https://doi.org/10.11606/issn.2446-5240.malala.2024.213860

A GUERRA CIBERNÉTICA SOB A ÓTICA DE CLAUSEWITZ: UM ESTUDO DE CASO SOBRE O STUXNET

CYBER WARFARE FROM CLAUSEWITZ'S PERSPECTIVE: A CASE STUDY ON STUXNET

Amanda Neves Leal Marini[1]
Lucas Chrystello Pederneiras[2]
Sandro Teixeira Moita[3]

Resumo: Nas pesquisas sobre Oriente Médio, há uma tendência e preponderância pelos estudos das guerras interestatais que assolam a região há décadas. Posto isto, nos últimos tempos, com o acelerado processo de desenvolvimento tecnológico e o impacto da relação entre ciência e guerra, os confrontos vêm adquirindo novos elementos, sem se afastar da máxima clausewitziana de que a guerra é a continuação da política com a entremistura de outros meios. Assim, na atualidade, o rápido progresso científico, com destaque às questões cibernéticas, apresenta componentes cruciais para se alcançar os objetivos militares e políticos em curso em uma guerra. Neste sentido, a presente pesquisa propõe responder a seguinte pergunta: o caso Stuxnet pode ser caracterizado como um ato de guerra, de acordo com a percepção clausewitziana? Assim, parte-se do entendimento clausewitziano de que a guerra é um ato político com o intuito de desarmar o oponente e impor sua vontade. Com base nisso, este artigo observa e analisa como o desenvolvimento deste worm se constituiu e foi aplicado, podendo compreender se confere como uma ocorrência de um ato de guerra. A hipótese desenvolvida e que se

Abstract: In research on the Middle East, there is a tendency and preponderance for studies of interstate wars that have plagued the region for decades. Having said that, in recent times, with the accelerated process of technological development and the impact of the relationship between science and war, confrontations have been acquiring new elements, without moving away from the clausewitzian maxim that war is the continuation of politics with the mixture of other ways. Therefore, nowadays, rapid scientific progress, with emphasis on cybernetic issues, presents crucial components for achieving the military and political objectives underway in a war. In this sense, this research proposes to answer the following question: can the Stuxnet case be characterized as an act of war, according to Clausewitz's perception? Thus, it is based on the clausewitzian understanding that war is a political act, with the aim of disarming the opponent and imposing their will. Based on this, this article observes and analyzes how the development of this worm is constituted and applied, being able to understand whether it constitutes an occurrence of an act of war. The hypothesis developed, which is intended to be corroborated, presents that Stuxnet

1. Doutoranda e mestra em Ciências Militares pelo PPGCM do Instituto Meira Mattos na ECEME, sendo bolsista CAPES. Graduada em Relações Internacionais pela UFF. Pesquisadora do Núcleo de Avaliação da Conjuntura/ Boletim Geocorrente, na área de Oriente Médio. Currículo Lattes: http://lattes.cnpq.br/2367832962491369. ORCID: https://orcid.org/0000-0003-2902-6901. Contato: amanda.nlmarini@gmail.com.

2. Mestre em Ciências Militares pelo PPGCM da ECEME e graduado em Relações Internacionais pela Unilasalle-RJ. Foi pesquisador da Unidade de Inteligência Comercial em parceria com a Subsecretaria de RI do RJ e autor do "Guia do Exportador Fluminense". Experiência em Geopolítica, Defesa e Segurança Cibernética. Currículo Lattes: http://lattes.cnpq.br/1742625560245256. ORCID: https://orcid.org/0000-0002-7596-8695. Contato: chrystellolucas@gmail.com.

3. Doutor em Ciências Militares pelo PPGCM da ECEME. Graduação e licenciatura em História pela UFF (2007), Especialização em História Militar Brasileira (2011) e Mestrado em História (2013) pela UNIRIO. Currículo Lattes: http://lattes.cnpq.br/1223210921186615. ORCID: https://orcid.org/0000-0003-4795-3880. Contato: sandrotm@gmail.com.

pretende corroborar, apresenta que o Stuxnet pode ser caracterizado como um ato de guerra, ao levar em consideração que fora um ato político com o intuito de compelir seu propósito ao adversário. Os resultados revelam uma abordagem contemporânea, sem ignorar as contribuições do passado, ao ressaltar esta relação entre guerra e tecnologia cibernética. A partir desse panorama, o trabalho consiste em uma discussão e análise crítica, utilizando um estudo de caso único sobre o Stuxnet, visando trabalhar com esse episódio, que teve como principal alvo o Irã, no início da década de 2010.

Palavras-chave: Cibernética; Ciências Militares; Clausewitz; Oriente Médio; Stuxnet.

can be characterized as an act of war, taking into account that it was a political act with the intention of forcing its purpose on the opponent. The results reveal a contemporary approach, without ignoring the contributions of the past, by highlighting this relationship between war and cyber technology. Based on this panorama, the work consists of a discussion with a single case study, in the area of Military Sciences, aiming to work with the Stuxnet episode that had Iran as its main target, in the early 2010s.

Keywords: Clausewitz; Cyber; Middle East; Military Sciences; Stuxnet.

Introdução

O presente trabalho constitui-se como uma pesquisa exploratória no âmbito das Ciências Militares, tendo como recorte o episódio do Stuxnet, um *worm*[4] que, no início dos anos 2010, atacou importantes centrífugas de enriquecimento de urânio no Irã. Neste sentido, a presente investigação propõe responder a seguinte pergunta: o caso Stuxnet pode ser caracterizado como um ato de guerra, de acordo com a percepção clausewitziana? Assim, parte-se do entendimento clausewitziano de que a guerra é um ato político com o intuito de desarmar o oponente e impor sua vontade. Com essa perspectiva em foco, é possível observar e analisar a configuração e a aplicação do *worm* em desenvolvimento, a fim de avaliar se pode ser considerado um ato de guerra.

Portanto, o propósito geral consiste em determinar se esse ataque cibernético pode ser classificado como uma ação de guerra. Para isso, recorreu-se a obra Da Guerra, de Clausewitz, como referencial teórico, assim como leituras e interpretações dos principais estudiosos sobre o pensamento do militar prussiano. Os objetivos específicos, a saber, são: contextualizar a conceituação dos termos apresentados, que perpassam desde os campos cibernéticos e militares; compreender o que foi o Stuxnet, em termos políticos, e os seus impactos na dinâmica regional. A hipótese trabalhada e que se pretende corroborar, apresenta que o Stuxnet pode ser caracterizado como um ato de guerra, de acordo com a percepção clausewitziana, ao levar em consideração que foi um ato político com o intuito de impor sua vontade ao oponente. Em outros termos, configura-se como um elemento político por outros meios, estes, tecnológicos. Os resultados mostram uma perspectiva atualizada, levando em consideração as influências do passado, ao lidar com a interação entre guerra e tecnologia cibernética.

4. *Worm* é um programa de computador malicioso que se replica e se espalha por conta própria, explorando vulnerabilidades de segurança em sistemas e dispositivos conectados sem a ação ou ajuda externa de um usuário (Belcic, 2020).

O procedimento de pesquisa empregado consiste na revisão conceitual da definição de guerra e a posterior análise de concepções do escopo cibernético, por meio do levantamento e pesquisa bibliográfica feitas nos principais sites e bases de dados acadêmicos. Também se recorreu a aplicação do estudo de caso único, com base nos itens basilares propostos por Gerring (2007) e George e Bennett (2006). O uso desta técnica deve-se ao fato de que tenciona mostrar e analisar como questões que, muitas vezes, são tão teóricas, acontecem, são postas em prática, além de ilustrar a dimensão do debate proposto: a guerra cibernética. Este fenômeno marca o acontecimento de ações do ciberespaço e questões mais tradicionais de Estratégia Militar, estando no âmbito e perpassando o espectro das Ciências Militares.

