto de vista econômico, especialistas chineses têm buscado os códigos-fonte de empresas multinacionais. Clarcke e Knake afirmam que isso tem impulsionado o aprimoramento 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. (CLARCKE; KNAKE, 2015, p. 53).

Pode-se observar, dessa forma, que o manuseio da Informação em um contexto de Guerra Cibernética se constitui em um ponto de intersecção entre China e Rússia.

Todavia, para que isso se realize, é necessário que sejam exploradas as vulnerabilidades do ciberespaço. Sendo assim, serão tratados alguns aspectos da *Internet*.

A primeira vulnerabilidade está na facilidade de propagação de tráfego malicioso para atacar computadores. Esses ataques 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; KNAKE, 2015, p. 70).

A segunda está no fato de grande parte do tráfego de dados ocorrerem sem criptografia[5]. "Atualmente, muitos *sites* (mas não a maioria) usam a conexão segura quando se faz o *log on*. Entretanto, devido ao custo e à velocidade, depois que a senha foi transmitida, muitos deles retornam à conexão em seu modo inseguro" (CLARCKE; KNAKE, 2015, p. 69).

Além disso, os vírus, bombas lógicas[6] e *hackers* também podem atuar sobre infraestruturas críticas[7]. Em conexão a isso, Clarcke e Knake (2015, p. 173)

4 Disponível em: http://www.bbc.com/portuguese/internacional-38525951. Acesso em: 30 jul. 2018

5 Codificação de uma informação de modo a torná-la ilegível para quem não possuir a chave de decodificação (CLARCKE; KNAKE. 2015, p. 224).

6 Códigos maliciosos

7 Art. 2°, da Portaria nº 02, de 08 de fevereiro de 2008, do Gabinete de Segurança Institucional (GSI) da Presidência da República: consideram-se Infraestruturas Críticas (IEC) as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional.

asseguram 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".

Somando-se ao exposto e, estudando esse cenário, é importante ressaltar que a Guerra Cibernética engloba aspectos ligados à iniciativa privada. Nesse escopo, estão incluídas as empresas de TI, que muitas vezes são contrárias às regulações que os Estados buscam impor.

De acordo com Mota (2017) atualmente, a abundância de meios de TI tem aumentado a complexidade tecnológica em todas as expressões do poder e, na mesma proporção, a necessidade de desenvolver estruturas de Defesa Cibernética.

Tornando essa questão mais complexa, Clarcke e Knake (2015, p. 119), afirmam que quanto ao "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".

O exemplo norte-americano atesta que "é mais fácil articular ataques informáticos do que se defender deles" (KISSINGER, 2014, p. 346). Isso fica evidenciado, já que no campo militar norte-americano, alguns analistas têm proposto a criação de uma Força Cibernética com status igual ao das demais Forças Armadas. Dessa forma:

> 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. (GRAHAM, 2016, p. 74).

Dessa maneira, conclui-se parcialmente que os meandros da Guerra Cibernética são multifacetados e complexos. Ela liga, de forma profunda, dois importantes atores (esferas governamental e privada) sem que seja desconsiderado o perfil das informações que serão manuseadas.

Sendo assim, como assevera Mota (2017), fica comprovado pelo fato de muitas das chamadas infraestruturas críticas funcionarem baseadas na *Internet*, que possui provedores privados e são suscetíveis a ataques cibernéticos. Entretanto, não há como garantir a sua proteção sem que haja estruturas e políticas de Defesa Cibernética.

Em que pese o exposto, para atender à análise proposta, é necessário abordar o Terrorismo para que possa ser estabelecido o teor de sua relação com a Guerra Cibernética no contexto informacional.

6 UMA *ABORDAGEM* SOBRE O "NOVO TERRORISMO"

O Terrorismo não é somente um dos frutos de uma Guerra de Ideologias. As questões políticas, sociais e informacionais também compõem o tecido que

estrutura o "Novo Terrorismo". É necessário, portanto, apresentar alguns dos conceitos deste fenômeno na atual conjuntura mundial.

Como afirma Woloszin (2010), o Terrorismo também pode ser um problema de segurança pública. Adotando a terminologia chamada "Terrorismo Criminal", o referido autor destaca que:

> Esse novo conceito pode ser definido como ações violentas, realizadas assistematicamente contra segmentos da sociedade (incluindo autoridades governamentais), praticadas por organizações criminosas, com o objetivo de causar pânico e intimidação, na busca de interesses restritos e pontuais (...) é um novo fenômeno ainda desconhecido ou não percebido pelas autoridades, cujos métodos tradicionais utilizados pelas forças policiais e a legislação penal existente são inócuos para combatê-lo. (WOLOSZIN, 2010, p. 116).

