ESCOLA DE GUERRA NAVAL

CC GUILHERME ALMEIDA MATOS DE CARVALHO

A TEORIA DE WARDEN APLICADA NA GUERRA CIBERNÉTICA:

a aderência do ataque do Stuxnet à Estratégia da Paralisia e à Teoria dos Cinco Anéis

Rio de Janeiro
2020

CC GUILHERME ALMEIDA MATOS DE CARVALHO

A TEORIA DE WARDEN APLICADA NA GUERRA CIBERNÉTICA:

a aderência do ataque do Stuxnet à Estratégia da Paralisia e

à Teoria dos Cinco Anéis

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CC Daniel Barbosa da Silva Barabani

Rio de Janeiro

Escola de Guerra Naval

2020

AGRADECIMENTOS

À minha esposa Liana, pelo amor, pela compreensão, pelo incentivo e pelo apoio incondicional.

Aos meus filhos Arthur e Luísa, por terem sido o meu momento de alegria e inspiração nos intervalos da elaboração deste trabalho.

Ao meu orientador, o CC Barabani, pelo suporte, pelas suas correções de rumo e pelo incentivo durante a elaboração da minha pesquisa.

E enfim, a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

O Espaço Cibernético alcançou um papel de protagonismo no mundo atual, graças ao avanço tecnológico observado nas últimas décadas. Este trabalho analisa a Operação "Jogos Olímpicos" e o planejamento para a utilização da arma cibernética que ficou conhecida como Stuxnet e culminou em um ataque realizado pelos Estados Unidos da América e por Israel ao programa nuclear do Irã. A destruição de centrífugas de enriquecimento de urânio tornou-se um marco na Guerra Cibernética por ter sido o primeiro ataque realizado a partir do ambiente cibernético que causou efeitos cinéticos em uma estrutura vital de um Estado. Ao confrontar a teoria do Coronel John Warden com o planejamento e as formas empregadas para a disseminação do *malware*, conclui-se que houve uma aderência parcial à Teoria dos Cinco Anéis. Por fim, o trabalho ressalta a importância do assunto para a Marinha do Brasil ao expor que ataques cibernéticos evoluíram, podendo causar efeitos físicos em todos os domínios operacionais da guerra, inclusive nos meios de nossa Força Naval.

Palavras-chave: Warden, Teoria dos Cinco Anéis, Estratégia da Paralisia, Stuxnet, Guerra Cibernética.

LISTA DE ABREVIATURAS E SIGLAS

AIEA - Agência Internacional de Energia Atômica
CG - Centro de Gravidade
EUA - Estados Unidos da América
MB - Marinha do Brasil
MD - Ministério da Defesa
PD - Ponto Decisivo
PLC - *Programmable Logic Controllers*
SCADA - *Supervisory Control and Data Acquisition*
TNP - Tratado de Não Proliferação Nuclear

SUMÁRIO

1 INTRODUÇÃO 7

2 A ESTRATÉGIA DA PARALISIA E OS CINCO ANÉIS DE WARDEN 10

2.1 O Coronel John Warden e as formas de aplicação da força 11

2.1.1 A coerção por meio de ataques paralelos 11

2.1.2 A Estratégia da Paralisia 12

2.1.3 A destruição do inimigo 13

2.2 As bases estratégicas para o estudo do inimigo como um sistema 14

2.2.1 O pensamento estratégico de Warden 15

2.2.2 A componente física como forma de atingir o Estado Final Desejado 15

2.2.3 A análise do sistema inimigo 17

2.3 A Teoria dos Cinco Anéis 18

2.4 A Teoria dos Cinco Anéis no Espaço Cibernético 22

3 O STUXNET E O ATAQUE AO PROGRAMA NUCLEAR IRANIANO 25

3.1 O programa nuclear do Irã e o panorama internacional 25

3.2 A Operação “Jogos Olímpicos” 27

3.3 O *malware* Stuxnet 28

3.3.1 O método de propagação do Stuxnet 29

3.3.2 A carga útil do Stuxnet 30

3.4 O Stuxnet e o futuro da Guerra Cibernética 32

3.5 Avaliação das consequências do Stuxnet 33

4 A ADERÊNCIA DO STUXNET À TEORIA DE WARDEN 36

4.1 A aderência do ataque do Stuxnet às três formas de aplicação da força 36

4.1.1 O ataque do Stuxnet e os ataques paralelos 37

4.1.2 O ataque do Stuxnet e a Estratégia da Paralisia 37

4.2 O ataque do Stuxnet e as bases estratégicas para o estudo do inimigo como um sistema 38

4.3 A aderência do ataque à Teoria dos Cinco Anéis. 40

4.3.1 O anel das forças militares iranianas 40

4.3.2 O anel da população 41

4.3.3 As Infraestruturas Críticas 42

4.3.4 Os elementos orgânicos essenciais 43

4.3.5 O anel da liderança central 43

5 CONCLUSÃO 45

REFERÊNCIAS 48

1 INTRODUÇÃO

Com o vertiginoso avanço da tecnologia nas últimas décadas, o mundo observou atentamente aos modernos recursos computacionais passando a satisfazer a anseios pessoais, trazendo benefícios indiscutíveis a diversos setores sociais e integrando sistemas vitais de um Estado ou de um conjunto de Estados. O acelerado desenvolvimento tecnológico alavancou a relevância do Espaço Cibernético.

O protagonismo do ambiente virtual afetou o fenômeno sociológico do conflito entre os Estados e resultou em episódios de ataques a infraestruturas e informações críticas dos contenedores. Essa novidade permitiu a obtenção de vantagens estratégicas, operacionais e táticas aos utilizadores desses artifícios tecnológicos. Sendo assim, o Espaço Cibernético começou a ser considerado um novo domínio operacional da guerra, agregando-se aos ambientes terrestre, marítimo, aéreo e espacial.

Essa nova dimensão da guerra permeou os demais ambientes, propiciando a liberdade para que o Espaço Cibernético pudesse criar efeitos além do seu domínio operacional. Diante disso, a Guerra Cibernética passou a se constituir em uma forma de agredir o oponente de maneira rápida e sem exposição, possibilitando a dissimulação da autoria de um eventual ataque. Com esse aperfeiçoamento, abriu-se um leque de possibilidades que permitiu que a arma cibernética pudesse ter como alvos desde redes elétricas e sistemas de controle de tráfego até radares e sistemas empregados a bordo de navios de guerra.

No entanto, a trajetória cibernética permanece em fase de consolidação, gerando dúvidas e discussões sobre o seu emprego e possibilidades. Por isso, a emergência do Poder Cibernético[1] guarda relativa semelhança com o caminho percorrido pelo Poder Aéreo a partir da Grande Guerra (1914-1918), a qual foi uma grande bancada de testes para a utilização da arma aérea.

---

1 O Poder Cibernético é a capacidade de utilizar o Espaço Cibernético para criar vantagens em outros domínios operacionais e em instrumentos de poder (BRASIL, 2014).

No presente trabalho, que se debruça sobre a Guerra Cibernética, é razoável utilizar como base de pesquisa uma teoria originada para aplicação do Poder Aéreo. Para tanto, dentre os diversos teóricos do Poder Aéreo que debateram o assunto e desenvolveram teorias sobre seu emprego, destaca-se o Coronel da Força Aérea dos Estados Unidos da América (EUA) John Ashley Warden III (1947-). Os estudos de Warden acerca Estratégia da Paralisia e o modelo teórico que analisa o inimigo como um sistema subdividido em cinco anéis estratégicos facilitaram a identificação de vulnerabilidades e Centros de Gravidade do inimigo. Suas ideias pregavam que a força poderia ser empregada de forma a gerar danos físicos ao inimigo, abalando seu componente moral e sua vontade de resistir. Por conseguinte, poderia ser alcançada uma vitória rápida e com economia significativa de recursos.

Com base no trabalho do Coronel Warden, será analisado o ataque cibernético à usina de enriquecimento de urânio em Natanz, ocorrido entre os anos de 2009 e 2010, no Irã. O incidente foi mais um capítulo do intrincado cenário geopolítico da região e da oposição estadunidense e israelense ao desenvolvimento da tecnologia nuclear por Teerã. Cabe ressaltar que a escolha da operação, que ficou conhecida com "Jogos Olímpicos", deveu-se ao seu pioneirismo e complexidade, visto que o ataque quebrou paradigmas no ambiente cibernético por ser o primeiro a causar efeitos cinéticos a partir do quarto domínio da guerra.

Com efeito, o propósito deste trabalho é responder ao seguinte questionamento: a Operação "Jogos Olímpicos" e o ataque realizado por meio da arma cibernética Stuxnet[2] tiveram aderência à Estratégia da Paralisia de John Warden e ao seu modelo teórico dos Cinco Anéis?

Para atingir o propósito, o trabalho se desenvolverá em cinco capítulos. Após esta introdução, serão apresentados, no segundo capítulo, os principais conceitos da teoria de Warden, com foco nas suas bases de pensamento estratégico e nos cinco anéis que representam a Liderança, os Elementos Essenciais, as Infraestruturas Críticas, a População e

2 No decorrer deste trabalho a arma cibernética Stuxnet será tratada como sendo um *software* malicioso, um *malware*, um *worm* ou um código malicioso. O conceito de cada uma dessas designações será abordado oportunamente.

as Forças Militares de um sistema. No terceiro capítulo, após apresentar de forma sucinta a situação geopolítica que envolvia Irã, EUA e Israel em 2010, serão descritas todas as singularidades do ataque realizado com pelo Stuxnet. No quarto capítulo, serão confrontadas as características do ataque cibernético com o modelo estudado, identificando como a Operação "Jogos Olímpicos" se adequa às bases estratégicas de Warden e como o Stuxnet afetou cada um dos cinco círculos concêntricos apresentados pela teoria. Por fim, no quinto capítulo, serão apresentadas as principais conclusões e a relevância do estudo para a Marinha do Brasil.

2 A ESTRATÉGIA DA PARALISIA E OS CINCO ANÉIS DE WARDEN

Neste capítulo, serão abordadas a Estratégia da Paralisia e a Teoria dos Cinco Anéis elaborada pelo Coronel John Warden, ex-piloto de combate da Força Aérea dos EUA. Suas ideias foram expressas em alguns livros, destacando-se a obra "*The Air Campaign*", de 1988, na qual Warden descreve o modelo de Estratégia da Paralisia empregado pela Força Aérea estadunidense durante a Primeira Guerra do Golfo (1990-1991).