Dentro deste panorama, entende-se que, quando se trata de Cibernética, especialmente no campo da Política Internacional e das Ciências Militares, é substancial discorrer e debater as conceituações, visto ser uma área onde há muitas discordâncias e poucos consensos em termos conceituais. Assim sendo, expor e identificar as sustentações investigativas das quais parte a presente investigação se torna primordial. Em síntese, devido a este cenário, optou-se por trabalhar a designação e compreensão conceitual dos termos deste estudo.

> Em todas as áreas científicas, a definição conceitual é central, e por isso ocupa espaço nobre na produção científica. Porque, por um lado, a precisão conceitual fornece a univocidade que permite a comunicação compreensiva da atividade científica e, por outro, porque o conceito bem definido deve garantir o acesso instrumental àquela parte da realidade que se pretende analisar. Todavia, na área específica da segurança, essas normas se tornam dramáticas, pois às considerações epistemológicas anteriores soma-se o fato de que esses conceitos se tornaram operativos no discurso político com consequências políticas e sociais pelas quais os acadêmicos nem sempre se responsabilizam. (Saint-Pierre, 2011, p. 426) (grifos nossos).

A respeito do porquê usar um episódio que ocorreu há mais de uma década, encontra-se base e legitimação nas próprias palavras do teórico prussiano, que afirmou que: "*Os exemplos históricos esclarecem tudo e também fornecem o melhor tipo de prova nas ciências empíricas. Isto é particularmente verdadeiro no que diz respeito à arte da guerra. O General Scharnhorst*[5]*[...] considera os exemplos históricos de primordial importância para o assunto, e faz deles um uso admirável*" (Clausewitz, 2007, p. 124) (tradução nossa)[6]. Sobre a importância da utilização de um episódio histórico, ao longo da análise teórica, percebe-se que os casos históricos têm a vantagem de serem mais realistas e dar vida às ideias que representam (Clausewitz, 2007).

5. Gerhard von Scharnhorst (1755-1813) foi um importante general prussiano que, além de ter lutado nas Guerras Napoleônicas, foi chefe do Estado-Maior da Prússia. Seus estudos e pensamentos a respeito da reforma do exército prussiano impressionam, influenciando no pensamento de Clausewitz, de quem foi tutor.

6. Historical examples clarify everything and also provide the best kind of proof in the empirical sciences. This is particularly true of the art of war. General Scharnhorst [...] considers historical examples to be of prime importance to the subject, and he makes admirable use of them" (Clausewitz, 2007, p. 124).

Por fim, a argumentação e relevância desta temática reside em ser um episódio histórico, tido como marco nos estudos de cibernética, além de servir como evidência e manifestação da competência dos instrumentos cibernéticos em sensibilizar infraestruturas críticas estatais, consoante ao que será analisado ao decorrer desta pesquisa.

Introdução ao conceito Clausewitziano de guerra

Como já apresentado, esta investigação opta por trazer a definição conceitual dos termos utilizados, para depois traçar uma análise sobre o que fora proposto. A escolha da obra Da Guerra, de Carl von Clausewitz, como referencial teórico, reside no fato de ser o primeiro esforço minucioso de designar uma teoria sobre a guerra, além de promover e trazer importantes compreensões para as Ciências Militares e a maneira pelo qual se enxerga a guerra. A primazia desta obra reside, além da grandeza do pensamento de Clausewitz, também ao fato de que, como aponta Proença (1999, p. 72-73): "*Da Guerra sistematizava o conjunto de suas reflexões sobre a guerra e as enquadra num arcabouço teórico de grande envergadura*."

Carl von Clausewitz (1780-1831) é considerado como um dos maiores estrategistas e teóricos de guerra de todos os tempos. Grande parcela dos seus escritos sobre a guerra foram refletidos a partir da sua experiência nas Guerras Napoleônicas. O axioma mais famoso do seu trabalho apresenta a guerra como sendo a continuação da política por outros meios. Ele também a descreve como um camaleão, em função da rápida adaptação das suas características. Fundamentado no pensamento Clausewitziano, Paret, Howard e Brodie (1984, p. 59) ponderam que: "*a guerra é diferente de qualquer outra coisa. Assim, por mais que ela possa mudar em si mesma de uma época para outra, as suas características essenciais permanecem distintas de todas as outras atividades do homem*."

Embora o estudo da guerra desenvolvido na sua obra tenha moldado o pensamento militar ocidental, desde a década de 1990, há questionamentos e críticas, especialmente, no que se refere aos conflitos contemporâneos e a sua capacidade de resposta frente a ameaças intraestatais. Grande parcela destes questionamentos se fundamentam em razão de que, com o término da Guerra Fria, novas ameaças, oriundas de atores não-estatais, como, por exemplo, grupos paramilitares, terroristas, fundamentalistas religiosos, entre outros, obtiveram maior projeção no Sistema Internacional. Ademais, de acordo com Buzan e Hansen (2012), neste espaço temporal, a área de estudos de Segurança e Defesa foi alargada e novas temáticas foram incorporadas, como, por exemplo, o papel da cibernética na política internacional. E assim, neste escopo, "*com o fim da Guerra Fria, a suposição clausewitziana de que a guerra é um ato de força destinado a realizar os objetivos da política passou a ser cada vez mais contestada*" (Hew Strachan, 2008, p. 12).

Nessa situação, transcorreram muitas discussões em torno de se a obra de Clausewitz continuaria sendo um trabalho atual e relevante, com ênfase às teses de pensadores como

John Keegan (2006), Mary Kaldor (1999), La Maisonneuve (1998) e Martin Van Creveld (2011). Eles argumentam sobre a relevância de ponderar a guerra como sendo não apenas um embate entre atores estatais e suas respectivas Forças Regulares, com vistas a alcançar um determinado objetivo político, como proferido, principalmente por Clausewitz (2007), mas também endossado por Aron (1986) e Tilly (1975). Muitas críticas dessas, além de derivarem de uma interpretação seletiva e descontextualizada, consideram que a guerra é estritamente uma forma de violência e não de força, esta última apresentando diferentes facetas, conforme teorizado por Clausewitz. Outro aspecto a ser considerado é que a violência deve ser entendida como um resultado da força e não como um sinônimo absoluto e irrestrito de uma convocação ou de um ato de guerra (Stone, 2013; Echevarria, 2007).

Outrossim, estes acadêmicos pretendiam e defendiam que seria a emergência de um novo contexto, requerendo dois tipos de guerra, a "velha" e a "nova", esta respaldada, em grande parte, por conflitos, em sua grande maioria, intraestatais, interpretados, cada vez mais, por entes não-estatais, concedendo um caráter irregular ao teatro de operações. Em síntese, os autores, previamente apresentados como críticos, pontuaram que neste novo momento geopolítico, entes não estatais protagonizam papéis de destaque na condução dos conflitos bélicos. Por fim, estas teses também se apoiavam no fato que as, então, "velhas guerras" seriam aquelas enfrentadas pelos Estados e suas respectivas Forças Armadas convencionais, oriundas do momento da Era Industrial (Mahnken; Maiolo, 2014; Gray, 2009).

Ainda neste embate, um ponto em que a crítica se fundamenta é que com o término da bipolaridade e a emergência dos atores não estatais, a interpretação da Trindade Notável ou Paradoxal, a depender da tradução e literatura, apresentada por Clausewitz, funcionaria como um sinal de declínio do seu pensamento, uma vez que os atores apresentados são o povo, o governo e as Forças Armadas. Dentro desta visão, vislumbravam que as forças rebeldes não se encaixariam, nem seriam descritas nestas categorias. Mas, essa visão coloca ênfase nas variáveis da trindade secundária, as instituições, e não na primária, que são os elementos e emoções que perpassam a síntese da sua obra, a saber: violência, ódio e inimizade, que podem ser encontradas também como paixão, força natural cega ou cego impulso natural, animosidade, jogo do acaso e da probabilidade, gênio, razão e política. Desse modo, funcionam como entes interligados, entre os quais o confronto se move, seguindo constantemente seu vínculo e propensão (Clausewitz, 2007; Echevarria, 2007; Souchon, 2020; Stone, 2007; 2018).