Para Walzer (p. 335, 2003) 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".

Além disso:

> O terrorismo, no mais comumente aceito 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. (WHITTAKER, 2005, p. 21).

Em adição aos conceitos apresentados, Simioni (2008) destaca que o Terrorismo 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".

Dessa forma, ao analisarmos as definições supracitadas, observamos que o terrorismo implicaria somente o assassinato de pessoas com fins políticos? Uma resposta a esse questionamento pode estar nas considerações a seguir.

A primeira: o "Novo Terrorismo" tem, na violência, uma valiosa ferramenta para ser bem-sucedido, e esta vem sendo apoiada por estruturas de TI.

A segunda: o "Novo Terrorismo" visa atingir não somente objetivos políticos, mas também sociomorais, o que nos motiva a analisar algumas de suas nuances.

No que tange à primeira consideração, o Terrorismo, de acordo com Walzer (2005, p. 347) "é a forma totalitária da guerra e da política, reduzindo a pó as

convenções de guerra e o código político. Ele desrespeita os limites morais além dos quais parece ser impossível qualquer outra limitação".

Esse desrespeito foi confirmado nos atentados terroristas ocorridos em Paris, no ano de 2015, conforme o disposto a seguir:

> Os ataques de novembro de 2015 em Paris foram uma série de atentados terroristas ocorridos na noite de 13 de novembro de 2015 em Paris e *Saint-Denis*, na França. Os ataques consistiriam de fuzilamentos em massa, atentados suicidas, explosões e uso de reféns. Ao todo, ocorreram três explosões separadas e seis fuzilamentos em massa, incluindo bombardeios perto do *State de France*, no subúrbio ao norte de Saint-Denis. O ataque mais mortal foi no teatro *Bataclan*, onde os terroristas fuzilaram várias pessoas e fizeram reféns até o início da madrugada de 14 de novembro. Pelo menos 137 pessoas morreram, incluindo os 7 terroristas que perpetraram os ataques, sendo 89 delas no teatro *Bataclan*. Mais de 350 pessoas ficaram feridas pelos ataques, incluindo 99 pessoas em estado grave. Além das mortes de civis, oito terroristas foram mortos. [8] (DELLAGNEZZE, 2016, p. 23).

Em complemento, podemos afirmar que, para que as organizações terroristas possam "exercer a violência" que desejam, estas vêm adotando, cada vez mais, métodos baseados em Tecnologia da Informação. Tais métodos têm facilitado a divulgação de suas ações, particularmente nas redes sociais.

> As plataformas de redes sociais *online* se tornaram um poderoso aparato para organizações terroristas na atração de potenciais membros e seguidores. Os conteúdos hospedados em redes sociais têm o potencial de atingir um público significativamente mais amplo e mais diverso do que aqueles postados em *sites* especializados tradicionais e fóruns na web, que geralmente apelam para um grupo selecionado de indivíduos. (ROCHA, 2016, p. 54).

A citação acima reforça a ideia de que a capacidade das redes sociais de divulgar dados não implica coordenação das ações, uma vez que, quantitativamente, os indivíduos alcançados pela retórica terrorista são, em determinados países, pessoas fora do perfil de um "terrorista padrão".

Desta feita e finda a primeira consideração iniciaremos a segunda, destacando outras peculiaridades do "Novo Terrorismo".

8 Disponível em: http://www.ecsbdefesa.com.br/defesa/fts/EITV.pdf. Acesso em: 30 jul. 2018

Ele está baseado em um dos tripés que, de acordo Visacro (2009, p. 293), orienta o planejamento das suas ações: a opinião pública.

Em que pese este fato, para a presente análise, será considerado que a opinião pública não coincide com a verdade, precisamente por ser opinião, mas, na medida em que se fortalece no debate, expressa uma atitude racional, crítica e bem informada. (BOBBIO, 1983, p. 842).

Além disso, destaca-se que:

> A existência da Opinião pública é um fenômeno da época moderna: pressupõe uma sociedade civil distinta do Estado, uma sociedade livre e articulada, onde existam centros que permitam a formação de opiniões não individuais, como jornais e revistas, clubes e salões, partidos e associações, bolsa e mercado, ou seja, um público de indivíduos associados, interessado em controlar a política do Governo, mesmo que não desenvolva uma atividade política imediata. (BOBBIO,1983, p. 842).

