DOI 10.21544/1809-3191.v25n2.p 517-543

A QUESTÃO CIBERNÉTICA E O PENSAMENTO REALISTA

Marcio Rocha[1]
Daniel Farias da Fonseca [2]

RESUMO

Esta pesquisa teve como objetivo analisar em que medida a teoria realista contribui para explicar a Questão Cibernética e a ocorrência de conflitos virtuais entre os Estados na atualidade. A pesquisa situa-se no contexto de que, nos últimos anos, vários Estados no Sistema Internacional passaram a atribuir às suas Forças Armadas a responsabilidade de Defesa não somente contra ameaças físicas, mas também contra aquelas com origem no espaço cibernético. O que justifica a pesquisa é a contribuição com a literatura existente sobre a temática cibernética que, na atualidade, ainda é relativamente reduzida. O estudo abordou o que caracteriza o conflito e o espaço cibernético, bem como esse fenômeno impacta a percepção de Segurança dos Estados. Foi realizada uma breve revisão sobre o pensamento realista e de suas premissas fundamentais. A conclusão da pesquisa aponta para uma aplicabilidade da lógica realista para a compreensão dos conflitos estatais em que atividades cibernéticas estejam presentes, de modo análogo ao que já ocorre em conflitos convencionais no Sistema Internacional, mesmo existindo uma certa resistência de alguns estudiosos dos conflitos interestatais, adeptos do pensamento realista, quanto à temática cibernética.

Palavras-chave: Questão Cibernética. Realismo. Defesa e Segurança. Estudos Estratégicos.

[1] Doutor. Universidade Federal Fluminense (UFF), Rio de Janeiro (RJ), Brasil. E-mail: marcioochamr@yahoo.com.br / *Orcid: https://orcid.org/0000-0003-0948-6863*.

[2] Mestrando. Universidade Federal Fluminense (UFF), Rio de Janeiro (RJ), Brasil. E-mail: danireload@gmail.com

INTRODUÇÃO

Esta pesquisa tem como objetivo analisar em que medida a teoria realista contribui para explicar a Questão Cibernética e a ocorrência de conflitos virtuais entre os Estados na atualidade.

É fato que o desenvolvimento e uso intensivo de avançadas tecnologias de transmissão e processamento de dados, levando a uma popularização e massificação de seu uso, à exemplo da Internet, e aliado ao processo de globalização, tornou o ciberespaço[3] o ambiente de ocorrência de inúmeros conflitos entre grupos políticos, grupos criminosos, empresas em geral e, também, entre os Estados. Sendo algo ainda recente, a compreensão do significado de espaço cibernético ainda está em desenvolvimento. Mas, também, é fato que ainda não existe controle ou domínio sobre o ciberespaço por um determinado país ou grupo de países. Isso nos leva a considerar que em um cenário de competição, conflito, ou mesmo guerra, ter a capacidade de invadir o ciberespaço de uma determinada instituição, ou país, permitirá conhecer mais sobre o mesmo e, se possível, obter o controle do mesmo, o que redundará em uma vantagem estratégica significativa para aquele que tiver tal capacidade. Na atualidade, não há como negar que o controle da informação ou de conhecimentos é um ativo estratégico para qualquer organização, empresa, ou Estado.

Nesse sentido, torna-se essencial, principalmente aos Estados, proteger suas informações e infraestruturas críticas. Em função do desenvolvimento e utilização de tecnologias de transmissão e processamento de dados cada vez mais avançadas, os Estados passaram a utilizar e depender de redes de computadores para enviar e receber dados, e promover a gestão de conhecimentos.

No caso específico das infraestruturas críticas, podemos entende-las como sendo aquelas infraestruturas que são vitais à sobrevivência do Estado e das quais ele possui grande dependência para seu funcionamento, tais como as usinas hidrelétricas, sistemas de comunicações e telecomunicações, sistemas de controle de tráfego aéreo, sistema bancário,

[3] Cyber é uma abreviação da palavra "cybernetic" (cibernético, em português), que se refere a algo ou algum lugar que possua grande concentração de tecnologia, principalmente redes, internet e computadores. Um fato interessante sobre a etimologia da palavra "cybernetic" é que se origina da palavra grega "κυβερνήτης", que significa "arte de governar" ou também a "arte de navegar".

etc. Utilizamos a definição do Governo Canadense para melhor explicitar o sentido de infraestrutura crítica:

> Infraestruturas críticas são o conjunto de sistemas, instalações, processos, redes, tecnologias, serviços e bens primordiais para assegurar a segurança, a saúde ou o bem-estar da sua população, assim como a eficácia do seu governo. O rompimento dessas infraestruturas pode ocasionar perda de vidas e efeitos econômicos adversos, além de prejudicar de maneira significativa a confiança do cidadão (CANADÁ, 2009, p. 2, tradução nossa).

Janczewski e Colarik (2008) defendem que o uso dessas redes de transmissão de dados provocou um aumento na eficiência e capacidade de atuação das empresas e Estados mas, também, ocasionou problemas de segurança em função de aumentar a automatização dos processos e da concentração das informações e dados mais importantes nos computadores.

> O uso desses sistemas e de redes significa que eles são agora uma grande fonte de concentração e centralização de recursos de informação. Essa consolidação criou uma maior vulnerabilidade para ataques e ações exploratórias. Durante os últimos 35 anos, a espionagem sobre os dispositivos eletrônicos, que geram riquezas econômicas, resultou no roubo de desenvolvimentos tecnológicos e militares, que mudou o equilíbrio de poder e continua a ameaçar a segurança e a estabilidade do mundo. (JANCZEWSKI; COLARIK, 2008)

Ou seja, os autores apontam para a existência de vulnerabilidades nos sistemas computacionais que se encontram em rede, assim como enfatizam que essas vulnerabilidades vêm sendo exploradas de maneira tal que ocorreram mudanças no equilíbrio de poder mundial, em uma referência indireta à capacidade da China de promover ações cibernéticas.

A constatação dessas vulnerabilidades, principalmente aquelas com potencial de ocasionar ameaças à Defesa Nacional dos Estados, obrigou um número considerável de países a utilizar suas Forças Armadas na defesa do espaço cibernético de seus interesses, capacitando-os ao desenvolvimento de ações tanto ofensivas quanto defensivas no espaço cibernético (TABANSKY, 2011).

Com essa lógica verifica-se que inúmeros Estados passaram a considerar que suas Forças Armadas, dentre suas atribuições

de Defesa, deveriam executar atividades para proteger seus países não somente contra ameaças físicas, mas também contra aquelas com origem no espaço cibernético (CAVELTY, 2012). O que explica essas decisões se deve ao fato de que, durante os últimos dez anos, houve um considerável aumento da ocorrência de ataques e de conflitos cibernéticos. Este aumento inclui aqueles que foram conduzidos por um Estado, e que tiveram como alvo algum país considerado como sendo um potencial inimigo (MILLMAN, 2018).

Nesse sentido, para alguns autores o espaço cibernético pode ser considerado, na atualidade, como um novo ambiente de atuação militar (KRAMER; STARR; WENTZ, 2009). Para eles, o espaço cibernético teria se tornado o quinto domínio de atuação militar, ao lado do terrestre, marítimo, aéreo e espacial.