Além do mais, por mais que exista uma visão de correlação direta entre a trindade primária e secundária, estas tendências não devem ser vistas como exclusivas, irrestritas e rigorosamente dirigidas a cada um dos entes, e sim como variáveis presentes no contexto da guerra como um todo. Com base no exposto, a guerra sob a óptica Clausewitziana é o resultado das associações e coeficientes complexos e mutáveis, que são empregados nos teatros de operações. Desse modo, estas ideias continuam sendo instrumentos analíticos fundamentais

para a análise da teoria da guerra. Por fim, regressa-se e correlaciona-se ao entendimento de que a guerra é mais do que um verdadeiro camaleão que altera suas características, atributos ao meio em que está exposto, mas é também como um conjunto de disposições e propensões que nele predominam (Clausewitz, 2007; Souchon, 2020; Stone, 2018).

Neste sentido, observa-se que a questão dos críticos de Clausewitz, na contemporaneidade, têm como fulcro uma leitura seletiva e pouco precisa da obra, tomando posse de expressões, compreensões e até mesmo parágrafos e lições isoladas, fora do contexto, deturpando o entendimento exposto na obra, assim não se atentando à grandeza do texto, cujo alcance atemoriza. Esta questão possui relação com o fato de que há uma certa herança de engendrar em Clausewitz, o que ele pretendia dizer ou escrever, trazendo, muitas vezes, interpretações e análises distorcidas, errôneas, díspares e ambíguas. Aliás, sobre o contexto temporal, o militar prussiano afirmara que quem se fundamenta apenas nas perspectivas do seu próprio momento histórico está fadado a tratar o que existe de mais atual como sendo o melhor, se ofuscando do que vem anterior e posteriormente, achando improvável atender o que é diferente (Handel, 2014; Hew Strachan, 2008; Gray, 2009).

Por fim, elementos apresentados em sua obra como fricção, fatores morais, acaso, centro de gravidade e incerteza continuam influenciando o desenrolar do conflito e a análise trinitária; além de ser a síntese do seu parecer, é relevante para entender todos os tipos de guerra, bem como sua ênfase na natureza política. Dentro deste contexto, Hew Strachan (2008, p. 31) retrata que: "*a relevância das ideias de Clausewitz hoje vai além da prevalência de guerras civis e conflitos entre atores não-estatais."* Assim, ilustra-se que a coerência das conceituações de Clausewitz, hoje, percorrem o predomínio de guerras civis e conflitos entre atores não-estatais, e não estão obsoletas, como defendido por alguns teóricos. Dessa maneira, esta relação se torna apropriada e procedente em todos os tipos e para guerras de quaisquer características, e não apenas interestatais. Vale ressaltar que Colin Powell, Chefe do Estado-Maior das Forças Armadas dos Estados Unidos, entre os anos de 1989 e 1993, citou que o pensamento Clausewitziano exposto em Da Guerra é *"como um raio de luz vindo do passado e que ainda ilumina as perplexidades militares do presente."* Desse modo, é admirável compreender que os apontamentos e considerações de Clausewitz possuem capacidade de resposta e continuam atuais, mais de um século e meio após sua publicação (Hew Strachan, 2008; Handel, 2014).

Um outro aspecto diz respeito às rápidas mudanças tecnológicas na indústria bélica[7], estas que transformaram a compreensão da natureza de guerra em algo ainda mais denso do que na época em que o pensador prussiano desenvolveu sua teoria. Clausewitz sobrepujou as delimitações aplicadas por percepções da conjuntura política e tecnológica da sua

7. Outrossim, a questão tecnológica transcorre da interpretação e execução da guerra, em virtude da relação existente entre estes elementos (confrontos armados e avanços tecnológicos), uma vez que Paret (2001, p.103) analisa que, *"a ciência e a guerra sempre estiveram intimamente ligadas"*.

época. Assim, compreender a guerra ainda exige muito mais explicação, e talvez, a lição mais importante, obtida a partir da obra Da Guerra, é que o confronto bélico pode ser estudado com um espírito diferente (Howard, 2002; Paret, 2001; Souchon, 2020).

Correlação entre as conceituações de guerra e política

Clausewitz discorre que a guerra é a continuação da política com a entremistura de outros meios, tendo por objetivo desarmar, aniquilar, destruir as forças do oponente. "*A intenção deve ser danificar as forças do inimigo de modo que ele não possa levar a guerra adiante ou não possa fazê-lo sem perigo para si [...] destruir o exército do inimigo*" (Hew Strachan, 2008, p. 76). O militar prussiano manifesta que um ato de guerra é sempre político, nunca isolado, e que o objetivo deve ser tornar o inimigo indefeso, para forçar e impor que o oponente aceite sua vontade, assim, cegando, temporariamente, os comandantes e até mesmo os estrategistas militares em relação ao intuito mais amplo da guerra, correlacionando com a compreensão sobre a Trindade, exposta anteriormente.

A relação dialética existente e exposta entre guerra e política, deve-se ao fato de que o propósito, objetivo político e o alvo militar coincidem. Dentro deste cenário, o prussiano não esclarece a guerra como um caso independente, tampouco deve ser entendida de forma isoladamente da política, mas sim como algo a ser depreendido como parcela de uma referência maior, que é a política. Em síntese, para além dessa definição, toda guerra, por estar submersa no âmbito político, é circundada pelo meio apresentado, e torna-se crucial analisar a conjuntura e o papel da política, enquanto uma ferramenta, ao investigar os pormenores e particularidades que caracterizam um confronto armado (Herberg-Rothe, 2007; Rid, 2014; Hew Strachan, 2008).

Portanto, visto o caráter significativo da ingerência da política na guerra, esta relação dialética foi central nos desenvolvimentos das observações de Clausewitz. Esta relação posiciona a guerra, rigorosamente, e com ênfase no campo da política, convertendo a teoria de guerra em mais científica e metódica. Assim, em outras palavras, observa-se a natureza subordinada do instrumento político, por via do qual, ela confere mais rigor à cientificidade da sua teoria da guerra (Hew Strachan, 2008; Stone, 2007; 2018).

Logo, por meio deste entendimento e perspectiva, pode-se inquirir se o desmantelamento de infraestruturas críticas (ICs), sensíveis e estratégicas para um país, pode ser conceituado como um esforço de guerra, como o *worm* Stuxnet, que acometeu e comprometeu o enriquecimento de urânio do país persa. Dentro deste âmbito, vale pontuar que, para Clausewitz, as guerras emanam de intuitos políticos, sendo útil ao analisar o Stuxnet, visto que aproxima a teoria formulada no século XIX a um evento do Sistema Internacional no século XXI, corroborando para a atualidade do pensamento Clausewitziano. Dessa maneira, entende-se de maneira prática e por meio da análise de um exemplo sobre o objetivo da guerra, impor a vontade ao adversário e destruir sua capacidade de resposta.

Por fim, observa-se que a política certifica racionalidade à guerra, visto que uma vitória militar está às ordens de um fim político impor sua vontade, como observado, e a ênfase da primazia da política na condução da guerra. Não é possível entender o fenômeno guerra, a partir da perspectiva Clausewitziana, sem compreender a política que o permeia.