A execução da Estratégia da Paralisia com a identificação e destruição da liderança adversária, a visão do inimigo como um sistema e os estudos sobre a necessidade de submeter o oponente a ataques paralelos são alguns dos conceitos formulados por Warden que serão estudados sob a ótica de determinação de Pontos Decisivos[3] (PD) e Centros de Gravidade[4] (CG). Dessa forma, os objetivos principais serão avaliados de modo a causar uma paralisia física ao oponente, garantindo àquele que a coloca em prática uma vantagem relativa que induzirá o inimigo a cumprir sua vontade.

Em que pese o fato de a obra de Warden ter sido naturalmente fundamentada no Poder Aéreo, neste trabalho não serão observadas as peculiaridades da teoria que tratam da sua compatibilização à posse da superioridade aérea, essencial para aplicação da Estratégia da Paralisia. Portanto, os estudos relacionados à utilização da arma aérea serão abordados unicamente como forma de introduzir o pensamento estratégico do autor, permitindo que os conceitos interessantes a uma aplicação sobre a Guerra Cibernética sejam estudados de maneira mais profunda.

---

3 Os Pontos Decisivos são locais, eventos específicos, sistemas críticos ou funções que permitem uma vantagem relevante sobre o inimigo, influenciando decisivamente no resultado de um ataque. Esses pontos podem estar relacionados à obtenção de efeitos sobre pessoas, meios militares ou sobre o caráter psicológico do oponente (BRASIL, 2011).

4 Os Centros de Gravidade, de acordo com Clausewitz (1979), são os pontos centrais de poder e movimento, dos quais tudo depende, sendo esse o ponto onde devem ser concentradas as energias para obtenção de resultados decisivos.

2.1 O Coronel John Warden e as formas de aplicação da força

No início de sua formação acadêmica na Força Aérea dos EUA, na década de 1960, o Coronel Warden já adotava uma postura inquisitiva e iniciava a construção da sua teoria do Poder Aéreo, questionando-se sobre a eventual preponderância dessa dimensão da guerra sobre os Poderes Terrestre e Marítimo (OLSEN, 2007).

Com o prosseguimento de sua carreira, Warden participou da Guerra do Vietnã (1960-1975), quando operou em mais de 2 missões como piloto de combate ou como controlador aéreo (ANRIG *et al*., 2004). Piloto habilidoso e criativo, rapidamente angariou o reconhecimento de seus superiores, tendo utilizado sua experiência na guerra para desenvolver seus conceitos estratégicos (OLSEN, 2007).

Tal experiência permitiu que o Coronel Warden emergisse como um dos principais defensores da aplicação da força na terceira dimensão do campo de batalha, tendo a oportunidade de materializar suas ideias durante a Primeira Guerra do Golfo, quando apresentou o plano inicialmente denominado "*Instant Thunder*". O plano foi concebido de forma a paralisar as forças militares iraquianas, sem devastar o Iraque e embutia o entendimento de que o Poder Aéreo poderia ser empregado de forma mais efetiva em um nível operacional (ANRIG *et al*., 2004).

Embora o nome "*Instant Thunder*" tenha sido alterado e o plano tenha sofrido alguns refinamentos para ser colocado em prática durante a Guerra do Golfo (ANRIG *et al*., 2004), a operação ainda refletia os pensamentos estratégicos de Warden, que identificava três formas possíveis para aplicação da força contra o oponente: a coerção por meio de ataques paralelos, a paralisia estratégica e a destruição do inimigo.

2.1.1 A coerção por meio de ataques paralelos

A estratégia da coerção procura fazer com que a resistência seja inviável para a

liderança inimiga. Nesse caso, tem-se a intenção de provocar danos parciais a estruturas importantes ou ameaçar a paralisia total do sistema inimigo, por meio de ataques simultâneos ou paralelos aos alvos designados. Dessa forma, o adversário é coagido a abdicar de seus objetivos (FADOK, 1995).

O surgimento de armas guiadas com precisão permitiu que ataques pudessem ser feitos de forma pontual. Assim, a ofensiva causaria danos aos centros vitais, reduzindo efeitos colaterais e abolindo a necessidade de ataques que causassem grande destruição e desperdício de meios. Por essa razão, o Coronel Warden acreditava na possibilidade de realizar, simultaneamente, ataques em alvos dos níveis tático, operacional e estratégico (COUTAU-BÉGARIE, 2010).

De tal maneira, ataques simultâneos contra parcela significativa desses objetivos conseguiriam causar danos irrecuperáveis ao inimigo (SIQUEIRA, 2007). Esse conceito, além de fundamental para os Ataques Paralelos, também é de suma importância para a Estratégia da Paralisia.

2.1.2 A Estratégia da Paralisia

A segunda e a mais conhecida forma de aplicação da força, descrita no livro *The Air Campaign,* é a Estratégia da Paralisia. Essa estratégia de emprego da força possui raízes históricas que remetem a pensadores clássicos, como o General prussiano Carl Phillip Gottlieb von Clausewitz (1780-1831), ao passo que também busca alvos prioritários do inimigo (COUTAU-BÉGARIE, 2010).

A Estratégia da Paralisia formulada por Warden recorreu a conceitos já consagrados de guerra, como a ideia de guerra relâmpago[5] da doutrina alemã. Essa estratégia

5 A guerra relâmpago, também conhecida como *Blitzkrieg,* foi um símbolo da atuação da Alemanha na Segunda Guerra Mundial (1939-1945). É conceituada como o emprego concentrado de armas e Forças para confundir o inimigo, objetivando derrotar o inimigo rapidamente em uma operação decisiva (FRIESER, 2013)

tinha alicerces nos princípios da surpresa e da velocidade, buscando efetuar ataques decisivos à frente adversária, possibilitando a destruição de seu apoio logístico e sistema de comando (COUTAU-BÉGARIE, 2010).

Observando esse exemplo histórico, percebe-se uma evolução da Estratégia da Paralisia que, para os efeitos deste trabalho, pode ser assim definida:

> A Estratégia da Paralisia é uma opção militar com dimensões físicas e morais que tem a intenção de incapacitar, em vez de destruir o inimigo. Ela busca o máximo efeito ou benefício político, com o mínimo esforço militar ou custo. Tem por objetivo uma decisão militar rápida, dirigida contra a capacidade física ou mental que tem o adversário de manter ou controlar o seu esforço de guerra, para diminuir sua vontade moral de resistir (FADOK, 1995, p. 17, tradução nossa)[6].

Dessa forma, a Estratégia da Paralisia, a fim de executar ataques rápidos e pontuais, exige a identificação correta dos PD para afetar a capacidade de resistência do adversário (FADOK, 1995). Esse processo de identificação de pontos nevrálgicos será detalhado no estudo do inimigo como um sistema, quando esse será subdividido em cinco anéis.

Por ora, cabe ressaltar que o Coronel John Warden e o também Coronel da Força Aérea estadunidense John Boyd[7] (1927-1997) foram responsáveis por uma rápida evolução da Estratégia da Paralisia, caracterizando-a com uma intenção não-letal e com a promessa de economia de forças empregadas em uma campanha, o que a diferencia das práticas de aniquilação e destruição do inimigo.

2.1.3 A destruição do inimigo

O enfoque da Estratégia da Paralisia formulado por Warden se diferenciou das

---

6 No original em inglês: *"The strategic paralysis is a military option with physical, mental, and moral dimensions which intends to disable rather than destroy the enemy. It seeks maximum possible political effect or benefit with minimum necessary military effort or cost. It aims at rapid decision directed against an adversary's physical and mental capability to sustain and control its war effort in order to diminish its moral will to resist*".

7 O Coronel John Boyd propôs um modelo de decisão estratégica, chamado ciclo de decisão OODA: Observação-Orientação-Decisão-Ação, que enfatiza as dimensões morais e mentais do conflito. (COUTAU-BÉGARIE, 2010).

estratégias mais tradicionais de emprego da destruição do inimigo. Essa prática de aniquilação se demonstrou rara, de difícil execução e com envolvimento de aspectos morais, não sendo muito útil para o alcance dos objetivos, pelo elevado potencial de trazer consequências indesejadas (FADOK, 1995).

Desse modo, o Coronel John Warden refutava o pensamento dos primeiros teóricos do emprego da arma aérea, como Giulio Douhet (1869-1930)[8], que acreditavam que a derrota do inimigo ocorreria com a destruição universal e o massacre cego de civis. Logo, ele descartava essa estratégia de emprego da força, considerando-a inviável para a guerra no século XXI.

Uma vez identificadas as estratégias previstas por Warden para emprego da força, verifica-se a importância dos ataques paralelos e, principalmente, do emprego da Estratégia da Paralisia. Esses fundamentos priorizavam a intenção de abalar o moral do oponente, com um propósito não-letal, procurando anular sua vontade de resistir. A partir de agora, serão descritas a análise do inimigo como um sistema e a visão sobre a identificação dos CG do adversário à luz da teoria do Coronel estadunidense.

2.2 As bases estratégicas para o estudo do inimigo como um sistema

Antes de estudar o inimigo como um sistema, é importante identificar as bases estratégicas que norteiam o pensamento de Warden.

Em *The Air Campaign*, o estadunidense destaca que as suas teorias não eram táticas, endereçando seus estudos àqueles que se encontram em um nível operacional e desejam atingir os objetivos militares estratégicos necessários a vencer uma guerra.

Portanto, salienta-se que tanto a Estratégia da Paralisia quanto a comparação do

8 O General Giulio Douhet formulou a estratégia aérea, concebendo-a para suplantar todas as demais dimensões. Em seus trabalhos, Douhet pensava que guerras poderiam ser vencidas infligindo pesadas baixas à população civil, rompendo o moral e levando à capitulação do oponente (COUTAU-BÉGARIE, 2010).

inimigo a um sistema foram ideias formuladas para atender a uma estratégia operacional[9] e para viabilizar a identificação dos pontos decisivos de um planejamento nesse nível de condução de um conflito (WARDEN, 1988).

Após definir o público-alvo de sua teoria, Warden procura estabelecer um método para atingir tais objetivos estratégicos, buscando a identificação de padrões para o planejamento e execução de missões em um nível operacional (WARDEN, 1988), que serão evidenciados a seguir.