Esta situação tem causado impactos consideráveis na área militar, afetando o escopo de suas tarefas e o modo pelo qual elas podem ser realizadas, passando a utilizar este ambiente para conduzir operações cibernéticas, que permitissem apoiar a realização de ações militares ou alcançar objetivos políticos (SHELDON, 2011).

Ainda necessitando de maiores análises e de uma melhor compreensão, o conflito entre Estados, envolvendo atividades cibernéticas, já conta com a atenção de estudiosos e pesquisadores das duas principais áreas acadêmicas voltadas para o estudo e pesquisa dos conflitos estatais: os Estudos Estratégicos e as Relações Internacionais.

No entanto, ainda verifica-se certa resistência, dentro das referidas áreas, quanto ao aprofundamento dos estudos das questões cibernéticas e como isso impacta o relacionamento entre os Estados. Isto se deve, principalmente, à predominância do pensamento realista dentre os pesquisadores dessas duas áreas, para os quais o tema Cibernética estaria fora do escopo a ser tratado por esta corrente de pensamento.

Foi nesse sentido que a questão de pesquisa que orientou este estudo esteve centrada em determinar em que medida a teoria realista contribui para explicar a Questão Cibernética, quando da ocorrência de conflitos virtuais entre Estados na atualidade.

O estudo teve um caráter exploratório e como base uma revisão bibliográfica sobre o tema em questão, devendo-se considerar que trata-se de um assunto recente, complexo, e que ainda apresenta limitações em termos teóricos e bibliográficos.

O que justifica esta pesquisa reside na possível contribuição

com a rarefeita literatura sobre o tema, bem como auxiliar na compreensão dos atuais conflitos estatais em que estiveram presentes ações cibernéticas ofensivas e defensivas.

A estrutura do trabalho ficou assim dividida: na primeira parte foi realizada uma análise sobre o significado de Questão Cibernética, espaço cibernético e a relação desses com aspectos da Defesa Nacional de alguns países; na segunda parte, foram abordados aspectos do pensamento realista, suas principais características e abordagens na análise de conflitos entre Estados no cenário internacional; e, finalmente, na terceira parte, foi desenvolvida uma análise de conflitos cibernéticos envolvendo Estados, tendo como referência o pensamento realista e determinando o nível de contribuição desta corrente do pensamento na abordagem e explicação dos conflitos estatais em que foram verificadas atividades cibernéticas.

A QUESTÃO CIBERNÉTICA

O período de surgimento do espaço cibernético pode ser apontado como sendo a década de 1970 com a criação da ARPANET[4]. Ela foi o primeiro sistema que possibilitou a conexão em rede de computadores, permitindo que eles pudessem se comunicar entre si e, assim, formando este ambiente (TABANSKY, 2011). O que justificou a criação da ARPANET remonta a uma necessidade do exército dos Estados Unidos de possuir uma rede de comunicações militares robusta e de longa distância (KREMER; MÜLLER, 2014). Assim, esta rede surge para atender e permitir a troca de informações entre equipamentos informatizados, fisicamente distantes, até mesmo no caso da ocorrência de um ataque nuclear, conforme a ótica dos Estados Unidos.

Para fins desta pesquisa, foi considerado que o espaço cibernético consiste em um ambiente virtual, composto pela informação, formado por redes de computadores que a transmitem e que interligam sistemas informatizados, através do qual a informação pode trafegar, ser armazenada, acessada e modificada (TABANSKY, 2011). Um dos

[4] ARPANET – A Advanced Research Projects Agency Network (ARPANET) foi uma rede de comunicações (inicialmente exclusiva para uso militar), criada para permitir a comunicação entre diferentes bases militares estadunidenses, localizadas em seu território ou não, e de seus sistemas informatizados, facilitando a transmissão de informações, a coordenação de suas ações, e aumentando a confiabilidade destas transmissões (KREMER; MÜLLER, 2014).

principais componentes deste ambiente é a Internet, ou seja, uma rede de comunicações global criada entre o final da década de 1980 e o início dos anos 1990 (CAVELTY; MAUER; KRISHNA-HENSEL, 2007). A Internet foi baseada nos protocolos e tecnologias desenvolvidas para a ARPANET, porém, seu uso era voltado para o meio civil. A Internet, assim como o próprio espaço cibernético, vivenciou um período de expansão, de popularização e do aumento de seu uso e de sua presença ao redor do mundo no final do século XX.

O espaço cibernético é amplamente utilizado, em âmbito mundial, em atividades diárias desempenhadas tanto pela população civil, quanto por empresas em geral e por governos. Seja através do uso da Internet, ou das Tecnologias de Comunicação e de Informação (TCI), ele se faz cada vez mais presente no nosso cotidiano (KREMER; MÜLLER, 2014).

Em função da importância e dos benefícios proporcionados pelo espaço cibernético, e como consequência deste fenômeno, especialistas começaram a enxergar que haveria um potencial para que perigos e ameaças pudessem surgir à partir do uso deste ambiente virtual (RIBEIRO; RIVERA, 2014). Acreditava-se que alguns deles, como por exemplo a ação de hackers e a propagação de vírus de computador, poderiam afetar negativamente as atividades essenciais dos Estados, especialmente no que diz respeito a sua segurança.

Os debates e as preocupações surgidas a partir deste prognóstico de insegurança deram origem ao que registramos como Questão Cibernética neste estudo. Portanto, para fins desta pesquisa, o entendimento de Questão Cibernética refere-se aos problemas potenciais e às consequencias para a sociedade e Estado, proporcionados pelo uso intensivo de avançadas tecnologias que dão suporte à transmissão e processamento de dados de interesse de instituições, empresas, grupos irregulares ou terroristas, e Estados. Esse processo levou a uma popularização e massificação de seu uso, bem como a consequente perda de controle sobre a mesma, permitindo sua utilização maléfica por pessoas, grupos diversos e mesmo Estados. A Questão Cibernética tem relação direta com os potenciais impactos negativos que as ameaças cibernéticas decorrentes podem ter, principalmente, para a Segurança e Defesa do Estado.

Por ameaças cibernéticas devemos entender as ações ofensivas e de intrusão virtual que possuem grande potencial para impactar ou comprometer a proteção dos Estados, seja ela física ou virtual. Este impacto pode ocorrer através do roubo de informações estratégicas e sigilosas, e da

condução de ataques e intrusões virtuais contra as infraestruturas críticas, cujo uso seja essencial para a realização de atividades relacionadas à Defesa do Estado. Neste caso, tais atos podem culminar com a destruição física e permanente dos mesmos, com a negação de seu uso ou com a sua inutilização, sejam elas de modo temporário ou indefinido. Essas ações podem incluir a interrupção de sistemas de comunicação, de posicionamento global, sistemas bancários, e de geração e distribuição de água potável, de combustíveis e de eletricidade, etc. (TABANSKY, 2011).

A falta de controle e o amplo uso do espaço cibernético torna possível que esses efeitos possam ser obtidos a partir da condução de atos de espionagem, sabotagem, e de ataque; possíveis de serem realizados através do espaço cibernético. Essas ações costumam ser realizadas através da invasão de equipamentos informatizados, ou de redes de computadores, com a finalidade de manipular informações armazenadas ou de ocasionar a interrupção de transmissões das mesmas. Dentre essas ações, destaca-se o ataque cibernético, em função do potencial destrutivo que possuí, bem como pela oportunidade que oferece para se conduzir conflitos cibernéticos.