Introdução ao domínio cibernético: conceituando e fundamentando o ciberespaço

Antes de se aprofundar sobre o episódio do Stuxnet, é de grande importância apresentar as definições e fundamentos do espaço cibernético, a fim de compreender o ataque cibernético estudado neste artigo. Primeiramente, deve ser entendido que o conceito de ciberespaço não é algo absolutamente definido, ou seja, ainda há um debate entre pesquisadores sobre o conceito conclusivo acerca deste domínio[8]. Porém, é concreto afirmar que o espaço cibernético possui um papel fundamental no desenvolvimento econômico e social, dada à ubiquidade e dependência crescente por parte da sociedade, das empresas e dos Estados, permitindo, por exemplo, desde a simples interação em redes sociais, à administração de um crítico sistema de uma instalação de energia elétrica. Em outras palavras, o ciberespaço virtualiza a economia e a sociedade, o que, consequentemente, leva ao surgimento de novas vulnerabilidades, não exclusivamente à defesa do Estado, como também à segurança da sociedade e das empresas. Isto é alcançado pelo fato das Infraestruturas Críticas (ICs), como as de água, energia, telecomunicações, finanças, transportes e comunicação, serem administradas no espaço cibernético devido às dependências administrativas e gerenciais das ICs das redes de informação. Portanto, estas estruturas também fazem parte do ciberespaço, que caso danificadas ou paralisadas, ocasionarão sérias consequências multifacetadas, sejam elas econômicas, sociais ou políticas, exigindo que este domínio seja assegurado e apropriadamente estruturado pelo Estado (Canongia; Mandarino, 2009; Pinto; Grassi, 2020).

A discussão sobre o conceito de ciberespaço é relativamente recente, pois considera-se a concepção de William Gibson, autor de ficção científica, sendo a primeira de todas. Em 1984, em seu livro intitulado "*Neuromancer*", quase 40 anos após a criação do primeiro computador e 15 anos após a ARPAnet (Rede da Agência de Pesquisas em Projetos Avançados dos Estados Unidos) transmitir uma informação em uma rede em 1969, Gibson poeticamente conjecturava o mundo cibernético.

> O ciberespaço. Uma alucinação consensual, vivida diariamente por bilhões de operadores legítimos, em todas as nações, por crianças a quem estão ensinando conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas que abrangem o universo não-espaço da mente; nebulosas e constelações infindáveis de dados. Como luzes de cidade, retrocedendo. (Gibson, 2014, p. 83).

8. Nota-se que os termos: espaço cibernético, ciberespaço e domínio cibernético, utilizados neste artigo, possuem a mesma expressão de sentido.

Neste panorama, utilizando-se autores mais recentes, as definições mais usadas geralmente gravitam em torno da segmentação de camadas do domínio cibernético. Para Kuehl (2009), por exemplo, o ciberespaço, em síntese, é interpretado como um domínio global dentro do ambiente informacional, estritamente operadas pelo homem, onde o uso do espectro eletromagnético e de equipamentos eletrônicos em uma rede virtual interdependente, são usados para analisar, produzir, modificar, permutar e armazenar informações. Ao longo de seu artigo intitulado "*From Cyberspace to Cyberpower: Defining the Problem*", o autor aponta também que há inúmeras definições para o domínio cibernético (Kuehl, 2009), ressaltando que a definição básica do conceito de ciberespaço não é consolidada.

Desse modo, utilizando os mesmos princípios sobre camadas que compõem o domínio cibernético, Libicki (2009), em seu livro "*Cyberdeterrence and Cyberwar*", indica que o ciberespaço é composto por três camadas: a física, a sintática e a semântica. Em primeiro lugar, a camada física é representada como o componente material do ciberespaço, exemplificado pela transmissão e armazenamento de dados por sistemas de informação via fios, cabos e satélites. Em segundo lugar, a camada sintática, representada pelos códigos e informações enviados entre os sistemas de informação. E por último, a camada semântica, que detém as informações contidas nas máquinas.

Ventre (2012), se aproximando da definição apresentada por Libicki (2009), divide o ciberespaço similarmente em três camadas: as superiores, médias e inferiores. As camadas inferiores e médias de Ventre correspondem respectivamente à camada física e sintática de Libicki. Contudo, na camada superior, o autor define como o usuário, ou seja, a interação humana com ciberespaço, desenvolvendo o argumento que o ser humano estabelece as infraestruturas, programa e opera o ciberespaço. Neste sentido, Ventre (2012) se diferencia de Libicki (2009), ao colocar o ser humano em evidência neste domínio, determinando que, para que este domínio exista, é necessário que o homem o construa, desenvolva e opere.

Destarte, a partir destes conceitos, percebe-se, sobretudo, que o domínio cibernético é um espaço exclusivamente artificial que pode ser entendido como uma sobreposição de camadas, sendo também estritamente criado e operado pelo homem a partir da evolução das tecnologias de informação e comunicação (TIC). Tendo isto compreendido, entende-se que cada país tem seu grau de inserção neste domínio por se tratar de uma dependência em investimentos e no desenvolvimento em TIC, infraestrutura e mão de obra qualificada. Desta forma, quanto mais um país é considerado desenvolvido, maior será sua dependência do espaço cibernético, que, por uma consequência lógica, maior deverão ser seus investimentos em segurança e defesa cibernética, não apenas visando o pleno funcionamento do Estado, como também assegurar a realização de seus objetivos nacionais.

Após esta breve introdução acerca dos conceitos do espaço cibernético, a seguir, serão introduzidos os fundamentos deste domínio. No artigo "*The Fundamental Conceptual Trinity of Cyberspace*" (2020), os autores propõem uma teoria edificada nos preceitos das Relações

Internacionais, em que o ciberespaço é firmado em três intrínsecas regras básicas, na qual pode ser usada como uma ferramenta analítica. Este tripé fundamental do ciberespaço, portanto, é caracterizado pela: (I) multiplicidade de atores; (II) desterritorialização; e pela (III) incerteza (Medeiros; Goldoni, 2020).

Em junho de 2022, estima-se que cerca de 5,38 bilhões de pessoas em todo o mundo utilizam a internet, rede global de computadores. Isto significa que 67,9% da população mundial utiliza o ciberespaço (*Internet World Stats*, 2022). Neste sentido, o primeiro fundamento apresentado, que é a multiplicidade de atores, é facilmente definido pela grande variedade de atores que utilizam o ciberespaço. Como já citado anteriormente, na introdução desta seção, a ubiquidade do espaço cibernético tornou-se imprescindível na comunicação e na gestão de dados e informações no século XXI, que tende a se tornar cada vez mais acessível a todos, justificando o barateamento de tecnologias da informação. Neste aspecto, segundo a *Internet World Stats* (2022), em julho de 2002, apenas 9,1% da população mundial tinha acesso à internet. Isto significa que, em 20 anos, mais da metade da população global passa a utilizar o ciberespaço (um índice que está em constante crescimento).

Em consequência deste grande número de atores que interagem entre si a todo momento, na troca de dados e informações em uma rede global, são produzidas também vulnerabilidades às ICs. Esta fragilidade se dá simplesmente pelo fato de que civis e militares de diferentes Estados de todo mundo e suas respectivas ICs, atuarem no mesmo domínio, permitindo, por exemplo, desde ataques cibernéticos, espionagem e manipulação de informações. Ainda neste tema, outro importante ponto a ser levantado é que estes atores, estatais ou não, possuem suas próprias agendas dentro do domínio cibernético (Medeiros; Goldoni, 2020), algo que será explorado ao serem abordados os objetivos do Stuxnet.