2.2.1 O pensamento estratégico de Warden

Em primeiro lugar, Warden enfatiza em seu artigo "*The Enemy as a System*", publicado em 1995, que um planejamento estratégico requer um pensamento *top-down* ou dedutivo. É dizer: deve-se raciocinar a partir de uma abordagem sobre o cenário mais amplo, descendo aos níveis mais específicos. Esse pensamento permite que se observem os princípios gerais de uma situação, de onde serão extraídos os detalhes que serão aplicados ao desenho de uma campanha. Logo, deve-se focar no inimigo de uma forma geral, depois nos objetivos principais e, por fim, sobre o que deve acontecer aos inimigos antes que esses objetivos se tornem a prioridade dele (WARDEN, 1995).

2.2.2 A componente física como forma de atingir o Estado Final Desejado

Após ter identificado a linha de raciocínio a ser seguida durante o planejamento, Warden apontou que o advento do poder aéreo e de armas precisas tornou possível a destruição da componente física, reduzindo os danos colaterais e evitando o aniquilamento do inimigo. A evolução do armamento, das comunicações e da forma de movimentação da tropa

9 A estratégia operacional é a arte de empregar as forças militares para alcançar objetivos estratégicos, conciliando-os com as possibilidades táticas e técnicas dessas forças, buscando superioridade em momento e local adequado para executar uma campanha (BRASIL, 2015).

no campo de batalha trouxe mudanças na lógica sobre como produzir o Estado Final Desejado[10] (EFD) no inimigo (WARDEN, 1995). Sob as novas circunstâncias, os componentes físico e moral passam a ter um papel diferenciado quando comparados àqueles observados por estrategistas clássicos, como Clausewitz (WARDEN, 1995).

Se no passado o atrito, o *fog* da guerra[11] e o moral eram aspectos intangíveis fundamentais para a condição do soldado e para seu desempenho em combate, com o advento de novas tecnologias a situação se transforma. O indivíduo se torna parte de artefatos maiores, como tanques, aeronaves e peças de artilharia, e o soldado apela a apetrechos físicos para condução de suas tarefas no campo de batalha (WARDEN,1995).

Como consequência, de acordo com Warden, pode-se representar a guerra de uma forma ampla, conforme a seguinte equação:

Eficácia no combate = Força Física x Força Moral

Diante disso, percebe-se que se o lado físico da equação é conduzido a zero, a variável moral, mesmo que permaneça intacta, não será capaz de manter a eficácia no combate. Por conseguinte, ele observa que destruir alvos físicos é mais fácil do que destruir a vontade moral do inimigo de resistir (FADOK, 1995). Tal afirmação é melhor compreendida ao se perceber que o componente físico é conceitualmente conhecido e calculável, ao passo que o lado moral está além do domínio da previsibilidade, uma vez que os homens são diferentes uns dos outros, podendo reagir de formas distintas e desproporcionais (WARDEN, 1995).

Dessa forma, o Coronel Warden estabelece que os esforços de guerra devem ser direcionados primariamente para o lado físico do oponente, tornando-o incapacitado de se opor às ações de seu contendente (FADOK, 1995).

---

10 O Estado Final Desejado é a condição geral que indica que uma missão foi cumprida, tendo alcançado seus objetivos políticos e estratégicos estabelecidos (BRASIL, 2011).

11 O *fog* da guerra também é conhecido como fricção geral ou atmosfera da guerra. De acordo com Clausewitz (1979), é tudo aquilo que torna difícil algo que parece fácil, devido ao perigo, esforço físico e informações contraditórias e incompletas.

Os pontos físicos para os quais os planejadores devem direcionar os esforços, já identificados anteriormente como CG, são assim descritos pela Doutrina de Operações Conjuntas do Ministério da Defesa (MD): “Um Centro de Gravidade pode incluir o conjunto das forças oponentes ou a sua estrutura de comando, a opinião pública, a vontade nacional ou a estrutura de uma coligação” (BRASIL, 2011, v. 1, p.80).

Como o público-alvo de Warden é o planejador em um nível operacional, é importante salientar que, de acordo com a Doutrina de Operações Conjuntas do MD, os CG em níveis operacionais são as forças militares, o que será parcialmente contestado pelo Coronel estadunidense em sua teoria, a qual prioriza os ataques às lideranças do inimigo. Por outro lado, em consonância com a análise do autor estudado, o documento também prevê que, quanto mais elevado o nível do planejamento, os CG se apresentam em menor número, com aspectos mais intangíveis (BRASIL, 2011).

2.2.3 A análise do sistema inimigo

Considerando que um sistema é um conjunto de elementos concretos ou abstratos, intelectualmente organizados, admite-se que em cada conjunto há uma organização central (HOUAISS, 2015). Warden enumera diversos tipos de sistemas e seus entes de organização central, como um átomo que controla as órbitas dos elétrons. O funcionamento de cada subsistema depende de seus líderes, que decidem sua forma de agir (WARDEN, 1995).

Assim, sistemas como um Estado, uma organização de negócios ou uma organização terrorista possuem tanto elementos físicos quanto biológicos, que em seus centros dispõem de um indivíduo que estabelece direção, sentido e até mesmo objetivos estratégicos (CHAPPEL JR., 2002). Esses elementos exercem o papel de líderes e, em uma guerra, passam a ser os alvos principais de todas as ações.

A seguir será detalhado o modelo criado por Warden para melhor compreensão de

sua Estratégia da Paralisia, denominado por ele como “Teoria dos Cinco Anéis”.

2.3 A Teoria dos Cinco Anéis

Warden era extremamente metodológico em sua abordagem. De forma a tornar sua teoria mais prática, ele afirmou que todas as entidades estratégicas podem ser divididas em cinco partes componentes. Essa subdivisão do sistema inimigo, em conjunto com um estudo minucioso sobre toda a sua capacidade de mobilização, facilitará a identificação dos CG, forçando ao planejador o estabelecimento de conexões entre esses pontos focais (WARDEN, 1995).

Após realizar a análise criteriosa do inimigo e estabelecer os CG, a Teoria dos Cinco Anéis define uma hierarquia entre eles, priorizando os objetivos que, se atacados, tornariam a guerra proibitiva para o inimigo e eliminariam a sua capacidade de reagir de forma temporária ou até mesmo definitiva.

Com uma linguagem simples e didática, Warden usa uma analogia biológica ao traçar um paralelo de sua teoria com o corpo humano. O cérebro, ao receber informações dos olhos e do sistema nervoso central, representa a liderança do corpo. A comida e o oxigênio são dois Elementos Orgânicos Essenciais, enquanto os vasos sanguíneos, ossos e músculos fornecem a infraestrutura. As células constituem a população do corpo, enquanto os linfócitos e leucócitos fornecem proteção contra ataques. Se qualquer uma das partes do corpo mencionadas parar de funcionar, isso terá um efeito mais ou menos importante no resto do corpo (FADOK, 1995).

Em resumo, nota-se que Warden enumera os cinco anéis concêntricos da seguinte forma: Direção ou Liderança Central, Elementos Orgânicos Essenciais, Infraestrutura, População e Forças Militares em campo.

Antes de descrever cada um dos cinco anéis, é importante ressaltar que todo

sistema terá um conjunto único de CG que, de acordo com o modelo teórico, deve ser atacado de dentro para fora, tendo como alvo principal a liderança adversária. Além disso, conforme já ressaltado anteriormente, a melhor forma de coagir o oponente é a realização de ataques simultâneos, ou paralelos.

Como anel mais crítico, destaca-se o anel de direção ou de liderança central, por ser a estrutura de comando ou o cérebro do sistema. Esse ente estratégico é o único capaz de tomar decisões complexas, necessárias para manter a direção do sistema em um curso específico. Ao tratar de um sistema específico que é o Estado, pode-se avaliar que as guerras ao longo da história foram travadas de modo a alterar a estrutura de comando do inimigo, obrigando-a a fazer concessões ou tornando-a incapaz de exercer seu papel de liderança. Caso não seja possível ameaçar diretamente o elemento de comando, deve-se aplicar pressão de forma indireta, impondo grau considerável de dano aos anéis sobrejacentes. Racionalmente, o órgão diretor decidirá por reconsiderar suas ações ou então pode ser submetido a uma paralisia estratégica, por meio da destruição de um ou mais CG posicionados nos anéis estratégicos externos (WARDEN, 1995).

O segundo anel mais crítico contém os Elementos Orgânicos Essenciais, ou seja, instalações ou processos sem os quais um sistema não pode se manter. Esse anel, que em um nível operacional pode ser considerado como logístico, não necessariamente está relacionado ao poder de combate do sistema. No entanto, os danos causados a um CG nele localizado podem levar ao colapso do sistema, tornando fisicamente árdua a tarefa de manter uma determinada política ou conduta (SIQUEIRA, 2007). Adicionalmente, ao exemplificar novamente o seu modelo utilizando um Estado, Warden pondera que ao deteriorar objetivos nesse anel, há repercussões políticas e econômicas importantes e difíceis de serem contornadas.

Em seguida, observa-se o terceiro ente estratégico que contém componentes

notáveis de infraestrutura, cuja importância advém da dinâmica normal do funcionamento do sistema e de organizações. Em um Estado, a infraestrutura é representada por linhas ferroviárias, companhias aéreas, rodovias, pontes, estradas, aeroportos, portos e outros dispositivos que impactam na circulação de bens, serviços e informações. Apesar do aspecto fundamental da infraestrutura, esse anel é marcado pela redundância de seus componentes (PINTO, 2003). Logo, a abundância de estruturas e instalações forma um organismo complexo, com alternativas caso um de seus elos falhe, levando a um maior esforço para causar danos suficientes para gerar consequências ao sistema como um todo.

O quarto anel operacional se constitui da população, que é um elemento importante para o funcionamento do sistema, pois sem ele, dificilmente os demais anéis funcionarão. Além das objeções morais, a existência de inúmeros alvos e a capacidade de resistência, fazem de qualquer operação direta contra a população uma tarefa extremamente difícil. Dessa forma, caso o inimigo demonstre ter um interesse relativamente baixo na guerra, podem ser eficazes os ataques indiretos à população, por meio de danos aos outros anéis, ou até mesmo na alimentação de dissidências no sistema político adversário (PINTO, 2003). De forma contrária ao que pensava Giulio Douhet, historicamente, os ataques diretos às populações não fizeram com que a população civil tivesse seu moral abalado.