O ataque cibernético pode ser definido como sendo "ações deliberadas para alterar, interromper, enganar, degradar, ou destruir computadores ou redes de informações e/ou programas que residam ou transitem por estes sistemas ou redes" (CAPLAN, 2013, p. 2). Este tipo de ataque possui o objetivo de ocasionar prejuízos e danos à terceiros, ao interromper — de forma temporária ou permanente — ou ao alterar a operação regular de um sistema alvo. Isto inclui copiar, apagar, ou alterar os dados que nele estejam armazenados, em outros conectados a este, ou que apenas trafeguem através dele (TABANSKY, 2011).

Na prática, os ataques cibernéticos podem ser utilizados para gerar danos materiais ou imateriais ao seu alvo, prejudicando a atuação do mesmo. Ele também possibilita impactar negativamente na segurança de um Estado, através da realização de intrusões virtuais que interfiram com o seu pleno funcionamento e de seus órgãos ou instituições.

Dentre essas consequências, destacamos a atuação das Forças Armadas, as quais se tornaram altamente dependentes do uso do espaço cibernético para suas operações cotidianas e relacionadas à proteção da pátria e ao preparo para participar de possíveis conflitos militares (MANESS; VALERIANO, 2016).

No caso das Forças Armadas, a dependência do espaço

cibernético está relacionada à necessidade e complexa atividade de obtenção e transmissão de informações em tempo real sobre as condições do campo de batalha, e à essencial coordenação das atividades de tropas e equipamentos bélicos de diferentes unidades militares envolvidas em batalhas. Esta dependência significa, também, que as Forças Armadas se tornaram significativamente suscetíveis às ameaças virtuais e aos impactos que elas podem ocasionar na condução de operações militares.

Quando relacionamos a atuação das Forças Armadas e o espaço cibernético, temos de considerar que um conflito cibernético pode ficar restrito apenas a ações realizadas no ambiente virtual, sem envolver o uso de ações militares tradicionais. Porém, ele também pode ocorrer de forma paralela a um conflito bélico em ambientes físicos, com o objetivo de apoiá-lo (TABANSKY, 2011).

O termo guerra cibernética é utilizado, de forma geral, para se referir a um possível tipo de conflito que pode ocorrer através do espaço cibernético. A guerra cibernética pode envolver o confronto de um ou mais Estados, além de grupos políticos ou criminosos diversos, e está baseada na exploração de brechas de segurança existentes nesse ambiente, com a finalidade de prejudicar o potencial adversário. Porém, ainda não se verifica a existência de um consenso, e que seja amplamente aceito por pesquisadores desta área e por estrategistas militares, sobre o que constituiria na realidade uma guerra cibernética. O mesmo questionamento existe para o fato de se considerar, ou não, se seria possível que um tipo de guerra pudesse realmente vir a ocorrer através do espaço cibernético. Por essas razões, este estudo abordou os conflitos cibernéticos de modo geral, porém sem entrar no mérito se eles podem ou não constituir um novo tipo de guerra.

O que os fatos recentes apontam é que conflitos cibernéticos podem oferecer vantagens ao Estado com capacidade para executá-lo, quando comparados com conflitos militares tradicionais. Isso está relacionado, principalmente, ao baixo custo dessas atividades e à dificuldade de se determinar a autoria e identidade de seus responsáveis, assim como de sua ocorrência. O que se destaca é que o caráter virtual desse tipo de conflito torna possível que seu responsável possa mascarar, ou ocultar, a sua verdadeira identidade, seja ele formado por um indivíduo, um grupo, ou um Estado.

Os países mais desenvolvidos constituem os alvos em potencial para ataques e conflitos cibernéticos. Quanto mais avançado tecnologicamente

é um país, mais dependente ele é do espaço cibernético. Assim sendo, o uso do espaço cibernético pode constituir uma vantagem militar a um adversário militarmente inferior, o que, em tese, pode constituir um meio relativamente barato e eficaz de minimizar a assimetria militar e torna-lo capaz de ocasionar danos significativos a um adversário mais poderoso.

Na atualidade, não existe nenhum órgão internacional que possua algum tipo de controle sobre a Internet como um todo (CAVELTY; MAUER; KRISHNA-HENSEL, 2007). Ela, que é um componente central do espaço cibernético, foi elaborada de uma maneira descentralizada, sem que fosse planejada a existência de uma única entidade global responsável por gerenciá-la (TABANSKY, 2011). Assim,

> A Internet é, portanto, um exemplo simples de um sistema sem limites, caracterizado por um controle administrativo distribuído sem que haja uma autoridade central, visibilidade limitada para além das fronteiras da administração local e uma falta de informações completas acerca da rede como um todo. (CAVELTY, MAUER e KRISHNA-HENSEL, 2007, p. 27)

Deste modo, o espaço cibernético é caracterizado pela condição de anarquia, ou seja, pela ausência de uma autoridade que seja hierarquicamente superior aos Estados e que tenha o poder de impor a sua vontade sobre eles (KREMER; MÜLLER, 2014). A condição de anarquia é um dos principais preceitos do pensamento realista e, também, um dos principais fatores para permitir a elaboração da lógica explicativa fornecida por esta corrente de pensamento. Esta lógica é a base para explicar as ações e os comportamentos adotados pelos Estados, durante e antes de conflitos militares que possam vir a ocorrer entre os mesmos, em um ambiente internacional marcado pelo fenômeno da anarquia.

Cabe ressaltar que esta corrente de pensamento não é a única abordagem teórica, ou linha de pensamento, relacionada à analise das Relações Internacionais. Poderíamos nos valer do pensamento da Escola Inglesa, do Neoliberalismo, da Teoria da Securitização da Escola de Copenhagen, ou do Construtivismo. Porém, o uso da teoria realista oferece uma abordagem mais adequada para a realização deste estudo. Quando aplicada a atuação dos Estados no espaço cibernético, ela permite auferir considerações mais amplas e genéricas, cujo escopo está associado a questões mais ontológicas, ou seja, em que se tem uma teoria mais geral (ACÁCIO; SOUZA, 2012).

O realismo identifica algumas características especificas do cenário internacional e aponta para o modo como elas podem influenciar o comportamento dos Estados. Em sistemas que sejam regidos pelos mesmos aspectos, ela poderia ser empregada para obter conclusões análogas.

O espaço cibernético possuí uma característica primordial que também está presente no Sistema Internacional (SI): a anarquia. Por este motivo, torna-se possível realizar uma aplicação desta teoria para analisar o comportamento dos Estados no espaço cibernético.

Segundo Reardon e Choucri:

> A teoria realista das Relações Internacionais é a mais aplicável a questões relacionadas à segurança cibernética e ao conflito cibernético. A teoria realista pode ajudar a explicar como os Estados usam tecnologias cibernéticas para avançar os seus interesses na área da segurança, e como eles podem responder às capacidades cibernéticas de outros Estados (REARDON; CHOUCRIL, 2012, p. 6).