Seguindo esta linha de raciocínio, percebe-se outro fundamento: a desterritorialização. Neste sentido, o fluxo de informações e dados através de uma rede mundial de computadores, transpassam as clássicas fronteiras geográficas estatais de forma instantânea, em alta velocidade pelo espectro eletromagnético, devido a condição de imaterialidade deste domínio (Medeiros; Goldoni, 2020). Para ilustrar este comportamento, a fim de facilitar o entendimento, um determinado ator que se encontra em um país A, com infraestrutura e capacidade técnica suficientes, pode desferir um ataque através da camada virtual (ataque cibernético), podendo provocar danos físicos em uma IC de um país B. A partir deste exemplo teórico, percebe-se a caracterização desterritorializante, na qual o aspecto do território físico tem sentido apenas de onde o ataque partiu e a qual lugar ele foi direcionado. O espaço cibernético, neste caso, é utilizado como uma ferramenta de ataque que permite cruzar fronteiras sem o contato físico direto entre os atores. Vale ressaltar que esta interação entre os atores apenas é possível através de uma infraestrutura física e pela capacidade técnica humana nesta operação.

Por fim, e não menos importante, outra característica do ciberespaço é a incerteza. Esta particularidade abrange diversos elementos. Em primeiro lugar, o anonimato, definido pela dificuldade de atribuir de onde o fluxo informacional desagregado se origina, alimentado pela multiplicidade de atores. Outro elemento é a incapacidade de medir um evento ou um acontecimento e suas consequências, devido à natureza mutável, interconectada e complexa das camadas da sintaxe e semântica do espaço cibernético. Em terceiro lugar, a ausência da permanência de um objeto neste meio virtual, devido justamente pela imaterialidade e pelo ambiente rapidamente mutável do ciberespaço, como citado anteriormente. E por último, a velocidade das ações que ocorrem nesse meio podem se sobrepor à capacidade do tempo da tomada de decisão estratégica dos atores afetados (Medeiros; Goldoni, 2020).

Com o entendimento das camadas virtuais, físicas e humanas que compõem o domínio cibernético, e a introdução dos três fundamentos apresentados de forma breve, tem como objetivo posterior serem aplicados ao caso do Stuxnet, como apresentado na próxima seção. Neste sentido, esta introdução conceitual não apenas facilita a compreensão de como funciona este domínio de modo geral, mas também analisa, de forma crítica, como os confrontos do século XXI têm se aprofundado no ambiente informacional, a partir de um dos principais casos de ataque cibernético mais sofisticados que o mundo já concebeu até o momento. Segundo Rid (2014), todos os ataques políticos cibernéticos pregressos e contemporâneos são meras manifestações sofisticadas de três práticas intrínsecas à guerra milenar: subversão, espionagem e sabotagem. Diante disso, compreende-se que o caso Stuxnet não passa de uma antiga atividade de sabotagem (objetivo), porém com métodos modernos (meio).

Descrição e análise: afinal, o que se entende por Stuxnet?

Os autores Falliere, o'Murchu e Chien (2011), com base no dossiê da *Symantec*, uma das principais e mais completas fontes na época, concluíram que até setembro de 2010, o Irã foi o país mais infectado pelo Stuxnet, sinalizando que fora o alvo principal, visto ter representado 60% das infecções globais. Neste sentido, é indicado também que outros Estados foram atingidos, pois, devido aos mecanismos de propagação deste *worm*, o ataque foi além de seu objetivo. O Stuxnet foi confeccionado para atingir o sistema industrial SCADA[9] e manuseado para refrear as centrífugas de enriquecimento de urânio iranianas. O desígnio do ataque visava subverter as centrífugas em um processo lento e gradual, enganando, desse modo, os operadores da usina. Presumivelmente, a sua linha de raciocínio residia na premissa de que, ao comprometer o funcionamento do hardware, uma considerável interrupção temporal seria imposta ao programa de enriquecimento nuclear do Irã (Rid, 2014).

9. Os sistemas de Supervisão de Controle e Aquisição de Dados (Scada), tem a finalidade de monitorar, analisar e controlar dispositivos e processos industriais. O sistema, portanto, permite o gerenciamento remoto das indústrias por parte das empresas (Scada Internacional, S/D).

Este *worm* de computador foi descoberto, em junho de 2010, após ter lesionado instalações nucleares[10], com destaque a Natanz, uma das principais usinas de enriquecimento de urânio do Irã, inutilizando e deixando inoperantes várias centrífugas, com dados oscilando de mil a 5 mil[11], e em Bushehr[12], o reator nuclear. O Stuxnet interrompeu o enriquecimento nuclear iraniano, sendo o primeiro caso conhecido de um ataque à rede de computadores a promover danos físicos a infraestruturas estratégicas além das fronteiras lógicas nacionais. Neste sentido, este acontecimento acarretou sérias implicações para a segurança em todo o mundo, com destaque a ICs, sistemas industriais, arcabouços críticos e sensíveis. Dessa maneira, o Stuxnet foi concebido objetivando acarretar um mau e prejudicial funcionamento em procedimentos industriais, deteriorando, assim, motores, turbinas, centrífugas e demais equipamentos e aparatos (Rid, 2014; Collins; Mccombie, 2012; Pinto; Grassi, 2020)

A princípio, acredita-se que a infecção do Stuxnet das centrífugas tenha sido através de um *driver* removível (conhecido popularmente como *USB*), pois tratava-se de um alvo isolado, ou seja, não era possível infectar de maneira remota através da rede mundial de computadores, pois, devido ao alto risco à exposição de invasores, as ICs precisam estar à parte da internet para seu funcionamento. Cabe apontar que um ataque cibernético não precisa ser feito de forma exclusivamente remota através da internet - a utilização de um *driver* removível é apenas uma opção pertinente de se invadir um alvo, que, neste caso, indica a necessidade da presença de um indivíduo que tenha acesso a esta rede privada (Rid, 2014). Neste sentido, foi necessária uma estratégia de infecção sofisticada por parte dos invasores, na qual a totalidade das capacidades requeridas para sabotar o sistema foi integrada diretamente no executável do Stuxnet, o que implica na incorporação plena e autossuficiente de todas as funcionalidades sabotadoras no código executável desse *malware*.

Segundo Rid (2014), quando este *worm* se instalava nos sistemas, tinha como configuração checar seu alvo e mudar as frequências dos *drivers*[13] que operavam os motores da usina, resultando em um mau funcionamento, danificando as turbinas, motores e centrífugas. O Stuxnet operava com sutileza e astúcia, pois possuía artifícios para contornar as defesas de softwares de segurança. Além de esconder réplicas de seus arquivos em

10. O Stuxnet tinha como alvos específicos a turbina a vapor na usina nuclear de Bushehr (identificada pelo código 417), e as centrífugas de gás em Natanz (designadas pelo código 315), onde, caso este *worm* conseguisse se conectar a esses controladores, ele verificava suas configurações para confirmar o alvo. Caso o alvo fosse confirmado, o Stuxnet alterava as frequências de saída de drivers específicos responsáveis pelo acionamento de motores. Caso negativo, simplesmente não faria nada (Rid, 2014, p. 416).

11. Antes do acordo nuclear de 2015, o uso de centrífugas em Natanz era de 20 mil. Com o acordo, o uso ficou limitado a 5 mil por uma década, sendo utilizadas as com menor capacidade e mais antigas.

12. *Bushehr Nuclear Power Plant* (BNPP), primeiro reator nuclear iraniano.

13. *Driver* é um *software* (um programa), que permite que o computador se comunique com o *hardware* (aparelho físico) (Microsoft, S/D).

dispositivos removíveis, ocultava seus próprios blocos de programa ao serem submetidos a um processo de enumeração em controladores e, de maneira eficaz, se auto destruía em máquinas que não conduziam ao alvo preestabelecido (Rid, 2014; Zetter, 2014).