O quinto e último anel do modelo abordado contém as forças militares de um Estado. Para Warden, apesar de as forças militares serem vistas como as mais importantes na guerra, elas possuem a função única de proteger os anéis internos ou ameaçar aqueles do inimigo (PINTO, 2003). Portanto, as forças militares são os CG mais difíceis de serem atacados, justamente por terem sido projetadas para serem resistentes. Apesar de uma campanha que tenha objetivos neste anel tender a ser mais longa e intensa para ambos os lados, por vezes ela poderá ser necessária para que objetivos operacionais ou estratégicos localizados em anéis mais internos sejam alcançados. Warden reconhece que tal visão não é

tradicional, uma vez que a maioria dos pensamentos clássicos sobre a guerra foram produzidos de forma a idealizar o enfrentamento entre as forças militares. Tal dissociação do pensamento tradicional é justificada pela tecnologia moderna, que possibilita que armas de precisão e até mesmo o poder aéreo façam das forças militares um meio e não um fim em si (WARDEN, 1995).

Uma vez designados os anéis operacionais, cabe mencionar que dentro de cada um deles pode existir um CG, ou uma série de CG que representam o núcleo de toda a força e movimento desse anel específico. Quando destruídos, levam à falência do anel, afetando todo o sistema de maneira mais ou menos significativa, dependendo da hierarquia do anel no modelo, ou seja, se é um anel interior ou exterior.

A fim de identificar com precisão esses CG, Warden sugere que cada anel seja subdividido em cinco subanéis, e esses em mais cinco, até que o verdadeiro CG seja encontrado (FADOK, 1995).

Por conseguinte, será apresentado na FIG.1 o modelo gráfico da "Teoria dos Cinco Anéis" de Warden, que sintetiza o posicionamento de todos os anéis descritos anteriormente:

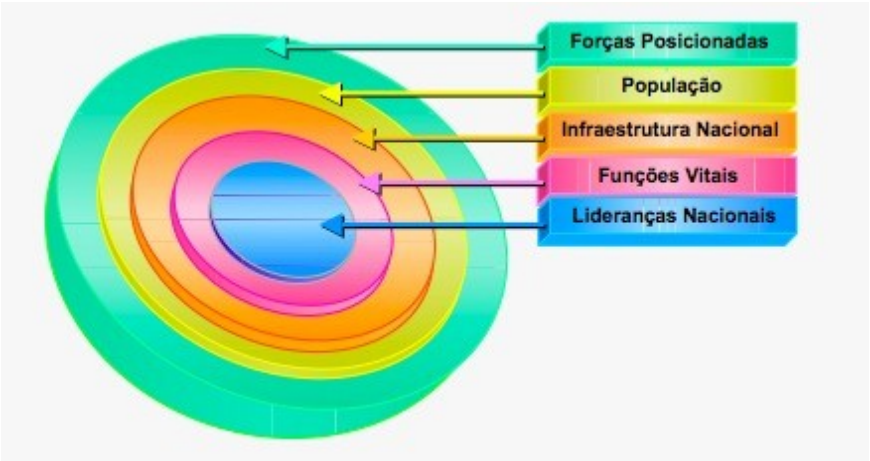

FIGURA 1 – Modelo gráfico da "Teoria dos Cinco Anéis".
Fonte: BRASIL, 2012. p. 27.

Embora o modelo analítico apresentado tenha sido desenhado para planejamentos

em níveis operacionais, ele é perfeitamente aplicável em outros níveis e segmentos, desde que seja mantida a ideia de que o objetivo principal estará presente no anel interior, que representa a liderança de um sistema (FADOK, 1995). Tal afirmação pode ser comprovada quando se verifica que os cinco anéis são atualmente utilizados por John Warden como cerne de uma ferramenta empresarial denominada *Prometheus*, pela qual o processo de abordagens de sistemas do mundo real permite encontrar centros críticos dentro de uma organização empresarial e em seus mercados (WARDEN, 2001).

A seguir, serão identificados possíveis empregos da Teoria dos Cinco Anéis em relação ao tema de estudo, que é a Guerra Cibernética.

2.4 A Teoria dos Cinco Anéis no Espaço Cibernético

É interessante observar que o Espaço Cibernético, por definição da *Joint Publication* 3-12 de 2018, pode ser dividido em três camadas inter-relacionadas: a rede física, a *cyber-persona* e a rede lógica. Intuitivamente, essas camadas poderiam ser relacionadas aos anéis de Warden, possibilitando que uma eventual operação cibernética venha a ser conduzida contra um CG a ser determinado. De acordo com a doutrina estadunidense, serão identificadas cada uma das camadas, realizando um paralelo à teoria já apresentada.

A camada da rede física é composta pelo *hardware* e pela infraestrutura computacional, como computadores, dispositivos de armazenagem e de rede. Esses componentes necessitam de medidas de segurança para evitar danos físicos ou acesso não-autorizados. É importante ressaltar que, devido ao alcance global das ações executadas no Espaço Cibernético, o domínio físico é o único que ainda goza de relativa soberania (ESTADOS UNIDOS DA AMÉRICA, 2018).

Em face do seu caráter físico, essa camada do Espaço Cibernético possui semelhanças com o terceiro anel de Warden, ao representar uma infraestrutura que possibilita

a circulação de informações e que conta com uma redundância significativa de seus componentes.

A *cyber-persona* é a camada do Espaço Cibernético que extrai dados da camada da rede lógica, de forma a criar uma planilha de identidades de todos os atores e entidades, que podem ser relacionadas a indivíduos, grupos, máquinas ou sistemas autônomos (ESTADOS UNIDOS DA AMÉRICA, 2018). Essa camada pode ser atrelada ao anel da População, uma vez que ataques realizados nesta camada afetariam diretamente os usuários do Espaço Cibernético.

A camada de rede lógica tem como base a programação de códigos que auxiliam na lógica de endereçamento, intercâmbio e processamento de dados. Ela é essencial para seleção de alvos, pois possibilita a localização lógica de qualquer objetivo no Espaço Cibernético (ESTADOS UNIDOS DA AMÉRICA, 2018). Por conter os softwares e a operação lógica do ambiente, essa camada pode ser tratada como um pilar, sendo associada ao anel interno da liderança. Assim, é na rede lógica que devem ser concentrados os esforços e a designação dos CG mais importantes.

Como se nota, ao analisar as camadas previstas na doutrina estadunidense de Operações no Ciberespaço, a princípio, não é possível identificar os anéis das forças militares e dos Elementos Orgânicos Essenciais. A incapacidade de constatação desses anéis não inviabiliza a utilização da teoria, pois a mesma pode ser perfeitamente aplicada com a identificação do CG mais valioso, sendo possível incapacitar o oponente em caso de danos ao ente que comanda e controla as operações de todo o sistema.

Embora a comparação anteriormente descrita possa ser bastante útil na análise do caso concreto desta pesquisa, ela não é a única maneira para classificar os possíveis CG de uma estrutura cibernética inimiga. O ordenamento de redes, computadores e dispositivos de acordo com o seu emprego é um outro método para aplicação do processo dos cinco anéis.

Analogamente, componentes da estrutura cibernética de organizações militares poderiam ser associados ao anel de Forças Militares, as redes sociais relacionadas ao anel da População, o sistema computacional de organizações econômicas atrelados aos anéis de Infraestrutura e Elementos Orgânicos Essenciais e, por fim, a estrutura cibernética governamental identificada como o anel central de Liderança do inimigo (OGÎGAU-NEAMTIU; MOGA, 2018).

3 O STUXNET E O ATAQUE AO PROGRAMA NUCLEAR IRANIANO

Neste capítulo, serão abordados os impactos do ataque cibernético que, em 2009, teve como alvos principais as centrífugas nucleares que operavam na cidade iraniana de Natanz. O episódio foi o primeiro a utilizar uma arma cibernética cinética[12] que permitiu a produção de efeitos cinéticos, ou seja, que afetou alguém ou algum ente no mundo real.

É importante salientar que, apesar de EUA e Israel[13] não terem assumido a responsabilidade pelo ataque, a complexidade da arma cibernética utilizada requeria uma tecnologia muito específica e um financiamento que só poderia ter sido suportado por entidades governamentais. Conforme apontam algumas evidências geopolíticas, para efeito de uma melhor condução deste trabalho, será considerado que esses Estados foram os responsáveis por planejar e executar o ataque que visava ao arrefecimento do programa nuclear iraniano.

Dessa forma, em uma breve apreciação do cenário geopolítico que envolvia o Irã e seus algozes, os EUA e Israel. Em seguida, serão detalhados a Operação "Jogos Olímpicos" e o *malware*[14] Stuxnet, abordando suas capacidades, os métodos utilizados para alcançar seus objetivos e as consequências do ataque para o programa nuclear iraniano.

3.1 O programa nuclear do Irã e o panorama internacional

Desde a década de 1950, os líderes iranianos buscam alcançar o domínio da tecnologia nuclear. A iniciativa contou com estímulo de nações ocidentais, principalmente dos EUA, motivados pela busca de influência no Oriente Médio, em meio ao cenário da Guerra Fria (1947-1989). O apoio ocidental durou até o final da década de 1970, quando o

12 Uma arma cibernética cinética é um software ou hardware projetado ou aplicado para causar danos físicos direta ou indiretamente por meio do domínio cibernético (BRASIL, 2019).

13 As evidências da participação israelense no ataque são bastante limitadas, restringindo-se ao uso de palavras importantes da religião hebraica no conteúdo do código malicioso (ZETTER, 2017).

14 Um *malware* é um *software* projetado para infiltrar um sistema computacional com a intenção de roubar dados, danificar aplicativos ou o sistema operacional (BRASIL, 2019).

fundamentalismo trazido pela Revolução Iraniana (1979) fez com que a cooperação fosse substituída pela preocupação a respeito das intenções iranianas em dar continuidade a seu programa nuclear (KERR, 2009).

A partir daí, houve uma forte oposição estadunidense às intenções nucleares iranianas. Sendo assim, o Irã conduziu suas atividades de forma discreta, até que, em 2002, um grupo de oposição iraniano[15] revelou ao mundo que Teerã estava construindo dois centros nucleares secretos, em desacordo com a Agência Internacional de Energia Atômica (AIEA): um em Natanz, onde era feito o enriquecimento do urânio, e o outro em Arak, onde era realizada a extração de plutônio (LIMA; FREITAS, 2016).