Por esta razão, abordamos a seguir as principais características e a lógica que orienta o pensamento realista

O PENSAMENTO REALISTA

A Escola Realista das Relações Internacionais surge, na década de 1920, como uma forma sistematizada de estudo e de análise científica das Relações Internacionais e em um contexto pós-Primeira Guerra Mundial. O seu foco é compreender as dinâmicas, as características e as possíveis consequências da interação entre os Estados na arena política global, em especial, sobre as relações conflituosas entre eles. O objetivo do pensamento realista consiste em elaborar teorias e conhecimentos científicos que permitam compreender a racionalidade que influencia os conflitos entre os Estados e, principalmente, compreender e explicar quais seriam suas causas.

A teoria realista, assim como outras, possui como base um conjunto de premissas simples, que são utilizadas para tentar simplificar e explicar uma realidade complexa e multifacetada (LAKE, 2008). Acreditava-se que através de um estudo sistemático sobre o fenômeno da guerra, seria possível determinar as condições necessárias para evitá-las, e assim, possibilitar a existência e a garantia da paz entre os Estados (WALTZ, 2002). O seu enfoque, ao contrário de correntes pacifistas, não

era a promoção de um amplo desarmamento global, como meio de obter uma paz. Na visão deles, esta seria uma paz utópica e fadada ao fracasso (CARR, 2001).

Para os realistas a guerra seria um fenômeno recorrente no Sistema Internacional e que poderia afligir ou envolver qualquer país, variando apenas o motivo e o momento no qual elas poderiam ocorrer. O pensamento realista possui três premissas principais, as quais constituem o cerne e a base de seu pensamento e de suas análises. São fatores que garantem a esta corrente de pensamento o seu poder explicativo sobre a dinâmica de atuação e comportamento dos Estados no Sistema Internacional. Essas premissas são: 1) a centralidade dos Estados no ambiente internacional, ou a crença de que eles seriam os principais atores deste ambiente; 2) que buscam e priorizam satisfazer os seus próprios interesses; e, 3) que este ambiente é marcado pelo seu caráter anárquico.

A primeira característica, aquela que considera o Estado como o ator principal no âmbito das Relações Internacionais, está baseada na crença de que os Estados são os únicos atores que possuem um nível de poder, especialmente o relacionado ao poder militar, que permite a eles a capacidade de projetar poder sobre os demais e impor a sua vontade sobre os mesmos.

Para os realistas, o poder é formado por determinados aspectos chamados de recursos de poder ou de capacidades. No entanto, em muitas de suas análises, os recursos e as capacidades de um Estado são consideradas como sendo elas próprias um tipo de poder (BALDWIN, 2012). Eles acreditam que a principal capacidade que o Estado deve manter e aprimorar são as suas capacidades militares, também chamadas de Poder Militar.

Segundo Edward Carr

> A suprema importância do instrumento militar repousa no fato de que a última ratio do poder, nas Relações Internacionais, é a guerra. Todo ato do Estado, no aspecto do poder, está dirigido para a guerra, não como uma arma desejável, mas como uma arma que pode ser necessária como último recurso. (CARR, 2001, p. 143)

Possuir uma adequada capacidade militar seria o último recurso ao qual os Estados podem recorrer para enfrentar seus potenciais inimigos, ou para impor a sua vontade sobre os demais. Isso pode ocorrer tanto através do uso da violência, quanto da simples ameaça da imposição da força.

A segunda caraterística destacada pelo pensamento realista refere-se a um suposto egoísmo dos Estados na busca de atingir ou manter seus interesses. Ou seja, que eles priorizariam cumprir seus próprios objetivos políticos do que ajudar outros Estados.

Esta característica está baseada no fato de que a classe política de um Estado, e por consequência seus diplomatas, seriam pressionados pelo povo para atender, principalmente, ao interesse nacional e a promover o desenvolvimento nacional, inclusive através de negociações no âmbito internacional.

Já a terceira característica destaca a inexistência de uma autoridade, em âmbito internacional, que seja hierarquicamente superior aos Estados, e que tenha a capacidade ou o poder de impor a sua vontade sobre eles, sendo capaz de exercer algum tipo de controle sobre as ações desses.

Conforme enfatiza Aron, em um ambiente anárquico, a mera existência de outros países e o seu relacionamento podem vir a representar uma ameaça em potencial para eles próprios (ARON, 2002). Isto decorre da falta de clareza e de certeza da intenção desses Estados para com os demais. Neste cenário verificamos que, caso uma nação viesse a declarar guerra contra outro país, não existe nenhuma Instituição que tenha a função, ou responsabilidade, ou uma capacidade clara e definida de impedir este ato de guerra.

No pensamento realista haverá sempre a possibilidade de que uma guerra possa ocorrer a qualquer momento, assim que um país decidir recorrer a este ato, contra qualquer um dos demais.

No entanto, a anarquia não pode ser considerada como sendo uma causa direta da guerra, mas sim como sendo uma causa permissiva da mesma (WENDT, 1992). Em outras palavras, a anarquia permite que a guerra ocorra, uma vez que não há uma entidade capaz de impedir confrontos armados interestatais (WALTZ, 2001).

Neste cenário, os Estados seriam os únicos responsáveis pela sua própria segurança e capazes de enfrentar potenciais inimigos. Segundo Baylis e Wirtz:

> Na ausência de um governo mundial, realistas observam que os Estados adotaram uma abordagem de autoajuda para os seus interesses e especialmente a sua segurança. Em outras palavras, eles se reservam ao direito de usar força letal para alcançar os seus objetivos (BAYLIS; WIRTZ, 2002, p. 7).

Esta abordagem pode ser entendida como sendo a concepção de que para sobreviver cada Estado precisa contar, antes de mais nada, consigo mesmo (ARON, 2002). Esta atitude, decorrente da desconfiança para com os demais Estados, reforça o caráter egoísta atribuído aos mesmos pelos realistas.

Nesse contexto, os incentivos para que possa existir alguma forma de cooperação entre os Estados é muito reduzida. O que justifica esta postura dos Estados reside na inexistência de uma Instituição com autoridade e capacidade de aplicar uma punição àquele que viesse a desrespeitar o estabelecido pela sociedade internacional.

Segundo Wohlforth

> Quando não existe nenhuma autoridade que possa forçar o cumprimento de acordos — "anarquia" — então qualquer Estado pode recorrer à força para obter o que deseja. Mesmo que um Estado esteja convicto de que nenhum outro Estado vai recorrer à força hoje, não há nenhuma garantia contra a possibilidade de que um possa fazê-lo amanhã. Como nenhum Estado pode descartar esta possibilidade, Estados tendem a se armar contra esta contingencia. Com todos os Estados armados, a política toma uma forma diferente. Disputas que seriam facilmente resolvidas se os Estados pudessem recorrer a uma autoridade superior para forçar o cumprimento de um acordo podem escalar para uma guerra, na ausência desta autoridade. O típico argumento realista é que então a anarquia torna a segurança dos Estados problemática e potencialmente conflituosa, e que isso é a chave para compreender a causa da guerra (WOHLFORTH, 2008, p. 135).

Assim, temos que em um ambiente anárquico, onde Estados buscam satisfazer seus próprios interesses, há a constante possibilidade da ocorrência de uma guerra (WALTZ, 2001). Ou de acordo com Raymond Aron

> Toda política internacional importa um choque constante de vontades, por estar constituída por relações entre Estados soberanos, que pretendem determinar livremente sua conduta. Enquanto essas unidades não estão sujeitas a leis ou a um árbitro, elas são rivais, pois cada uma é afetada pela ação das outras, e suspeita inevitavelmente das suas intenções. (ARON, p. 100, 2002)

Esta situação influencia diretamente o comportamento dos Estados, levando-os a se sentirem constantemente inseguros, o que resulta

na busca para reforçar a sua segurança. Ao mesmo tempo, eles também buscam se preparar para a possível ocorrência de um conflito.