Neste sentido, segundo o autor, a sofisticação tecnológica, elevada complexidade e finalidade cirúrgica deste *worm*, traz uma forte evidência de que foi desenvolvido por um ou um conjunto de Estados. Em outras palavras, Rid (2014), supõe que: (I) o Stuxnet tenha sido desenvolvido por Israel em conjunto com os EUA, devido à grande capacidade de demanda técnica, recursos e tempo em sua elaboração, somando-se ao fato da grande instabilidade regional no Oriente Médio caso o Irã desenvolva armas nucleares - retomando a relevância da temática política trabalhada em relação a um conflito bélico; (II) Apesar de saber que este ataque cibernético trouxe prejuízos ao enriquecimento de urânio, os dados e pesquisas, a respeito do intermédio temporal, em termos de anos, são muito oscilantes. Nestes dois pontos retoma-se o fundamento da incerteza, respectivamente sobre o anonimato (dificuldade e demora em atribuir concretamente quem desenvolveu o Stuxnet) e a incapacidade de medir as reais consequências desse ataque ao Irã, mesmo sabendo que os planos nucleares iranianos foram retardados em algum nível, como frisado anteriormente.

Zetter (2014), ratificando o argumento de Rid, questiona quem seriam os autores da criação deste *worm*. Devido à complexidade do mesmo e o emprego de tecnologia de ponta, além do fato de ter atingido um alvo bem específico (as centrífugas iranianas), algumas hipóteses foram consideradas, todas retomando à compreensão política, como a de que o autor seja um (ou mais de um) ente estatal e que não tem interesse que o Irã desenvolva armas, tampouco tecnologia nuclear. Essa questão surge da natureza intrincada e complexa do Stuxnet, o que leva à atribuição de sua operacionalidade a agências governamentais, inclusive a possibilidade acerca de uma eventual colaboração interinstitucional (Zetter, 2014; Lindsay, 2013).

Como mencionado, vários estudiosos apontam e argumentam que tal ação foi orquestrada e coordenada pelos Estados Unidos, em razão do fato de que o país não tem interesse que o Irã desenvolva tal tecnologia e que, com o Stuxnet, houve uma retração das ambições iranianas por um período. Sobre esta temática e neste cenário, os Estados Unidos, devido a questões de Segurança e Defesa, tinham um forte intuito de neutralizar o programa nuclear iraniano. Este fator deve-se ao fato que, desde a Revolução Iraniana, em 1979, os dois países possuem relações conturbadas e estão em posições opostas no tabuleiro geopolítico, além de que, se o Irã detivesse tal tecnologia, suscitaria o dilema de segurança, promovendo uma corrida armamentista na região e alterando a balança de poder. Como o Oriente Médio é uma região onde os Estados Unidos são, tipicamente, presentes, este desdobramento só acentuaria a ingerência estadunidense na região, aumentando ainda mais os dilemas políticos. Ademais, outro ponto que corrobora é que Washington não estava conseguindo bons

resultados nem êxito, por meios diplomáticos, para conter o programa nuclear iraniano. Esta situação é compreendida e percebida à luz da explicação de Clausewitz sobre a guerra como sendo a imposição da vontade sobre o oponente, e também sobre como o aspecto político permeia toda a compreensão e se manifesta até nos elementos estritamente militares (Lopes; Oliveira, 2014; Freilich, 2022; Zetter, 2014).

Outrossim, os Estados Unidos entendiam que promover ataques militares convencionais para este intento não seria interessante para a sua imagem e política externa naquele contexto político e histórico, visto que o país já estava tendo que lidar com os desdobramentos da Guerra ao Terror e sua ação militar no Iraque. Neste cenário, aumentaram-se os rumores e hipóteses, apesar da ação do Stuxnet não ter sido reivindicada. O uso de armamentos e ferramentas cibernéticas, enquanto opção e possibilidade às investidas e ações militares tradicionais, se sobressai como uma predileção conveniente, em termos de imagem política, e financeiramente menos custosa de interferência no programa nuclear iraniano. Assim, "*o governo dos EUA lançou mão de um tipo de poder que atrela política externa a um novo ambiente de atuação das Forças Armadas: o poder cibernético*" (Lopes; Oliveira, 2014, p. 56).

Nesse sentido, outro ponto a ser ressaltado, dentro do espectro político, é que a maior parte das potências ocidentais, principalmente as que compõem o Tratado de Não Proliferação de Armas Nucleares (TNP) e que possuem esta tecnologia, como Estados Unidos, França e Reino Unido, além de potências regionais, como Israel, não tinham interesse e enxergavam com preocupação o fato do Irã estar desenvolvendo seu programa nuclear, visto que desde a Revolução, o país é alvo de desconfianças por parte do Ocidente, no que diz respeito a suas atividades com o manuseio de energia nuclear. O que corrobora, novamente, a hipótese de que o *worm* tenha sido criado por um Estado. Assim, no entorno regional, a possibilidade de o Irã desenvolver armas nucleares modificaria a balança de poder, retomando a discussão do dilema de segurança, como já delineado. Países como Israel, Emirados Árabes Unidos e Arábia Saudita temem esta realidade e mesmo com diferenças geopolíticas e posturas políticas diferentes, se aproximaram, em virtude de terem um obstáculo, um oponente em comum – o Irã com armas nucleares – e, assim, por objetivos estratégicos. Com destaque ao governo de Tel-Aviv, a estratégia de segurança nacional do país revela que o Irã é uma ameaça estatal à sua sobrevivência. Dessa maneira, enquadra-se o caso Stuxnet, visto que o Irã ter a posse de urânio enriquecido, podendo desenvolver armamentos nucleares e reatores químicos, confrontava os interesses dos Estados Unidos a nível regional - podendo alterar o equilíbrio de poder do Oriente Médio - e a nível internacional (Lopes; Oliveira, 2014; Freilich, 2022; Zetter, 2014).

Contudo, como apontado, até hoje não houve reivindicação da autoria de tal feito; só emprego de hipóteses, sendo os principais voltados ao fato de que o *worm* foi desenvolvido pelos Estados Unidos e, em alguns exemplos, com cooperação israelense, sendo ao mesmo

tempo um ato estatal e de interagências, em decorrência da conjuntura política, como analisado anteriormente. Entretanto, apesar deste cenário, vale ressaltar que o foco do trabalho é compreender se esta ação praticada por meio do Stuxnet pode ser considerada um ato de guerra, com base no referencial teórico da obra Da Guerra (Lopes; Oliveira, 2014; Rid, 2014).

A argumentação do governo de Teerã que os objetivos para deter energia nuclear tem como fins questões de cunho energético e medicinais, em muitos casos, pauta ainda mais a incredulidade dos Estados, que não acreditam nesta narrativa[14]. Assim, em decorrência destas presunções, investidas são feitas por parte dos Estados Unidos e Israel, com o intuito de obter mais detalhes e informações sobre o programa nuclear, para saber como agir e atuar contra a República dos Aiatolás, e se antecipar contra alguma investida ou tentativa de agressão. Dentro deste panorama, a exequibilidade e contingência do uso do poder cibernético enquanto um ente tecnológico de intervenção, se transformou em uma medida notável. Neste sentido, a guerra cibernética, concepção abordada pela literatura especializada em defesa cibernética, encontra-se inseparavelmente ligada ao poder cibernético (Lopes; Oliveira, 2014).

A respeito do ataque a uma IC, Hausken (2011) menciona que estas são analisadas, estando sujeitas à defesa e ao ataque por múltiplos atacantes estratégicos. Sobre estratégia, a percepção apresentada por Schelling (1980, p. 5) elucida que: *"a estratégia não se preocupa com a aplicação eficiente de forças, mas com a exploração da força potencial."* Afirmação esta que se coloca como relevante e pode ser aplicada na análise do caso do Stuxnet, como, por exemplo, para abordar sobre o distúrbio causado nas ICs. Ademais, partindo deste fato, aplicam-se os três fundamentos anteriormente explicitados: a capacidade de propagação do Stuxnet no espaço cibernético para outros países, pelo princípio da desterritorialização; a multiplicidade de atores; e a incerteza no que tange sobre a velocidade de propagação do *worm* para além do seu alvo, e, novamente, a complexidade em quantificar as consequências deste ataque não apenas ao Irã, mas também a todos os outros países, a nível regional e global (Harknett; Smeets, 2022).