Isso reforça o pensamento, ou melhor, a necessidade de controlar a opinião pública, algo que o Terrorismo busca influenciar. A violência, a Tecnologia da Informação e o emprego sistemático e simultâneo dessas ferramentas se constituem no centro nervoso de ações como os Atentados de Paris que feriram, de forma profunda, a opinião pública, particularmente a Ocidental.

Dado o exposto, infere-se parcialmente que o Novo Terrorismo, ao mesmo tempo em que quer atingir a opinião pública, não tem transmitido de forma clara as suas ações, uma vez que ao externar em redes sociais o seu "pensamento" perdeu, paradoxalmente, parte do controle das ações que podem ocorrer em qualquer parte do globo pela influência das redes sociais, que estão baseadas em Tecnologia da Informação.

7 A RELAÇÃO ENTRE O TERRORISMO E A GUERRA CIBERNÉTICA NO CONTEXTO INFORMACIONAL

Ao tentarmos visualizar como se relacionam o Terrorismo e a Guerra Cibernética, enfocando a dimensão informacional, serão analisados os dois pontos de intersecção levantados no tópico anterior. A partir dessa análise será possível propor a sua validação.

Para isso, será utilizado o quadro a seguir de modo a ilustrar esta relação.

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

Dimensão	Pontos de Intersecção	Terrorismo	Guerra Cibernética
Informacional	Opinião Pública (perspectiva cognitiva)	- Busca chocar e transformá-la pela violência ou simples intimidação pelo uso desta. - É um dos Centros de Gravidade[1] para as ações terroristas	- Busca influenciar a sociedade apresentando as vulnerabilidades da Internet. - Pode criar uma "multiplicidade de opiniões públicas"
	Amplo emprego de TI (perspectiva 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.

Fonte: REVISTA DE CIÊNCIAS MILITARES, 2017.

De posse do Quadro acima, para que possamos construir uma concepção da relação entre o Terrorismo e a Guerra Cibernética, é necessário tecer alguns comentários sobre eventuais ataques a infraestruturas críticas.

Nesse sentido, *Clarcke* e *Knake* afirmam que:

> As leis internacionais de guerra proíbem atingir hospitais e alvos civis em geral, mas é impossível atingir uma rede elétrica sem afetar instalações civis. Na última guerra entre os Estados Unidos e o Iraque, a campanha americana *Shock and Awe*[9] empregou munições precisamente guiadas que dizimaram edifícios-alvo e deixaram outros praticamente destruídos. Enquanto todos somos cuidadosos com bombas, os Estados Unidos e outras nações desenvolveram armas de guerra cibernética que têm o potencial de atacar indiscriminadamente. (CLARCKE; KNAKE, 2015, p. 163).

Atualmente, um ataque militar que provoque danos a infraestruturas críticas atinge a opinião pública com rapidez, em virtude da capacidade dos meios de comunicação.

9 É uma doutrina militar baseada no uso de força avassaladora, manobras dominantes e mostras espetaculares de força para paralisar a compreensão do adversário e destruir sua vontade de lutar. É uma criação da National Defense University, dos Estados Unidos.

Sendo assim, um ataque que conjugue meios cibernéticos a ações terroristas, voltado para estações de abastecimento de água, de energia elétrica, escolas e hospitais pode trazer grande repercussão, influenciando a sociedade pela qualidade e quantidade das informações divulgadas.

Quanto a isso, o próprio Estado nem sempre estará pronto para responder, seja nas medidas que previnam ações dessa natureza seja naquelas que detenham medidas repressivas a atentados com tais características.

Dado o exposto, podemos inferir parcialmente que ataques a infraestruturas críticas podem reunir, de forma eficaz, o Terrorismo com a Guerra Cibernética, uma vez que, ao considerarmos a sua Dimensão Informacional, estes serão de grande alcance e com capacidade de influenciar diversos setores da sociedade.

8 CONSIDERAÇÕES FINAIS

Pelo exposto, podemos afirmar que a presente análise destacou o papel da Informação apontando para uma relação entre o Terrorismo e a Guerra Cibernética. Isso pôde se materializar, basicamente, em questões ligadas à opinião pública e aos meios de TI.