Ainda, segundo Morghentau

> Os preparativos militares, seja qual for a sua modalidade, têm por objetivo político fazer parecer demasiado arriscado para outras nações o emprego de força militar, dissuadindo-as, desse modo, de recorrer a tal recurso. Em outras palavras, os preparativos militares têm por alvo político tornar desnecessária a aplicação efetiva de forca militar, ao levar potenciais inimigos a desistir do recurso à força militar. (MORGENTHAU, 2003, p. 57)

Os preparativos militares podem ser compreendidos tanto como um esforço do Estado para defender seus interesses frente ao de outras nações, quanto para torná-la capaz de perseguir os seus próprios interesses no âmbito internacional. Dentre esses interesses e necessidades, encontra-se o de garantir a sua própria sobrevivência, bem como a segurança de seus cidadãos. Na prática, um Estado que possua um poder maior do que os demais pode ser capaz de subordiná-los à sua vontade. Caso a maior preocupação seja com a segurança estatal, poderá utilizar este poder para desestimular ameaças ou tentativas de ataques contra ele.

A busca da "segurança", pelos Estados poderosos, enseja os mesmos a perseguir políticas de poder (CARR, 2001). Uma vez que o poder que eles possuem sobre outros países é passível de sofrer alterações ao longo do tempo, isto contribui para que haja uma constante competição entre eles pelo poder.

Ou, segundo Raymond Aron:

> Supondo que a segurança seja o objetivo último da política dos Estados, o meio eficaz de alcançá-la será o estabelecimento de uma nova relação de forças, ou a modificação da relação existente, para que os inimigos potenciais não sejam tentados a tomar a iniciativa da agressão, devido à inferioridade do rival (ARON, p. 128, 2002).

A competição por incremento de poder entre os Estados é chamada pelos realistas de Dilema de Segurança, ou seja, aquela situação em que o aumento do poder de um Estado pode levar os seus vizinhos a buscar realizar esta mesma ação. Assim, nesta situação, países próximos

deste passariam a temer que esta ação pudesse sinalizar uma possível preparação para utilizá-lo contra algum deles, em um futuro próximo. Desse modo, os demais passam a temer pela sua segurança e buscam reforçá-la, ao replicarem este mesmo ato, de buscar aumentar o seu poder.

Considerando que o principal aspecto do poder dos Estados reside em seu Poder Militar, então o investimento e a capacidade de produzir conhecimentos e tecnologias bélicas torna-se essencial para a sobrevivência dos mesmos. Essas tecnologias impactam diretamente no nível da capacidade militar e, por consequência, no poder desses atores.

As tecnologias militares, de modo geral, influenciam na capacidade de atuação das forças militares, sendo capazes de aumentar a eficiência e o escopo de seu desempenho. Muitas vezes, a diferença entre o nível tecnológico das forças armadas de dois Estados pode ser decisiva no resultado das guerras. Segundo Hans Morgenthau "o destino de muitas nações e civilizações é frequentemente determinado por um diferencial na tecnologia das artes bélicas que o lado perdedor não foi capaz de compensar por outros meios" (MORGENTHAU, 2003, p. 237).

Porém, desde a segunda metade do século XX, os Estados têm cada vez mais envidado esforços para alcançar os seus objetivos políticos através do uso de meios diplomáticos e econômicos, e não através do uso da força. O principal motivo para isso, se deve aos elevados custos para realizar este tipo de ação, os quais recaem sobre aquele que opta pelo uso da força.

Assim sendo, a decisão de utilizar o poder, ou não, costuma envolver uma análise racional acerca do custo-benefício desta ação. Esta análise envolve tanto este tipo de ação – uso do poder -, quanto a comparação entre ela e outros cursos de ação possíveis, e que sejam viáveis de serem utilizados para se alcançar o mesmo objetivo político.

Mesmo assim, ainda existem consideráveis motivos para que os Estados reservem elevadas quantias de recursos para investir no preparo, na melhoria da eficiência e da atuação de suas Forças Armadas. Isto se deve, principalmente, à existência da possibilidade de exercer poder sobre os demais, através da simples ameaça do emprego da violência e de seus instrumentos. Caso o alvo desta ação acredite que é possível que ela seja cumprida, ele pode vir a ceder e a realizar a vontade daquele que teve a capacidade de promover a ameaça. Porém, a fim de tornar esta ameaça crível, é necessário possuir um Poder Militar superior àquele que o país ameaçado possua.

Na atualidade, e conforme mencionado anteriormente, no espaço cibernético também tem sido verificadas ocorrências de conflitos entre Estados, bem como da condução de operações militares com apoio de ações virtuais.

A capacidade de desenvolver ações ofensivas e defensivas no espaço cibernético pode ser considerada, hoje, como mais um instrumento de poder dos Estados. Assim, a capacitação Estatal de executar ações cibernéticas em apoio a operações militares, e considerando o caráter anárquico do espaço cibernético, possibilitam a aplicação do pensamento realista sobre conflitos virtuais entre Estados, seja sobre a sua ocorrência ou sobre os motivos que poderiam levar ao mesmo.

Na seção a seguir serão analisadas as abordagens que o pensamento realista dedica ao entendimento da Questão Cibernética na atualidade.

A QUESTÃO CIBERNÉTICA NO PENSAMENTO REALISTA

Os defensores do pensamento realista, de modo geral, defendem apenas o impacto que tecnologias bélicas possam ter para as atividades da guerra, bem como para a compreensão dos motivos que podem levar um Estado à Guerra. Deste modo, as tecnologias aplicadas à Internet e ao espaço cibernético, como um todo, costumam ser ignorados pelos realistas em suas análises. O mesmo tem sido válido para a análise de conflitos cibernéticos, assim como para as possíveis ameaças e impactos que possam surgir do ambiente cibernético onde eles ocorrem.

A possibilidade de um Estado obter ou utilizar algum tipo de poder, dentro ou através do espaço cibernético, é contestada pelos realistas. Para eles, um recurso virtual não poderia, por si só, influenciar ou ser utilizado para influenciar no comportamento de países. Deste modo, ele não poderia ser considerado como sendo um tipo novo de poder estatal.

Este tipo de conflito seria secundário e de menor importância, segundo os realistas, quando comparados com a guerra convencional, que pode ser realizada no ambiente físico. Inclusive questionam se ações ofensivas e defensivas virtuais poderiam realmente constituir um conflito.

Na ótica realista, isto se deve a primazia do uso de meios militares físicos para permitir que um Estado projete poder sobre um ou mais dos potenciais adversários, seja através da imposição de uma derrota militar

ou da mera ameaça de declarar uma guerra. Além disso, eles questionam o próprio uso deste termo, bem como da designação de guerra, para qualquer tipo de interação entre Estados ou não, que possa vir a ocorrer através do espaço cibernético.

A definição realista clássica de poder, ligada a aspectos militares e a outros que sejam relacionados a formas tradicionais dele, não permite levar em consideração a existência de suas novas formas (KREMER; MÜLLER, 2014).