Além disso, acrescenta que: *"uma estrutura é desenvolvida onde cada agente determina quanto investir na defesa versus ataque a cada um dos vários alvos. Um alvo pode ter valores econômicos, humanos e simbólicos, que geralmente variam entre os agentes*" (Hausken, 2011, p. 11) (tradução nossa)[15]. Além disso, este panorama revela o uso de meios cibernéticos para acometer infraestruturas que, anteriormente, acreditava-se que só seriam atingidas por meio de ataques aéreos, bombardeios e explosões. Em suma, concluindo este assunto, Farwell e Rohozinski (2011) argumentam que o domínio cibernético oferece um vasto

14. Neste âmbito, outro aspecto que vale mencionar é que no final de 2021 e início de 2022, quase saiu um novo acordo nuclear, mas, acabou não tendo um prosseguimento.

15. "A framework is developed where each agent determines how much to invest in defending versus attacking each of multiple targets. A target can have economic, human and symbolic values, which generally vary across agents" (Hausken, 2011, p. 11).

potencial em atacar adversários com menor exposição a riscos, comparado a métodos militares convencionais. Neste sentido, os autores argumentam que os Estados se apropriam e exploram tecnologias cuja evolução é instigada por atividades criminosas no ciberespaço, possivelmente, externalizando investidas cibernéticas a entidades não plenamente rastreáveis, entre elas, organizações de índole criminosa.

De acordo com esta perspectiva, Zetter (2014) elucida que o Stuxnet é um exemplo do uso de uma classe de artefatos cibernéticos, e politicamente contestados, que teve uma participação em conflitos geopolíticos, além de ter sido o ataque mais sofisticado já realizado. Stevens (2020) discorre sobre a natureza política situada na segurança cibernética, concluindo que o trabalho da *Symantec* não era neutro ou sem dimensões políticas, e sim que os especialistas fizeram escolhas profundamente geopolíticas em suas análises, reforçando e ressaltando o potencial de ataques cibernéticos. Conforme destacado por Rid (2014), a inteligência é também a etapa inicial e fundamental de um ataque cibernético, devido ao fato de que os invasores precisam de informações detalhadas sobre o sistema de controle de configuração único. Dessa maneira, torna-se evidente que o conhecimento aprofundado obtido por meio da inteligência proporcionou aos engenheiros e programadores responsáveis pelo Stuxnet uma compreensão minuciosa da infraestrutura singular do sistema-alvo iraniano. Tais informações desempenharam um papel crucial no processo de desenvolvimento do malware, viabilizando sua capacidade de explorar essas vulnerabilidades de forma eficiente, maximizando os danos de forma furtiva.

Por fim, com base no que discorreu-se aqui, o Stuxnet é um dos ciberataques de maior notoriedade internacional, o qual comprometeu e retardou o programa nuclear iraniano à época. Assim, pode-se considerar que o Stuxnet é a primeira arma cibernética criada voltada à capacidade de destruição para uma infraestrutura essencial, como as instalações nucleares, que trabalham na produção de energia, além do primeiro grande ataque militar cibernético da História, em termos de proporções. Este fato trouxe modificações na noção de ciberespaço no escopo da guerra, revelando uma exposição e fragilidade em que todos os atores estatais se encontram, além de perpassar as compreensões de soberania, fronteira, ataques, violação, além dos próprios conceitos de guerra, apresentando a cibersegurança como uma preocupação de política internacional, Segurança e Defesa.

CONSIDERAÇÕES FINAIS

Sendo assim, esta investigação científica se propôs a examinar se o episódio histórico do Stuxnet poderia vir a ser cunhado como um ato de guerra, visto a interpretação Clausewitziana de que a guerra é a continuação da política com a entremistura de outros meios, sendo uma ação para compelir o inimigo a exercer o seu intuito, sendo, assim, uma disputa de vontades e um ato de violência. Em outras palavras, há como propósito enfraquecer o adversário para torná-lo inapto de executar resistência e, desse modo, implementar

sua vontade. Para analisar e realizar esta pesquisa, observou-se a compreensão da teoria de guerra e o pensamento clausewitziano, bem como o domínio cibernético, até o espectro político, crucial na análise de Clausewitz, sobre o contexto em que o Stuxnet se encaixa, por meio de um estudo de caso único sobre este episódio.

Assim, na circunstância alcançada, a presente investigação corrobora a hipótese apresentada no início deste texto, de que o Stuxnet pode ser caracterizado como um ato de guerra, de acordo com a percepção clausewitziana, ao levar em consideração que fora um ato político com o intuito de impor seu propósito ao oponente. Portanto, a estratégia planejada para interromper o processo de enriquecimento de urânio no Irã foi alcançada, correlacionando com o descrito anteriormente, de imposição da vontade em uma situação bélica. Sendo assim, a ação por trás do Stuxnet foi crucial para alcançar essa finalidade. Em outras palavras, ao que tange à política, o Stuxnet, enquanto instrumento cibernético, obteve um desempenho e resultado político, visto que retardou o enriquecimento de urânio e, consequentemente, a tecnologia nuclear, por parte do Irã. Desse modo, conclui-se que este *worm* funcionou como sendo a continuação da política por outros meios, estes tecnológicos, para impor a sua vontade ao país persa. Além disso, por mais que até hoje o regime de Teerã não tenha desistido do seu projeto e arcabouço, este episódio histórico auxiliou no seu adiamento. Assim, a questão política se fez presente e irrompeu em todo este cenário, confirmando mais uma vez a hipótese apresentada, visto que foi a continuação da política e que esta irrompe até mesmo nos elementos puramente de segurança e defesa, além de evidenciar a conexão existente entre cibernética e fins geopolíticos.

Para além deste viés, um dos principais resultados desta pesquisa encontra-se na correlação com o espectro de Tecnologia e Cibernética ao campo das Ciências Militares e Política Internacional, em decorrência do impacto de Infraestruturas Críticas (ICs). Desta forma, ressalta-se o alcance desta ferramenta cibernética e o seu poder de efeito e ataque, potencial destrutivo, bem como evidencia a vulnerabilidade e sensibilidade encontrada nestes tipos de estruturas, sendo mecanismos pelos quais, ao serem aprofundados, há impacto e correlação direta com a política. O que reforça o quanto a estratégia não é apenas, unicamente, a respeito do uso eficaz do poder aplicado, mas o uso do poder potencial, ou seja, de mostrar que há capacidade para agir com maior aptidão em determinada área.

Por fim, os resultados que este trabalho expõe representam e derivam de uma abordagem contemporânea, sem ignorar as colaborações e subsídios do passado, ao analisar esta relação entre guerra e tecnologia cibernética. Esperou-se, por meio desta investigação, ressaltar um olhar mais apurado sobre o episódio histórico que foi o Stuxnet, visto que, em um mundo cada vez mais globalizado, ações cibernéticas se tornam cada vez mais atuais, e como a correlação entre tecnologia, cibernética, ciências militares e política internacional tem muito a contribuir, em conjunto, para elucidar melhor as debilidades das infraestruturas críticas e como estas impactam os Estados como um todo.

BIBLIOGRAFIA

ARON, Raymond. *Pensar a Guerra: Clausewitz – a Era Planetária.* Tradução de Elisabeth Maria Speller Trajano. Brasília, DF: Editora Universidade de Brasília, 1986.

BELCIC, Ivan. *O que é um worm de computador?* AVAST. 20 de Jul. de 2020. Disponível em: https://www.avast.com/pt-br/c-computer-worm#. Acesso em: 13 de mai. 2024.

BUZAN, Barry; HANSEN, Lene. *The Evolution of International Security Studies*. Cambridge University Press, 2012.