Embora tenha argumentado que suas atividades nucleares tinham um fim pacífico, o Irã, como signatário do Tratado de Não Proliferação de Armas Nucleares (TNP), deveria prestar informações sobre o seu programa, o que não ocorreu (LOPES; OLIVEIRA, 2014). Nesse sentido, as revelações de 2002 causaram tensões e tornaram-se elementos essenciais ao discurso de que o Irã desenvolvia seu programa nuclear para fins militares.

Ao analisar a posição estratégica do Irã no Oriente Médio, verifica-se que em seu entorno três Estados são detentores de armas de destruição em massa: Índia, Paquistão e Israel. O desenvolvimento de armas nucleares por Teerã poderia provocar um reajuste de forças na região, pondo fim à hegemonia israelense frente aos seus vizinhos árabes. Esse equilíbrio poderia ser benéfico para a região, a exemplo do que ocorreu entre Índia e Paquistão, que reduziram o ímpeto de hostilidades entre si, quando esses Estados alcançaram o *status* nuclear formal, em 1999 (GERMER *et al*., 2010).

Contudo, em 2005, com a ascensão de Mahmoud Ahmadinejad (1956-) ao poder, o Irã passa a adotar uma atitude mais agressiva no cenário internacional, assumindo uma postura antiestadunidense e propondo a extinção do Estado de Israel (ZETTER, 2017).

15 O Grupo de resistência iraniano conhecido como Conselho Nacional de Resistência do Irã (NCRI na sigla inglesa – National Council of Resistance of Iran) (ZETTER, 2017)

Nesse contexto, sob o ponto de vista dos EUA, caso o Irã se consolidasse como uma potência nuclear, o equilíbrio geopolítico do Oriente Médio estaria ameaçado.

Levando-se em conta os elevados custos políticos e materiais de uma investida militar em território iraniano, EUA e Israel aventaram a possibilidade de utilização do Poder Cibernético para realizar uma intervenção que impedisse a construção de bombas por parte do Irã (LOPES; OLIVEIRA, 2014). Identificada a oportunidade de realizar um ataque cibernético, o desafio a partir de então era desenvolver uma arma cibernética que pudesse executar ataques por *software* e que fosse capaz de trazer danos a objetos físicos de outros Estados.

3.2 A Operação "Jogos Olímpicos"

Em um mundo altamente conectado, a tendência de integração de todos os sistemas e equipamentos passou a ser uma preocupação constante aos usuários de redes de computadores. No entanto, esse risco também pôde ser encarado como uma oportunidade, justamente como ocorreu no caso da Operação "*Olympic Games*" ou "Jogos Olímpicos".

A operação consistia no planejamento de um ataque cibernético e teve início em 2006, ainda no governo do então presidente dos EUA, George Walker Bush (1946-). A iniciativa apresentou-se como uma alternativa mais segura aos planos israelenses de utilizar sua Força Aérea para bombardear o Irã, utilizando bombas para penetrar concreto reforçado, de modo a reduzir o ritmo do programa nuclear iraniano (CLARKE, 2015). Sendo assim, Bush autorizou o desenvolvimento da arma cibernética, deixando claro que só a empregaria se houvesse comprovação de que a sua utilização atrasaria o programa nuclear iraniano, sem causar danos colaterais (ZETTER, 2017).

Em 2009, já no governo de Barack Hussein Obama II (1961-), como resultado da Operação "Jogos Olímpicos", ocorreu o lançamento do ataque cibernético que ficou

conhecido como Stuxnet. O ataque cibernético, por meio do *software* malicioso[16] infectou, inicialmente, cinco organizações iranianas[17], utilizando-as como forma de afetar indiretamente seu objetivo final (CLARKE, 2015), que posteriormente foi identificado como sendo a usina nuclear em Natanz.

Por conseguinte, a Operação "Jogos Olímpicos" foi o pontapé inicial da campanha, que tinha como CG usinas de enriquecimento de urânio iranianas. Portanto, o interesse em destruir fisicamente as centrífugas localizadas em Natanz gerou a mais poderosa arma cibernética já vista até então, que será estudada mais detalhadamente a seguir.

3.3 O *malware* Stuxnet

Tendo em vista o caráter sigiloso da Operação "Jogos Olímpicos", apesar de as evidências apontarem para o início do ataque ainda em 2009, o Stuxnet permaneceu oculto até junho de 2010, quando, acidentalmente, foi descoberto por especialistas em segurança cibernética na Bielorrússia. Na ocasião, os técnicos analisavam um computador pessoal infectado de um cliente iraniano (ZETTER, 2017). Vale destacar que todas as informações aqui descritas correspondem a um misto de descobertas feitas por profissionais independentes ou por escritórios especializados em estudar as ameaças constantemente encontradas no Espaço Cibernético.

Com efeito, o Stuxnet será apresentado da forma como ele foi descoberto, ou seja, por seções. Para facilitar a compreensão dessas seções, pode-se comparar a sua forma de atuação como arma cibernética à composição de uma arma convencional: será utilizada uma analogia a um míssil de combate, identificando como partes componentes desse armamento o seu sistema de guiagem e a sua cabeça de combate (ZETTER, 2017). Assim, a sua forma de

16 Um *software* malicioso ou *malware* é um código que tem por objetivo que computadores ou redes realizem tarefas que seus donos ou usuários normalmente não fariam. *Worms*, bombas-lógicas, vírus, capturadores de pacotes e gravadores de tela são tipos de *softwares* maliciosos (CLARKE, 2015).

17 As cinco organizações afetadas eram, na verdade, empresas ligadas à automação industrial, à indústria metalúrgica e ao desenvolvimento das centrífugas nucleares. Ou seja, todas elas estavam ligadas diretamente ao programa nuclear iraniano (ZETTER, 2017).

propagação representa o sistema que guia o "míssil" ao seu alvo. Da mesma forma, as sequências lógicas que cumpriram o objetivo do Stuxnet serão analisadas como sendo a cabeça de combate do *software* malicioso.

3.3.1 O método de propagação do Stuxnet

Guardando semelhança com o sistema de guiagem de um míssil, o Stuxnet analisou o padrão de seu alvo final para calcular a sua trajetória. Além disso, identificou que o seu objetivo provavelmente não teria equipamentos conectados à internet, sendo impossível sua infecção de forma tradicional, por intermédio de e-mails ou *sites* maliciosos (SHAKARIAN, 2011). De acordo com Zetter (2017), a maneira encontrada para espalhar o *worm*[18] era a sua transmissão por *pen drives*, contando com pessoas que carregariam o Stuxnet até o seu ponto final. Embora, à época, a transmissão de softwares maliciosos por *pen drives* fosse pouco comum, os desenvolvedores acreditaram que esse seria um método eficaz para possibilitar a transmissão do Stuxnet.

De forma a não ser interceptado ou descoberto em sua tarefa de infecção, a arma cibernética utilizava *rootkits,* que são *softwares* que permitiam sua invisibilidade aos programas destinados a detectar anomalias, como os antivírus. Já para propagar a infecção de máquina a máquina, o *malware* utilizava *exploit*s[19] Dias-Zero[20] que atacavam funções do sistema operacional *Windows*, o que poderia colocar milhões de computadores em risco (SHAKARIAN, 2011).

Ao considerar que os *exploits* Dia-Zero eram um recurso raro, que explorava erros ainda desconhecidos em sistemas operacionais, os especialistas entendiam que somente um

18 Um *worm* é um programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores (BRASIL, 2019).

19 Um *exploit* é um código de ataque utilizado para instalar vírus e outras ferramentas maliciosas em máquinas, aproveitando-se da vulnerabilidade de aplicativos para injetar um vírus em um sistema (ZETTER, 2017).

20 Um Dia-Zero é a designação atribuída a uma ameaça capaz de explorar uma vulnerabilidade de segurança descoberta em sistemas computacionais, com correção ainda não disponibilizada pelo desenvolvedor ou fabricante (BRASIL, 2014).

Dia-Zero caracterizava um ataque comum, sendo o suficiente para propagar um código malicioso. Contudo, o Stuxnet carregava quatro *exploits* Dia-Zero (ZETTER, 2017), o que denotava que os seus desenvolvedores prezavam pela confiabilidade de que o código atingiria o seu alvo.

Além dos *exploits* Dia-Zero do sistema operacional *Windows*, os analistas descobriram outras quatro maneiras de disseminação do *malware*, totalizando oito métodos de disseminação. Essa característica, por si só, já fazia do Stuxnet um código notável e inovador (ZETTER, 2017). No entanto, o ineditismo do *worm* ainda pôde ser observado em outras características, as quais confirmam a semelhança de sua propagação ao método de guiagem de um "míssil cibernético".

A primeira delas de acordo com Falliere (2011), é o fato de o Stuxnet ter utilizado certificados digitais[21] válidos, provavelmente subtraídos das empresas RealTek Semicondutores e JMicron, fabricantes de hardware e circuitos localizados em Taiwan, a fim de enganar os sistemas invadidos, fazendo-os acreditar que o Stuxnet era um programa confiável. Atacantes tradicionais já se utilizavam dessa artimanha, no entanto, esses certificados eram ilegítimos, o que trazia riscos para uma identificação de certificado suspeito, que poderia fazer com que o acesso do código malicioso ao sistema fosse rejeitado (ZETTER, 2017). Mais uma vez, a consequência do Stuxnet para o futuro do ambiente cibernético era avassaladora, pois essa atitude colocava em risco todos os certificados digitais, antes considerados acima de quaisquer suspeitas.

3.3.2 A carga útil do Stuxnet

Graças aos seus métodos de propagação altamente eficientes, o Stuxnet infectou um grande número de computadores ao redor do mundo. Para os analistas que estudavam o

21 Um certificado digital é um documento de segurança confiável, que é destinado a comprovar para outros a identidade do terminal que utiliza o certificado. Ele é confiável quando assinado por uma autoridade de certificação, ou se ele próprio é um certificado confiável (BRASIL, 2019).

código, era curioso que o Irã fosse o local mais afetado pelo *software* malicioso, uma vez que, até então, Teerã nunca estivera entre os locais mais contaminados por ameaças cibernéticas (ZETTER, 2017). Ao aprofundar as análises sobre o *malware*, o aspecto inusitado da contaminação ao Irã começou a fazer sentido.