Alguns realistas consideram o uso de ações ofensivas virtuais como sendo meros instrumentos pontuais em uma guerra tradicional, semelhantes a atos tradicionais de sabotagem. O enfoque principal desses realistas enfatiza o respeito às formas tradicionais de poder e de segurança de Estados, os quais são aspectos tradicionalmente relacionados ao seu próprio poderio militar. Assim, o uso de meios cibernéticos não poderia ser capaz de substituir conflitos tradicionais e nem de ser utilizado por si só. No máximo, as ações cibernéticas permitiriam potencializar o conflito do tipo convencional.

Deste modo, independente dos possíveis impactos que o espaço cibernético pode ter para com estes aspectos, os realistas não acreditam que seja necessário revisar as suas teorias e preceitos para conseguir compreender a segurança na era digital (JORGE, 2012). Ainda, segundo este autor:

> Os realistas, presumivelmente, combateriam o desafio da revolução da informação (...). Estas tendências são vistas como fenômenos secundários, que podem afetar as políticas e as estruturas domésticas dos Estados, mas que não enfraquecem o sistema anárquico da política internacional, e assim não afetam a primazia do Estado como a unidade política suprema. (JORGE, 2012, p. 19)

Na prática, a ressalva dos realistas com a temática cibernética diz respeito ao fato deles utilizarem uma definição mais restritiva dos conceitos de Segurança e Poder. Em tese, esses conceitos não permitiriam incluir aspectos relacionados ao espaço cibernético, ou a outros tipos de ameaça, e que possam afetar a soberania dos Estados na arena internacional. Para os realistas, a manutenção e a violação da segurança de um Estado diz respeito, principalmente, a aspectos relacionados às ameaças das forças militares convencionais. Portanto, executar estas ameaças por outros meios é algo que merece menor importância em seus estudos.

Porém, já se percebe na fala de alguns realistas mudança de postura quando o tema é a cibernética. Ou conforme Kremer e Muller, atualmente há uma tendência comum de que governos encarem ameaças advindas ou relacionadas ao espaço cibernético como desafios relacionados à segurança internacional e nacional (KREMER; MÜLLER, 2014). Ou seja, começam a surgir aqueles, adeptos do realismo, que desejam aplicar esta teoria para tentar explicar conflitos cibernéticos. Acreditam que o potencial que este tipo de conflito pode ter no futuro, envolvendo confrontos entre Estados, justifica esta aplicação.

Apesar de todas as restrições dos realistas a temática cibernética, conforme anteriormente mencionado, isso não significa que esta teoria seja incapaz de explicar esta nova realidade, ou que possa ser um meio inadequado para fazê-lo. A existência de semelhanças entre as características atribuídas pelos realistas ao ambiente internacional e as características presentes no espaço cibernético, tornam possível que realistas possam considerar, futuramente, incluir o estudo das ameaças originadas no espaço virtual como impactando o relacionamento entre os Estados.

Podemos verificar essa mudança de postura de Jan-Frederik Kremer e Benedikt Müller, quando afirmam que seria relevante para os realistas estudar o ambiente virtual, em especial a dinâmica dos Estados dentro dele. Ainda, que as ações realizadas dentro ou através dele podem afetar a distribuição de capacidades de países, o seu poder relativo e, desse modo, a sua sobrevivência no Sistema Internacional. Na ótica desses estudiosos, o espaço cibernético constituiria uma nova arena onde os Estados, e seus interesses, poderiam colidir, incluindo aqueles relacionados com a garantia de sua própria segurança ou de enfraquecer um possível adversário.

Ao analisar autores realistas que abordaram o espaço cibernético, Acácio e Souza concluíram que:

> os autores que puderam ser associados a um pensamento Realista sobre o ciberespaço, em geral, imaginam este campo como sendo um novo domínio operacional para a atuação dos Estados, em que estes deveriam projetar mais e mais poder e ganhar cada vez mais influência vis-à-vis outros Estados. (ACÁCIO; SOUZA, p. 8, 2012)

Nesse sentido, verifica-se que outros autores encaram o estudo do uso do espaço cibernético, para obtenção ou utilização de algum tipo

de poder, como uma possibilidade concreta. Para eles, este ambiente permitiria a existência de uma nova forma deste fenômeno, o qual recebeu o nome de Poder Cibernético, e que pode ser definido seguinte forma:

> Poder Cibernético é a habilidade de obter ganhos desejados através do uso de recursos de informação do domínio cibernético, que estejam eletronicamente conectados (NYE, p. 3, 2011).

De acordo com Nye, esses recursos incluem a Internet, computadores conectados em rede, intranets, ondas de rádio, cabos de fibra ótica, formas de comunicações baseadas no uso de satélites, e tecnologias de informação e comunicação (NYE, 2011).

Como exemplo de ações que integram e permitem que o Poder Cibernético possa ser exercido podemos citar os seguintes: ataques cibernéticos, espionagem cibernética, sabotagem cibernética, e conflitos cibernéticos. Alguns fenômenos, ocorridos recentemente, nos permitem verificar que alguns Estados já vêm utilizando uma ou mais dessas ações para conseguir obter benefícios próprios frente a outros países e através do uso de ações específicas no espaço cibernético.

Dois exemplos de atividades cibernéticas envolvendo conflitos entre Estados, e que tem sido veiculado na literatura, atualmente, referem-se aos Estados Unidos, Israel e Iran e, o outro, à Rússia e a República da Geórgia.

No primeiro caso, atribui-se aos Estados Unidos e Israel ações de sabotagem das centrífugas de enriquecimento de urânio do programa nuclear iraniano, ocorrido em 2010, quando foi realizado um ataque cibernético e tendo como resultado a destruição física das centrífugas.

Essa ação cibernética teria sido realizada com a finalidade e evitar a opção de uma ação militar com o mesmo objetivo. Ela foi vista como sendo uma ação menos arriscada e dispendiosa do que o emprego de tropas militares. Ela permitiu a consecução de um objetivo político de longa data dos Estados Unidos, o enfraquecimento do programa nuclear do Iran. Este programa era visto pelo governo estadunidense como sendo uma ameaça a sua segurança e aos seus interesses (JORGE, 2012).

No segundo caso, ocorrido em 2008, uma série de ataques cibernéticos foram realizados contra a Geórgia, supostamente pela Rússia, enquanto esses dois países se enfrentavam em um conflito militar.

Segundo alguns especialistas, uma primeira onda de ataques cibernéticos teria sido realizada contra os sistemas de comunicação e de transmissão de informações da Geórgia pouco antes do início da campanha

militar russa (HAGEN, 2012). Durante os primeiros dias dela, houve uma segunda onda de ataques, porém, desta vez em maior quantidade e com maior nível de sofisticação. (SHAKARIAN; SHAKARIAN; RUEF, 2013; HAGEN, 2012).

Esta série de ataques interferiu com a comunicação entre este país e o mundo exterior, durante o conflito com a Rússia. Ele teve um impacto na capacidade dos georgianos em acessar e transmitir informações, efetivamente isolando este país do mundo exterior (SHAKARIAN; SHAKARIAN; RUEF, 2013; HAGEN, 2012). Ela também afetou negativamente os sistemas de comunicação utilizados pelas tropas georgianas, interferindo com o seu uso. Isto teria dificultado a coordenação e a atuação destas tropas, consequentemente prejudicando o seu desempenho no campo de batalha.