Em síntese, podem ser destacados alguns aspectos que conferem sustentação ao trabalho proposto, tendo como norte a análise da Informação. O Terrorismo vem empregando, de forma crescente, as redes sociais e a TI para a execução de seus atentados. A Guerra Cibernética, por sua vez, vem aproveitando as vulnerabilidades da *Internet* para mostrar-se como uma nova modalidade de conflito.

O Terrorismo está mais articulado e ramificado. Diferentemente do passado, as organizações terroristas estão mais independentes tanto financeiramente quanto de Estados que lhes davam homizio. As suas variadas capacidades têm lhe possibilitado um alcance mundial, ainda que descontrolado em alguns momentos.

A Guerra Cibernética vem sendo transversal às esferas privada e governamental. Isso tem impactado todos os campos do poder, em particular o político, o econômico e o de ciência e tecnologia. Neles temos o Governo e as Forças Armadas que, em alguns países como Estados Unidos e China, estão buscando estruturar-se ciberneticamente.

Diante desse cenário, poderíamos retornar, em uma visão holística, à ideia de intensificar a proteção às infraestruturas críticas, como uma necessidade estratégica.

Nesse sentido, ao considerarmos a importância da Informação e os necessários dispositivos para o seu manuseio e proteção, podemos afirmar que um dos caminhos para isso pode residir na criação de uma Instituição inserida no nível Estratégico, de Tratamento da Informação, onde estariam incluídos, dentre outros, órgãos de Combate ao Terrorismo e de Guerra Cibernética trabalhando de forma integrada.

Para isso, importa destacar que para o caso do Brasil:

- ✓ essa Instituição poderá estar ligada ao Ministério da Defesa e formada por indivíduos oriundos tanto do meio civil quanto militar; e
- ✓ essa Instituição estaria permanentemente estruturada e vocacionada para a proteção das infraestruturas críticas nacionais.

Dado o exposto, analisar a Informação é algo complexo, em virtude de sua vastidão de feições. Contudo, quando esta fica restrita a questões específicas (como é o caso da relação entre o Terrorismo e a Guerra Cibernética), o trabalho de estudar as suas variáveis torna-se menos complexo e passível de propor soluções para o nosso dia a dia, cada vez mais caracterizado pela influência dos meios de TI e da opinião pública.

Entender como isso se processa pode conferir ao Estado e, também à iniciativa privada, a condição de estruturar-se melhor para transitar em um mundo complexo e marcado por reações sociais inesperadas tanto no tempo quanto no espaço.

REFERÊNCIAS

A BÍBLIA. Jesus lava os pés aos discípulos. Tradução de João Ferreira Almeida. Rio de Janeiro: King Cross Publicações, 2008. 1110 p. Velho Testamento e Novo Testamento.

BOBBIO, Norberto. *Dicionário de Política*. Universidade de Brasília. Brasília – DF. 1983.

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

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

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

DELLAGNEZZE, René. *O Estado Islâmico, o Terrorismo, a violação dos Direitos Humanos e da Soberania dos Estados*. Minas Gerais : Universidade Federal de Juiz de Fora. 2016.

FERREIRA, Andréia da P.. *A invenção do rádio: um importante instrumento no contexto da disseminação da informação e do entretenimento*. Revista Múltiplos Olhares em Ciência da Informação. v.3, n.1. Universidade Federal de Minas Gerais. 2013.

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].

HERODOTO. *História*. Brasília-DF, Universidade de Brasília, 1978.

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

MESSIAS, Lucilene C. da S, 2005*. Informação: um estudo exploratório do conceito em periódicos científicos brasileiros da área de Ciência da Informação*. Marília-SP. Universidade Estadual Paulista, 2005.

MOTA, Dardano do N., *Uma Concepção da relação entre o Terrorismo e a Guerra Cibernética no contexto da Guerra de Informação*. Instituto Universitário Militar. Portugal. Revista de Ciências Militares, Vol V, n. 01, Maio de 2017.

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

SINGER, Peter W. FRIEDMAN, Allan. *Segurança e Guerra Cibernéticas: o que todos precisam sabe*. Rio de Janeiro: Biblioteca do Exército, 2017.

TZU, Sun. *A Arte da Guerra*.19. ed. Rio de Janeiro: Record, 1997.

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

WELLS, H. G.. *A guerra dos mundos.* Tradução de Rodrigo Breunig. Porto Alegre (RS): LP&M Editores, [198?].

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

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

WOLOSZYN, André L.. *Terrorismo Global*. Rio de Janeiro: Biblioteca do Exército, 2010.

Recebido em: 22 ago. 2018
Aceito em: 19 nov. 2018

1 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)