Primeiramente, de acordo com Shakarian (2011), os pesquisadores identificaram que os ataques eram direcionados a computadores que possuíam programas componentes de um Sistema de Controle Industrial conhecido como SCADA (*Supervisory Control and Data Acquisition*). Os alvos específicos seriam os SCADA da empresa alemã *Siemens,* projetados para trabalhar com controladores lógicos programáveis, ou *Programmable Logic Controllers* (PLC)[22]. Com isso, o Stuxnet adquiria um caráter diferenciado, visto que a grande maioria dos ataques cibernéticos, até aquele momento, eram voltados a sistemas bancários ou outros alvos que pudessem garantir um retorno financeiro ao atacante.

Os programas-alvo do Stuxnet, o *Siemens WinCC-7 e Step 7*, estavam disponíveis em Infraestruturas Críticas[23] controladas por sistemas digitais em todo o mundo. Dessa forma, a concentração de casos de infecção do *worm* no Irã ainda não se justificava. Logo, percebeu-se que o *malware* era, na verdade, uma arma de precisão de nível militar, haja vista que o seu código carregava configurações técnicas bastante específicas. Os objetivos do ataque eram sistemas de controle industrial que só poderiam ser encontrados no Irã: conversores de frequência fabricados nas empresas *Vacon*, da Finlândia, e *Fararo Paya,* do Irã (ZETTER, 2017).

Tais conversores eram empregados nas centrífugas de enriquecimento de urânio IR-1 iranianas (SHAKARIAN, 2011), e a revolucionária arma cibernética fora planejada para forçar uma mudança de velocidade no rotor da centrífuga, aumentando e reduzindo sua

22 Os PLCs eram pequenos computadores utilizados para controlar componentes mecânicos em fábricas automatizadas, como braços mecânicos e esteiras de linhas de montagem (ZETTER, 2017).

23 As Infraestruturas Críticas são as instalações, serviços, bens e sistemas que tem potencial para provocar impacto social, político, internacional ou à segurança do Estado, caso tenham seu desempenho degradado ou interrompido (BRASIL, 2014).

velocidade, com a intenção de causar vibrações, distorções excessivas e a destruição do equipamento (CLARKE, 2015). O processo como um todo pode ser explicado da seguinte forma:

> Após a fase inicial de reconhecimento gravando dados por 13 dias, o Stuxnet primeiro aumentava a frequência dos conversores para 1.410 Hz por 15 minutos e depois a reduzia para 1.064 Hz, presumidamente a frequência de operação normal, por aproximadamente 26 dias. Após gravar todos os dados que precisava gravar durante essas três semanas, o Stuxnet derrubava a frequência drasticamente para 2 Hz por cinquenta minutos, antes de restaurá-la para 1.064 Hz novamente. Após outros 26 dias, o ataque começava de novo (ZETTER, 2017, p. [4101]).

Portanto, percebe-se que cada ciclo de ataque do Stuxnet durava 65 dias, tendo como aspecto interessante a sofisticação da arma cibernética, que permitia que todo o processo ocorresse sem que os operadores percebessem qualquer anormalidade no sistema (GAZULA, 2017).

Isso posto, foram enumeradas as principais características que permitiram que o Stuxnet fosse considerado uma arma cibernética inovadora e desafiadora. A complexidade de seus métodos de propagação, a especificidade de sua carga útil e o seu pioneirismo em atacar Infraestruturas Críticas traziam oportunidades a planejadores operacionais. Assim, os novos métodos empregados poderiam proporcionar ataques precisos a diversos setores essenciais de uma sociedade, adotando como alvos sistemas como redes elétricas, sistemas de controle de tráfego e outros controlados por sistemas digitais.

3.4 O Stuxnet e o futuro da Guerra Cibernética

Embora o *worm* tenha contaminado milhares de máquinas em todo o mundo, o fato de a configuração do Stuxnet direcioná-lo para um alvo específico evitou um efeito devastador, devido à tendência de aumento de Infraestruturas Críticas que se utilizavam de sistemas de controle industriais era uma realidade à época.

Além disso, o ataque cibernético inovador demonstrou novas vulnerabilidades e

derrubou conceitos até então solidificados no ambiente cibernético, cabendo destacar os seguintes: a utilização de quatro *exploits* Dia-Zero, explorando vulnerabilidades desconhecidas; o emprego de certificados digitais válidos, colocando em xeque a confiança de um sistema que garantia a idoneidade de *softwares*; a propagação da ameaça a sistemas não conectados a alguma rede de computadores; e a possibilidade de causar danos físicos consideráveis a alvos remotos, por meio de um código malicioso (ZETTER, 2017).

Por conseguinte, é notório que o Stuxnet abriu as portas para futuros riscos consideráveis à segurança dos Estados. Desse modo, o novo estado da arte no ambiente cibernético implicou em novas políticas de utilização e proteção de plantas industriais. Adicionalmente, foi necessária a reestruturação dos sistemas de uma forma mais segura, evitando que novas ameaças pudessem se fazer valer de vulnerabilidades já identificadas anteriormente.

No que diz respeito ao aspecto mais amplo da guerra, o *software* malicioso desenvolvido pela Operação "Jogos Olímpicos" alterou o patamar das ações cibernéticas. O ataque realizado em Natanz criou o entendimento de que os danos causados a partir do ambiente cibernético podem causar mudanças duradouras no equilíbrio de poder em um conflito, sem a necessidade de intervenção de armas convencionais.

3.5 Avaliação das consequências do Stuxnet

Conforme já analisado, o Irã foi o epicentro das infestações pelo Stuxnet. A forma de propagação e o conteúdo lógico do *malware* evidenciaram que os planejadores da Operação "Jogos Olímpicos" buscavam a certeza de que o seu artefato cibernético obedecesse ao Princípio do Efeito da atividade cibernética, ou seja, que transformasse as ações cibernéticas em vantagem estratégica, operacional ou tática, afetando o mundo real (BRASIL, 2014).

Nesse sentido, o Stuxnet obteve significativo sucesso em suas intenções. Sua forma de atuação arrojada garantiu que, entre o final de 2009 e o início de 2010, cerca de mil centrífugas IR-1 da planta de enriquecimento de urânio da usina de Natanz, no Irã, fossem desativadas ou substituídas (ALBRIGHT *et al*, 2010).

No entanto, as centrífugas não foram as únicas estruturas afetadas pelo Stuxnet, já que o ataque cibernético também teve efeitos nos aspectos sociais, políticos e econômicos iranianos.

As consequências sociais e políticas estão associadas à indefinição do governo iraniano ao tratar publicamente dos ataques, o que pode ter afetado a credibilidade das lideranças daquele Estado. De acordo com Shakarian (2011), inicialmente em setembro de 2010, as declarações das autoridades tentaram minimizar o revés sofrido pelo programa nuclear iraniano, alegando que somente computadores pessoais foram afetados. Em contrapartida, dois meses mais tarde, em novembro do mesmo ano, o então presidente iraniano Mahmoud Ahmadinejad admitiu que suas usinas de enriquecimento de urânio foram alvos de ataques cibernéticos que afetaram suas centrífugas. Ainda de acordo com as declarações, o *malware* esteve ativo na planta nuclear de Natanz durante o período de aproximadamente um ano, enquanto especialistas buscavam conter e remover o código malicioso (ALBRIGHT *et al*, 2010).

Além desse fator, o ataque a Natanz também trouxe consequências negativas para o setor econômico iraniano. De acordo com Zetter (2017), o Irã, que já sofria com embargos econômicos internacionais, viu-se em uma situação complicada para substituir as cerca de mil centrífugas avariadas em Natanz e para manter a expectativa de produção de urânio enriquecido. Dessa forma, o Irã foi obrigado a adquirir material nuclear no mercado internacional, a despeito do seu limitado orçamento para suas usinas. Além de gerenciar os atrasos no seu programa nuclear, Teerã foi obrigado a rever medidas de segurança e investir

um significativo valor em cibersegurança para evitar novos ataques às suas Infraestruturas Críticas.

Por fim, Shakarian (2011) frisou que, apesar de as consequências do ataque terem sido rapidamente minimizadas pela república islâmica, as agências de inteligência estadunidenses e israelenses apontavam para retrocessos e atrasos significativos de, pelo menos, dois anos ao programa nuclear iraniano. Desse modo, é importante ressaltar que o EFD do ataque foi alcançado, diminuindo ligeiramente as tensões internacionais e demovendo Israel da ideia de lançar ataques aéreos para interrupção física do enriquecimento de urânio.

4 A ADERÊNCIA DO STUXNET À TEORIA DE WARDEN

Nos capítulos anteriores, foram descritas as ideias apresentadas pelo Coronel John Warden, com destaque para suas teorias de aplicação da força contra o oponente e a sua percepção do inimigo como um sistema, mais conhecida como a Teoria dos Cinco Anéis. Observou-se ainda, o caráter inovador do Stuxnet, um artefato cibernético que rompeu paradigmas ao aplicar um ataque que gerou danos físicos à usina de enriquecimento de urânio em Natanz, no Irã.

A partir de agora, será examinado se há aderência entre a estratégia operacional utilizada pelos planejadores da Operação "Jogos Olímpicos" e os postulados teóricos do Coronel Warden. Serão identificadas semelhanças e divergências entre o ataque do *software* malicioso e o pensamento de Warden sobre as três formas de aplicação da força. Tal análise abrangerá ainda a avaliação do Irã como um sistema, enfatizando os entes estratégicos representados pelos cinco anéis de Warden.

4.1 A aderência do ataque do Stuxnet às três formas de aplicação da força

Conforme já descrito, o pensamento estratégico do Coronel Warden é subdividido em três formas de aplicação da força contra o inimigo: a coerção, ou ataques paralelos; a paralisia estratégica; e a destruição.

Tendo em vista que Warden refutava a aplicação da força de destruição ao inimigo, e que o objeto da pesquisa – o ataque do Stuxnet – claramente não se destinou a uma destruição total do Irã, é razoável descartar preliminarmente a aderência dessa forma de aplicação da força à realidade. Com relação à estratégia da coerção por meio de ataques paralelos e à Estratégia da Paralisia, será conduzida uma análise mais aprofundada a seguir.