Segundo alguns especialistas, estes ataques também teriam sido parte de uma operação de inteligência. Eles teriam permitido ao seu responsável acessar sistemas informatizados do governo e as informações armazenadas neles. Isto teria possibilitado a realização do roubo e acumulo de informações políticas e militares, que estivessem armazenadas nestes sistemas (HAGEN, 2012).

Muitos autores consideram que ele foi utilizado pela Rússia para apoiar a condução de suas operações militares e, que ele teria sido um dos fatores que contribuíram para a derrota militar de sua vítima. (SHAKARIAN; SHAKARIAN; RUEF, 2013). Segundo o governo georgiano, estes ataques cibernéticos teriam sido um dos fatores que contribuíram para a derrota militar que eles sofreram neste conflito (SHAKARIAN; SHAKARIAN; RUEF, 2013).

Este caso representou a primeira vez na história em que ataques cibernéticos, de larga escala, foram conduzidos em conjunto com uma grande operação de combate militar, tendo ambas o mesmo alvo (LANGNER, 2016; SHAKARIAN; SHAKARIAN; RUEF, 2013).

Os exemplos acima relatados, ao lado de inúmeros outros já registrados pela literatura, podem ser considerados operações estratégico-militares no espaço cibernético, e suscitam a ideia de que atores estatais utilizam tal ambiente como uma nova alternativa para o pressuposto realista-morgenthausiano da demonstração do poder (VILAR-LOPES, 2017). Assim sendo, o espaço cibernético pode ser considerado como "uma nova arena política na qual Estados podem agir, onde eles precisarem, a fim de projetar poder e influência sobre outros atores" (FERREIRA et al., 2015, p.03).

Esses exemplos nos apontam que, no espaço cibernético, os Estados teriam incentivos para buscar obter um determinado nível de poder cibernético. Os motivos para isso dizem respeito tanto à possibilidade de alcançar objetivos políticos quanto incrementar o nível de sua segurança estatal. Ainda, a busca pelo Poder Cibernético poderia ocorrer devido à percepção de que, este tipo de poder, poderia conceder àquele que tiver tal capacidade vantagens comparativas em relação àqueles que não possuem tal capacidade, tanto no campo militar quanto político.

Considerando as ameaças possíveis e presentes no espaço cibernético, e segundo o pensamento realista, o contexto da anarquia, também presente no espaço cibernético, pode contribuir para que os Estados busquem obter capacidade de projetar poder na arena virtual, sendo que essa postura pode ser explicada pela incerteza sobre as intenções dos demais atores.

Ao contrário das ameaças verificadas no mundo físico, não existem fronteiras físicas ou naturais no espaço cibernético. Assim, independente da distância física entre dois inimigos potenciais, na arena virtual as informações e ameaças decorrentes que podem fluir entre eles estão apenas a alguns segundos de distância. Nesta situação, é estabelecido um Dilema de Segurança virtual, no qual a incerteza quanto às reais intenções e possibilidades de um potencial adversário, obriga que Estados que percebam ameaças a seus interesses promovam ações para incrementar seu próprio poder na área cibernética.

Deste modo, pode ser considerado que o comportamento dos Estados dentro do espaço cibernético pode ser análogo àquele que eles desempenham no Sistema Internacional, dentro das concepções realistas. Ou seja, influenciado sempre pela busca do incremento de sua própria segurança e de um consequente aumento do seu poder frente aos demais atores. Isto se deve, principalmente, à existência de similaridades entre os ambientes físico e virtual, qual seja, a característica da anarquia, leva os Estados a desenvolver o seu potencial de utilizar o poder e seus instrumentos para subordinar outros à sua vontade, de modo a minimizar a possibilidade de ter a sua segurança comprometida por outro ator, bem como influencia a um desestímulo para que haja cooperação entre eles.

Destaca-se que, desde a década de 1990, é crescente o número de países que delegaram às suas Forças Armadas a tarefa de protegê-los dentro do espaço cibernético. Isso se deve, em parte, à crença de que estas Instituições se encontram melhor estruturadas e tenham melhor potencial

para assegurar uma adequada proteção nessa área. Neste caso, e não coincidentemente, tem ocorrido uma persistente discussão sobre o conceito de guerra cibernética, de cogitar agressões virtuais como possíveis atos de guerra, além de possíveis respostas por parte dos Estados e que poderiam ser consideradas legais e adequadas a esse tipo de ação.

Assim sendo, as evidências apontam que a Questão Cibernética tem afetado e influenciado o comportamento dos Estados no Sistema Internacional, especialmente no que se relaciona à busca de um Poder Cibernético compatível com os interesses estatais a serem preservados ou conquistados. Esta influência é possível de ser explicada e analisada pela teoria realista, constituindo esta teoria um valioso instrumento para possibilitar a compreensão desta nova realidade envolvendo os conflitos estatais.

CONSIDERAÇÕES FINAIS

Foi possível verificar, em relação ao comportamento dos Estados, a existência de significativas evidências de que estes tenham decidido, conscientemente ou influenciados por outros fatores, adotar uma postura similar àquela que já adotam no Sistema Internacional, segundo o enfoque realista, com relação ao domínio e uso do espaço cibernético.

No entanto, um adequado entendimento das ações e consequências, para os Estados, decorrentes da Questão Cibernética ainda depende de um maior aprofundamento em pesquisas e reflexões sobre o que representa este fenômeno, considerando que essas atividades são recentes. Nesse sentido, destacam-se os investimentos e os esforços de países mais avançados no desenvolvimento de avançadas tecnologias relacionadas à transmissão e processamento de dados, hardwares, softwares, capacitação de recursos humanos, centros de pesquisas, etc., e que possam garantir-lhes vantagens no Espaço Cibernético.

Porém, apesar desses esforços, o Espaço Cibernético ainda é um espaço que apresenta vulnerabilidades e que, de alguma forma, pode oferecer riscos àquilo que os Estados consideram como essencial à sua segurança, ou seja, a vulnerabilidade de suas infraestruturas críticas frente a ações cibernéticas ofensivas de potenciais adversários. Portanto, a Questão Cibernética é origem, também, de insegurança e fonte de conflitos entre Estados. Nesse contexto, a Questão Cibernética tornou-se um fator que influencia os Estados a uma constante busca de maior capacitação na

área cibernética, ou seja, obtenção de Poder Cibernético, tanto ofensivo quanto defensivo.

Os conflitos originados pela Questão Cibernética envolvendo os Estados, e considerando a característica de "anarquia" presente nessas atividades, nos permite uma relação com o que ocorre com os Estados no âmbito do Sistema Internacional. Assim, torna-se possível aplicar a lógica realista para a compreensão dos conflitos estatais em que atividades cibernéticas estejam presentes, bem como compreender a lógica e o comportamento dos Estados no ambiente cibernético.

Porém, o estudo mostrou que os realistas ainda oferecem certa resistência em valorizar as atividades e as consequências relacionadas à Questão Cibernética, pois consideram que, no âmbito e importância que a teoria realista atribui ao Poder Militar, aqueles fatores envolvendo o Estado e o Espaço Cibernético ainda estariam relegados a um segundo plano.