CANONGIA, Claudia; Raphael, MANDARINO. Segurança cibernética*:* o desafio da nova Sociedade da Informação. *Parcerias Estratégicas*, v.14, n.29, jul-dez, 2009.

CLAUSEWITZ, Carl von; HOWARD, Michael.; PARET, Paret (Eds.). *On War.* Princeton: Princeton University Press, 1984.

CLAUSEWITZ, Carl von. *On War*. Comentários de Beatrice Heuser. Oxford University Press, 2007.

COLLINS, Sean; McCOMBIE, Stephen. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, v.7, n.1, mar, 2012.

ECHEVARRIA, Antulio Joseph. *Clausewitz and contemporary war*. New York: Oxford University Press, 2007.

FALLIERE, Nicolas; O' MURCHU, Liam; CHIEN Eric. W32. Stuxnet Dossier. *Symantec Security Response*, fev, 2011.

FARWELL, James P.; ROHOZINSKI, Rafal. Stuxnet and the Future of Cyber War. *Survival Global Politics and Strategy*, v.53, n.1, jan, 2011.

FREILICH, Chuck. Israel and the Iran Nuclear Deal: The Best of Bad Options. *Survival Global Politics and Strategy*, v. 64, n.3, maio, 2022.

GEORGE, Alexander L.; BENNETT, Andrew. *Case Studies and Theory Development in the Social Sciences.* Cambridge, Harvard University, 2005.

GERRING, John. *Case study research: principles and practices.* New York: Cambridge University Press, 2007.

GIBSON, William F. *Neuromancer.* Edição especial de 30 anos. Tradução: Fábio Fernandes. São Paulo: Aleph, 2014.

GRAY, Colin S. *Strategy and History*: essays on theory and practice. Oxon: Routledge, 2009.

HANDEL, M. Who's Afraid of Carl von Clausewitz? *In*: MAHNKEN, T.; MAIOLO, J. *Strategic Studies*: a reader. New York: Routledge, 2014.

HARKNETT, Richard J.; SMEETS, Max. Cyber campaigns and strategic outcomes. Journal of Strategic Studies, v.45, n.4, 2022.

HAUSKEN, Kjell. Protecting complex infrastructures against multiple strategic attackers. *International Journal of Systems Science*, v.42, n.1, 2011.

HERBERG-ROTHE, Andreas. *Clausewitz's puzzle: the political theory of war.* Oxford University Press, 2007.

HEW STRACHAN. *Sobre a Guerra de Clausewitz/* Hew Strachan; tradução, Maria Luiza X. de A. Borges. - Rio de Janeiro: Jorge Zahar Ed., 2008.

HOWARD, M. *Clausewitz:* a very short introduction. Oxford: Oxford University Press, 2002.

KALDOR, Mary. *New and old wars- organized violence in a global era*. Stanford: Stanford University Press, 1999.

KEEGAN, John. *Uma história da guerra*. São Paulo: Companhia das Letras, 2006.

KUEHL, Daniel. "From Cyberspace to Cyberpower: Defining the Problem". In KRAMER, Franklin D.; STARR, Stuart S.; WENTZ, Larry K. (Eds.) *Cyberpower and National Security.* University of Nebraska Press, 2009, p. 24-42.

LA MAISONNEUVE, Eric de. *Metamorfosis de la violencia: ensayos sobre la guerra moderna*. Buenos Aires: Grupo Editor Latinoamericano, 1998.

LIBICKI, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica: RAND, 2009.

LINDSAY, Jon R. Stuxnet and the Limits of Cyber Warfare. *Security Studies*, v.22, n.3, ago. 2013.

LOPES, Gills; OLIVEIRA, Carolina Fernanda J. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. *Revista Brasileira de Estudos de Defesa*, ano 1, nº 1, jul./dez. 2014, p. 55-69.

MAHNKEN, T.; MAIOLO, J. *Strategic Studies*: a reader. New York: Routledge, 2014.

McGRAW, Gary. Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies,* v.36, n.1, fev. 2013.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The Fundamental Conceptual Trinity of Cyberspace. *Contexto Internacional*. v.42, n.1, 2020.

PARET, Peter. *Construtores da estratégia moderna*: *de Maquiavel à era nuclear/* Editado por Peter Paret com colaboração de Gordon A. Graig e Felix Gilbert, traduzido por Joubert de Oliveira Brízida. - Rio de Janeiro: Biblioteca do Exército Editora, 2001.

PARET, Peter; HOWARD, Michael; BRODIE, Bernard. *Ensaios introdutórios*. *In*: CLAUSEWITZ, Carl von. *Da Guerra*. London: Oxford University Press, 1984.

PINTO, Danielle Jacon Ayres; GRASSI, Jéssica Maria. Guerra Cibernética, Ameaças Às Infraestruturas Críticas e a Defesa Cibernética Do Brasil. *Revista Brasileira de Estudos de Defesa*, v.7, n.2, p. 103–31, 2020.

PROENÇA JÚNIOR, Domício et al. *Guia de Estudos de Estratégia.* Rio de Janeiro: Zahar, 1999.

RID, Thomas. Cyber war will not take a place. *In:* MAHNKEN, Thomas G.; MAIOLO,Joseph A. (Eds.) *Strategic Studies*: a reader. New York: Routledge, 2014, pp.408-429.

S/N. Detectar um dispositivo desconhecido e encontrar seus drivers. S/D. Microsoft. Disponível em: https://support.microsoft.com/pt-br/topic/detectar-um-dispositivo-desconhecid o-e-encontrar-seus-drivers-ede88764-40b0-8219-14e0-ca59fc44b320. Acesso em: 3 jun. 2023.

S/N. Internet Usage Statistics: The Internet Big Picture World Internet Users and 2022 Population Stats. Internet World Stats. 2022. Disponível em: https://www.internetworldstats.com/stats.htm. Acesso em: 2 jun. 2023.

S/N. Internet Growth Statistics: Today's road to e-Commerce and Global Trade. Internet Technology Reports. Internet World Stats. 2022. Disponível em: https://www.internetworldstats.com/emarketing.htm. Acesso em: 2 jun. 2023.

S/N. O que são ataques de DDoS?. Kaspersky. S/D. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ddos-attacks. Acesso em: 6 jun. 2023.

S/N. What is SCADA? SCADA INTERNATIONAL. S/D. Disponível em: https://scada-international.com/what-is-scada/. Acesso em: 3 jun. 2023.

SAINT-PIERRE, Hector. Defesa ou Segurança? Reflexões em torno de conceitos e ideologias. *Contexto Internacional,* v.33, n.2, 2011.

SCHELLING, Thomas C. *The Strategy of Conflict.* Harvard University Press, 1980.

SOUCHON, L. *Strategy in the 21st Century*: the continuing relevance of Carl von Clausewitz. Springer, 2020.

STEVENS, Clare. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Comparative Security Policy*, v.41, n.1, 2020.

STONE, John. Clausewitz's Trinity and Contemporary Conflict*. Civil Wars*, v.9, n.3, 2007.

STONE, John. Cyber War Will Take Place! *Journal of Strategic Studies*, v.36, n.1, 2013.

STONE, John. Rebooting Clausewitz: On War in the Twenty-First Century. *The RUSI Journal*, v.163, n.2, 2018.

TILLY, Charles. *The Formation of National States in Western Europe*. Princeton: Princeton University Press, 1975.

VAN CREVELD, Martin; OLSEN, John Andreas. *The Evolution of Operational Art – From Napoleon to the Present*. Oxford: Oxford University Press, 2011.

VENTRE, Daniel. Ciberguerra. In: *Academia General Militar*. Seguridad Global y Potencias Emergentes en un Mundo Multipolar. XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza, 2012.

ZETTER, Kim. *Countdown to Zero Day*: *Stuxnet and the launch of the world's first digital weapon*. Crown Publishers. Nova York, 2014.