4.1.1 O ataque do Stuxnet e os ataques paralelos

De acordo com o pensamento de Warden (1995), a estratégia da coerção busca, por meio de ataques paralelos, tornar a capacidade de resistência do inimigo inviável, provocando danos parciais a estruturas importantes ou ameaçando a paralisia total do sistema inimigo. Sendo assim, a realização dessa estratégia conseguiria causar danos irrecuperáveis ao adversário, forçando-o a desistir de seus objetivos.

Ademais, observa-se que o Stuxnet carregava um código que ambicionava atacar Infraestruturas Críticas, entretanto as suas características lógicas direcionaram sua atuação, limitando-a a conversores de frequência específicos (CLARKE, 2015). Em razão disso, o ataque cibernético afetou somente as centrífugas IR-1 de enriquecimento de urânio em Natanz, poupando os demais sítios nucleares iranianos.

Pelo exposto, é possível afirmar que o Stuxnet não efetuou ataques paralelos ou operou simultaneamente nos níveis táticos, operacional e estratégico. Logo, nota-se que o ataque cibernético estadunidense e israelense ao programa nuclear iraniano não teve aderência à teoria dos ataques paralelos, apesar de ter buscado o esgotamento físico do inimigo, afetando-o em estruturas importantes.

4.1.2 O ataque do Stuxnet e a Estratégia da Paralisia

Sob a ótica de Warden, a Estratégia da Paralisia tem a intenção de incapacitar o inimigo (WARDEN, 1995), buscando um benefício político máximo, com o mínimo esforço militar ou custo. A busca pela decisão militar rápida, dirigida e contra a capacidade física ou mental do inimigo é utilizada como um meio para reduzir sua vontade moral de resistir.

Levando em consideração que as lideranças estadunidenses e israelenses decidiram por realizar um ataque cibernético a fim de impedir um esforço militar na região (ZETTER, 2017), pode-se afirmar que o Stuxnet garantiu um benefício político elevado frente

a um esforço militar relativamente reduzido.

Além disso, a Estratégia da Paralisia postulava que os esforços para incidir sobre o CG do inimigo devem ser feitos por meio de ações intermediárias e que deveriam priorizar estruturas vulneráveis do inimigo (WARDEN, 1988).

Comparando essa teoria ao método de propagação do *software* malicioso que afetou a usina de Natanz, constata-se que o Stuxnet aproveitou-se de vulnerabilidades do sistema de controle industrial da *Siemens*, utilizando *exploits* Dia-Zero que permitiram a penetração em um sistema que, na teoria, possuía uma segurança intransponível (SHAKARIAN, 2011). Ademais, a infecção de cinco organizações iranianas pode ser considerada como uma ação intermediária que precisava ser realizada para afetar o CG iraniano, caracterizando a aderência da teoria à realidade.

4.2 O ataque do Stuxnet e as bases estratégicas para o estudo do inimigo como um sistema

Antes de observar se a estratégia utilizada pelos planejadores da Operação "Jogos Olímpicos" tem aderência à visão do inimigo como um sistema, é imperioso verificar se essa campanha recorreu aos pressupostos estratégicos que o Coronel Warden empregou em seu postulado teórico. Sendo assim, será analisado se o desenvolvimento do Stuxnet pode se assemelhar ao processo de pensamento dedutivo e, ainda, se mirou a componente física do inimigo antes de compará-lo a um sistema composto por cinco anéis.

Destarte, tendo como alicerce o pensamento dedutivo, deve-se avaliar se o raciocínio que preparou o ataque cibernético pode ter observado a situação geral e o cenário mais amplo, passando ao foco no objetivo e no detalhamento das ações. Logo, considera-se que o pensamento dedutivo se enquadra na postura dos EUA e Israel que, desde 2006, levaram em consideração a conjuntura geral do Oriente Médio, identificando como objetivo o arrefecimento das intenções nucleares do Irã. Essa avaliação geral permitiu que a aplicação da

força e de armas convencionais fossem preteridas em prol da arma cibernética, pois a primeira alternativa poderia levar a uma indesejada campanha militar estadunidense na região. Em seguida, corroborando mais uma vez com o pensamento dedutivo de John Warden, os planejadores partiram para o detalhamento das ações carregando o *worm* Stuxnet com as frequências específicas das centrífugas IR-1 que, de acordo com Zetter (2017), existiam somente no sítio nuclear de Natanz.

No que diz respeito à utilização da componente física para atingir os efeitos desejados, de acordo com Warden (1995), o advento de armas precisas tornou factível a destruição do componente físico do inimigo, reduzindo os danos colaterais provocados pelos ataques e alterando sua relação com o moral do adversário. Assim, o postulado teórico estabeleceu que os esforços deveriam ser direcionados, primariamente, para o lado físico do oponente, tornando-o incapaz de se opor às nossas ações. Essa conclusão era compreensível, pois a destruição de alvos físicos é mais factível que um ataque ao moral do oponente.

Sob esse aspecto, é notório que o Stuxnet revolucionou o Espaço Cibernético, causando danos físicos por intermédio de um código malicioso. Anteriormente, a Guerra Cibernética era vista como limitada, por ser incapaz de coagir um oponente caso não fosse acompanhada de um poder convencional da guerra capaz de atuar causando efeitos de destruição ao espaço físico.

Portanto, a produção de efeitos cinéticos, além de ter sido uma quebra de paradigmas, possibilitou a concretização de uma premissa estabelecida pelo então presidente estadunidense George W. Bush: a de não causar efeitos colaterais ao Irã, restringindo os danos ao programa nuclear daquele Estado (ZETTER, 2017).

Dessa forma, ao concluir seu processo de propagação e seu ciclo de ataque, o Stuxnet se enquadrou de maneira satisfatória na categoria de arma precisa, permitindo um ataque em que as avarias causadas fossem limitadas às centrífugas de enriquecimento de

urânio em Natanz. Logo, o ataque teve como objetivo a componente física do programa nuclear e o comprometimento do moral iraniano em prosseguir com as suas intenções nucleares.

Por fim, nota-se que a Operação “Jogos Olímpicos” e o *software* malicioso Stuxnet tiveram aderência às bases estratégicas que permitiram a observação do inimigo como um sistema, dado que o planejamento aparentemente seguiu um raciocínio dedutivo e o ataque foi empregado como uma arma precisa que atingiu a componente física do inimigo.

4.3 A aderência do ataque à Teoria dos Cinco Anéis.

Em virtude do que foi mencionado durante a análise teórica, constatou-se que o postulado teórico de Warden considerava que todas as entidades estratégicas poderiam ser fragmentadas em cinco componentes. Essa compartimentação do sistema inimigo possibilita a identificação dos CG de uma forma mais simplificada, sendo que esses segmentos distintos contêm os pontos focais de uma campanha. Essa subdivisão do inimigo foi designada por Warden como Teoria dos Cinco Anéis.

Antes de prosseguir, é importante salientar que o teste de aderência será realizado na ordem inversa àquela apresentada no capítulo teórico, ou seja, primeiro será o anel mais externo, finalizando o estudo com o diagnóstico das consequências do ataque ao anel mais crítico: o anel da liderança.

4.3.1 O anel das forças militares iranianas

Consideradas como quinto e último anel do modelo teórico, as forças militares são enxergadas por Warden como protetoras dos demais entes estratégicos localizados nos anéis mais internos do sistema. Por ser projetado para resistir a ataques, esse anel deve ser tomado como um objetivo quando um CG localizado em anéis mais centrais só seja alcançável caso as

forças militares sejam suplantadas. Dessa forma, o coronel estadunidense rompe com o pensamento tradicionalista e passa a enxergar as forças militares como meios e não como um fim em si.

Relacionando essa teoria ao caso concreto do *worm* Stuxnet, é notório que a Operação "Jogos Olímpicos", em princípio, não visava a um ataque direto às forças militares iranianas. Na realidade, o ataque cibernético foi considerado justamente para impedir um conflito entre as forças convencionais dos EUA, Israel e Irã. Essa contenda seria inevitável caso a Força Aérea Israelense fosse empregada para frear o ímpeto nuclear de Teerã.

Por outro lado, em uma análise mais abrangente, é possível relacionar o ataque ao convencimento ocidental de que o Irã estava engajado em desenvolver seu armamento nuclear. Portanto, percebe-se que o Stuxnet afetou, indiretamente, o quinto anel de Warden, ao protelar o desenvolvimento nuclear do Estado iraniano, impedindo que suas forças armadas tivessem acesso ao armamento nuclear, tornando-se um contraponto ao poderio israelense na região.

4.3.2 O anel da população

O quarto anel operacional é aquele que comporta a população do sistema, neste caso a população iraniana. Apesar de ser um anel importante para o funcionamento do sistema como um todo, o pensamento estratégico de Warden refutava o ataque direto a esse ente estratégico. A recusa em utilizar esse tipo de ataque é baseada na dificuldade em atingir um grande número de alvos simultaneamente e pela impossibilidade de medir e de controlar os efeitos dessas investidas.

No que diz respeito ao *malware* Stuxnet, o código infectou cerca de 14.000 computadores no Irã, não distinguindo computadores pessoais de seu objetivo final: o programa nuclear iraniano (FALLIERE *et al*, 2011). No entanto, o *software* malicioso era

inativo em computadores pessoais, não tendo causado danos ou prejuízos diretos à população em geral.

Embora o episódio tenha gerado uma grande repercussão midiática à época, não há evidências de que os atacantes tenham explorado indiretamente a sensação de desconfiança e insegurança causada na população após a infecção pelo código malicioso. Portanto, os argumentos apresentados permite observar que o Stuxnet não buscou afetar o quarto anel do sistema iraniano.

4.3.3 As Infraestruturas Críticas

O terceiro anel estratégico é composto por infraestruturas críticas ao funcionamento do sistema. Essas infraestruturas representam elementos notáveis que impactam na circulação de bens, serviços e informações de um Estado, tais como as indústrias, os transportes e a estruturas de geração e transmissão de energia.

Apesar de Warden apontar para dificuldade de gerar danos consideráveis a CG localizados nesse anel, a parte lógica do *software* malicioso Stuxnet foi desenvolvida para atacar um CG em particular, considerado como uma Infraestrutura Crítica para Teerã.