A lição que a pesquisa nos oferta é que, na atualidade, a obtenção e manutenção de um Poder Cibernético adequado às ameaças presentes no Espaço Cibernético não é mais uma opção, mas uma exigência frente aos interesses estatais a serem preservados em termos de Segurança e Defesa, o que nos impõe um aprofundamento nos estudos e reflexões sobre todos os aspectos relacionados com a Questão Cibernética.

THE CYBER ISSUE AND THE REALIST THOUGHT

ABSTRACT

This research had as objective to analyze to what extent the realistic theory contributes to explain the Cybernetic Question and the occurrence of virtual conflicts between the States at the present time. The research is in the context of the fact that in recent years several States in the International System have started to assign their armed forces the responsibility of defense not only against physical threats but also against those originating in cyberspace. What justifies the research is the contribution with the existing literature on the cybernetic subject that, at present, still is relatively reduced. The study addressed what characterizes conflict and cyberspace, as well as this phenomenon impacts the perception of State Security. A brief review was made on realistic thinking and its fundamental premises. The conclusion of the research points to an applicability of the realist logic to the understanding of the state conflicts in which cybernetic activities are present, analogous to what already occurs in conventional conflicts in the International System, even though there is some resistance from some scholars of the interstate conflicts, adepts of the realist thought, on the cybernetic subject.

Keywords: Cybernetic Issues. Realism. Defense and Security. Strategic Studies.

REFERÊNCIAS

ACÁCIO, Igor Daniel P; SOUZA, Gills Lopes M. Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço?. In: Encontro Anual da Anpocs, 36. Lindóia, São Paulo, 2012.
ARON, Raymond. Paz e Guerra entre as Nações. 1. ed. Brasília: Editora Universidade de Brasília, 2002.

BALDWIN, Stephen. Power and International Relations. In: Carlsnaes, Walter; RISSE, Thomas; SIMMONS, Beth. Handbook of International Relations. 2. ed. Londres: Sage Publications, 2012.

BAYLIS, John; WIRTZ, James. J. Introduction. In: BAYLIS, John; et al. Strategy in the contemporary world: an introduction to strategic studies. 1. Ed. Oxford: Oxford University Press, 2002.

CANADA. Sécurité publique Canada. Stratégie nationale sur les infrastructures essentielles, Ottawa, 2009. Disponível em: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-fra.pdf. Acesso em: 20 jan. 2017.

CAPLAN, Nathalie. Cyber War: the Challenge to National Security. Global Security Studies, v. 4, n. 1, p. 93-115, 2013.

CARR, Edward Hallett. Vinte anos de crise: 1919-1939 - Uma Introdução ao estudo das Relações Internacionais. 2. ed. Brasília: Editora Universidade de Brasília, 2001.

CAVELTY, Myriam Dunn; MAUER, Victor; KRISHNA-HENSEL, Sai Felicia. Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. 1. ed. Hampshire: Ashgate Publishing, 2007.

CAVELTY, Myriam Dunn; MAUER, Victor; KRISHNA-HENSEL, Sai Felicia. The militarization of Cyberspace: why less may be better. International Conference on Cyber Conflict, 4. 2012.

CRAIG, Anthony J. S; VALERIANO, Brandon. Realism and Cyber Conflict: Security in the Digital Age. In: ORSI, David E; AVGUSTIN, J. R; NURNUS, Max. Realism in practice: an Appraisal. 1. ed. S.l: E-International Relations,

2018.
DAHL, Robert A. The Concept of Power. Behavioral Science, v. 2, n. 3, p. 201-2015, jul. 1957.

FIGUEIREDO, Eurico de Lima. Estudos Estratégicos como Área de Conhecimento Cientifico. In: Revista Brasileira de Estudos da Defesa, v. 2, n. 2, p. 107-128, jul. 2015.

JANCZEWSKI, Lech J; COLARIK, Andrew M. Cyber Warfare and Cyber Terrorism. Hershey, PA: IGI Global, 2008.

JORGE, Bernardo Wahl Gonçalves de Araújo. Das "Guerras Cibernéticas". In: Anais do XI Ciclo de Estudos Estratégicos: Segurança e Defesa cibernética. Rio de Janeiro, 2012.

KRAMER, Franklin D; STARR; Stuart H; WENTZ, Larry K. Cyberpower and National Security. 1. ed. Washington: Potomac Books, 2009.

KREMER, Jan-Frederik; MÜLLER, Benedikt. Cyberspace and International Relations: Theory, Prospects and Challenges. Ed. 1. Nova Iorque: Springer, 2014.

LAKE, David A. The State and International Relations. In: Reus-Smit, Christian; Snidal, Duncan. The Oxford Handbook of International Relations. Oxford: Oxford University Press, 2008.

MANESS, Ryan C; VALERIANO, Brandon. The Impact of Cyber Conflict on International Interactions. Armed Forces & Society, v. 42, n. 2, 2016.

MILLMAN, Rene. Nation state cyber-attacks on the rise: detect lateral movement quickly. SC Media UK, 2018. Disponível em: https://www.scmagazineuk.com/nation-state-cyber-attacks-on-the-rise--detect-lateral-movement-quickly/article/746561/. Acesso em: 11 abr. 2018.

NYE JR, Joseph S. Power and National Security in cyberspace. In: LORD, Kristin M; SHARP, Travis. America's Cyber Future: security and prosperity in the information age. Washington: Center for a new American study, 2011.

MORGENTHAU, Hans J. A política entre as Nações: A luta pelo poder e pela paz. Brasília: Editora da Universidade de Brasília, 2003.

REARDON, Robert; CHOUCRIL, Nazli. The Role of Cyberspace in International Relations: A View of the Literature. In: ISA Annual Convention, 5. San Diego, Califórnia, 2012.

RIBEIRO, Vinicius G; RIVERA, César G. A inserção da segurança cibernética na agenda de segurança dos EUA no Século XXI. Século XXI, v. 5, n. 2, p. 135-150, 2014.

SHAKARIAN, Paulo; SHAKARIAN, Jana; RUEF, Andrew. Introduction to cyberwarfare: a multidisciplinary approach. Waltham: Elsevier, 2013.

SHELDON, John B. Deciphering Cyberpower: strategic purpose in peace and war. In: Strategic Studies Quarterly, v. 5, n. 2, p. 95-112, 2011.

TABANSKY, Lior. Basic Concepts in Cyber Warfare. Military and Strategic Affairs, v. 3, n. 1, p. 75-92, 2011.

VILAR-LOPES, Gills. Relações Internacionais cibernéticas (CiberRI): o impacto dos estudos estratégicos sobre o ciberespaço nas Relações Internacionais. In: Congresso Latinoamericano de Ciência Política, 9. Montevideo, 2017.

WALTZ, Kenneth J. O Homem, o Estado e a Guerra: uma análise teórica. 3. ed. Nova Iorque: Columbia University Press, 2001.

WENDT, Alexander. Anarchy is what States make of it: the Social Construction of Power Politics. International Organization. v. 46, n. 2, p. 391-425, 1992.

WOHLFORTH, William C. Realism. In: REUS-SMIT, Christian; SNIDAL, Duncan. The Oxford Handbook of International Relations. Oxford: Oxford University Press

Recebido em: 13/05/2019
Aceito em: 25/09/2019