Embora o Estado iraniano não tenha sido afetado de forma mais grave, o impacto na usina de enriquecimento de urânio de Natanz foi considerável. De acordo com Zetter (2017), esse dano pode ser mensurado em até vinte por cento da capacidade total da usina, causando avarias em aproximadamente mil centrífugas e gerando um prejuízo econômico importante ao programa nuclear iraniano. De acordo com estimativas das agências de inteligência estadunidenses e israelenses, o ataque atrasou as intenções nucleares do Irã em aproximadamente dois anos.

Além disso, o ataque cibernético trouxe consequências para o monitoramento de todas as Infraestruturas Críticas do Irã, pois a inovação da arma cibernética foi responsável

por comprometer o funcionamento do sistema SCADA. Dessa forma, o Stuxnet escancarou uma vulnerabilidade mundial de instalações industriais que faziam uso do referido sistema de monitoramento e obrigou o Irã a investir em cibersegurança, evitando ataques a outras estruturas importantes que eram controladas pelo SCADA (ZETTER, 2017).

4.3.4 Os elementos orgânicos essenciais

Com relação ao segundo anel do modelo teórico de John Warden, serão encontradas instalações que, se afetadas, tornam a manutenção do funcionamento do sistema praticamente inviável. Os aspectos logísticos e econômicos de um Estado estão localizados nesse círculo concêntrico e um ataque ao CG ali contido pode representar uma ameaça direta no abastecimento de insumos importantes como o petróleo, a energia e a alimentação, refletindo indiretamente nos demais círculos do sistema.

Conforme análise anterior, o ataque à usina de Natanz trouxe consequências negativas para o setor econômico iraniano, principalmente por demandar a substituição das centrífugas avariadas e por atrasar o programa nuclear do Irã (ZETTER, 2017). No entanto, esses impactos não chegaram a causar rupturas aos sistemas orgânicos essenciais daquele Estado. Logo, não houve um colapso econômico tampouco a paralisação do fornecimento de insumos importantes para o funcionamento dos demais círculos do modelo teórico.

4.3.5 O anel da liderança central

Por fim, será avaliado se o *malware* Stuxnet afetou o anel mais crítico do sistema iraniano, buscando compreender se o ataque modificou a estrutura do comando do Irã, obrigando-o a fazer concessões ou tornando-o incapaz de exercer seu papel de liderança e de direção do sistema. Caso não haja evidências de ameaças diretas às lideranças, que assumem a posição central no dispositivo dos cinco anéis, serão medidas eventuais aplicações de força

indireta aos demais anéis foi fundamental que possam ter influenciado decisões das autoridades iranianas.

Destarte, verificou-se que o ataque não foi direcionado diretamente ao anel da liderança. No entanto, os danos causados ao anel da Infraestrutura Crítica afetaram indiretamente o anel central, causando descrédito para as lideranças iranianas. Tal desconfiança foi gerada quando o governo de Teerã divulgou informações desencontradas sobre como o Stuxnet degradou a capacidade da usina de Natanz, retardando seu programa nuclear. A demora em admitir o impacto da invasão cibernética foi agravada pela incapacidade de identificar os autores dos ataques, impossibilitando uma retaliação a altura. Certamente, essa inação trouxe prejuízos à imagem do governo iraniano, apesar de não ter afetado a estrutura de comando do sistema como um todo.

Após encerrar a análise da aderência do ataque do Stuxnet às bases do pensamento estratégico do Coronel John Warden, à Estratégia da Paralisia e à Teoria dos Cinco Anéis, será feita uma síntese alinhavada no último capítulo, de forma a concluir esta pesquisa.

5 CONCLUSÃO

Ao estudar o episódio do ataque da arma cibernética Stuxnet à luz da Estratégia da Paralisia e da Teoria dos Cinco Anéis, buscou-se responder à pergunta que serviu como referência para o atingimento do objetivo deste trabalho: a Operação "Jogos Olímpicos" e o ataque realizado por meio do código malicioso Stuxnet tiveram aderência à Estratégia da Paralisia de John Warden e ao seu modelo teórico dos cinco anéis?

O modelo teórico apresentado expressava a ideia do uso da força, tendo como prioridade a Estratégia da Paralisia, que pregava a utilização de ataques paralelos aos oponentes. Tais ataques seriam mais eficazes se afetassem simultaneamente o inimigo em seus níveis tático, operacional e estratégico. A fim de identificar os melhores CG para o ataque, o inimigo deveria ser comparado a um sistema, composto por cinco anéis concêntricos, que representam a Liderança, os Elementos Essenciais, as Infraestruturas Críticas, a População e as Forças Militares. Esses anéis deveriam ser atacados tendo como prioridade a Liderança.

No que diz respeito ao ataque à usina de enriquecimento de urânio iraniana em Natanz, ocorrido em 2010, verifica-se que a investida tinha como pano de fundo uma disputa geopolítica cujo mote era o balanceamento de poder entre Estados na região do Oriente Médio. A intenção de manter o *status quo* na região levou os EUA e Israel a delinearem a Operação "Jogos Olímpicos", que tinha como EFD o refreamento do programa nuclear do Irã. Para atingir o objetivo, o ataque cibernético pelo *malware* Stuxnet se apresentou como alternativa a um ataque convencional pela Força Aérea Israelense.

Durante o desenvolvimento deste trabalho, percebeu-se que, apesar dos avanços tecnológicos das últimas décadas, até o ano de 2010, o Espaço Cibernético ainda possuía limitações na capacidade de coagir um oponente, face à sua impossibilidade de gerar danos físicos ao inimigo. Com o Stuxnet, a percepção sobre a importância das ações cibernéticas foi

alterada, dando margem para que as mesmas pudessem gerar consequências cinéticas, tornando-as um elemento essencial na condução da guerra.

A fim de atingir o propósito deste trabalho, confrontaram-se as características do ataque que destruiu cerca de mil centrífugas nucleares em Natanz ao modelo teórico apresentado pelo Coronel John Warden. Dessa maneira, foram alcançadas algumas conclusões, que serão detalhadas a seguir.

No que tange às formas de aplicação da força vislumbradas pelo modelo teórico, depreende-se que o ataque de 2010 não teve aderência à aplicação da destruição ou à coerção do Irã por intermédio de ataques paralelos e simultâneos.

A respeito da Estratégia da Paralisia, a pesquisa observou que a forma de propagação do Stuxnet e o delineamento do ataque ao programa nuclear iraniano visaram a um benefício político máximo, com o mínimo esforço militar. A semelhança do ataque com a Estratégia da Paralisia foi ainda além, uma vez que a investida explorou fragilidades dos componentes físicos da usina nuclear de Natanz e utilizou ações intermediárias para alcançar o CG do sistema iraniano.

De forma similar, o conteúdo lógico do *software* que infestou computadores ao redor do mundo foi planejado a partir de uma observação de um amplo cenário geopolítico chegando ao detalhamento necessário para atingir o CG da usina nuclear iraniana. Por tais razões, conclui-se que houve uma concordância entre o planejamento da Operação “Jogos Olímpicos” e o raciocínio dedutivo constante no arcabouço teórico utilizado.

Portanto, é possível observar aderência do ataque aos pressupostos teóricos da forma de aplicação da força por meio da Estratégia da Paralisia, com a utilização de um pensamento dedutivo e o emprego da componente física para o atingimento dessa estratégia. A utilização dos métodos de propagação do Stuxnet ainda garantem uma concordância do objeto analisado ao fato de que o Coronel Warden privilegiava armas precisas, que evitassem

danos colaterais desnecessários.

Já no que diz respeito ao aspecto mais conhecido do modelo teórico do Coronel Warden, a Teoria dos Cinco Anéis, chega-se à conclusão de que houve uma aderência parcial entre o ataque e os seus postulados. A concordância limitada entre o objeto e a teoria ocorre em virtude de não haver evidências de que o ataque tenha atuado no anel da população. Nos anéis da Liderança Central, dos Elementos Orgânicos Essenciais e das Forças Militares, observa-se que o Stuxnet os afetou de forma contida e indireta, não gerando o colapso desses entes. A comparação foi positiva, indicando uma aderência total no que diz respeito ao anel da Infraestrutura Crítica da usina nuclear de Natanz, que foi atingida em grande escala.

Por fim, depreende-se a validade do estudo para a MB, visto que o ambiente cibernético e os sistemas de controle industriais estão amplamente integrados a diversos componentes encontrados a bordo dos navios e meios operativos. O objeto da pesquisa demonstrou que os ataques cibernéticos evoluíram de forma tal, que mesmo os equipamentos mais protegidos estão sujeitos a ataques maliciosos. Por esse motivo, o desenvolvimento de uma mentalidade cibernética é fundamental, principalmente após a identificação da capacidade que os meios não cinéticos adquiriram de causar efeitos físicos em todos os domínios operacionais da guerra.

REFERÊNCIAS

ALBRIGHT, David; BRANNAN, Paul; WALROND, Christina. **Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?** Washington D.C.: Institute for Science and International Security Report, 2010. 10 p. Relatório.

ANRIG, Christian F.; WARDEN. John A. III; PAPE, Robert A. **The Art of Targeting:** A Comparison of Two Theoretical Conceptions, Zurique, *Air Power Revue Schweizer Armee* n. 3, p. 16-26, Dez. 2004. Disponível em: <http://doi.org/10.5169/seals-69342> Acesso em: 27 abr. 2020.

BRASIL. Ministério da Defesa. **MD-30-M-01: Doutrina de Operações Conjuntas**. vol I. 1 ed. Brasília, 2011.

BRASIL. Ministério da Defesa. **DCA 1-1/2012. Doutrina Básica da Força Aérea Brasilei**ra. vol I. 1 ed. Brasília, 2012

BRASIL. Ministério da Defesa. **MD-31-M-07: Doutrina Militar de Defesa Cibernética**. vol I. 1 ed. Brasília, 2014.

BRASIL. Ministério da Defesa. **MD35-G-01. Glossário das Forças Armadas.** 5 ed. Brasília, 2015.

BRASIL. Gabinete de Segurança Institucional. **Glossário de Segurança da Informação**. 1 ed. Brasília, 2019.

CHAPPEL JR., George G. **A Terrorist Organization as a System:** Unleashing Warden´s Five-Ring Model. 31 f. Dissertação – Faculty of the Naval War College, Newport, 2002.

CLARKE, Richard A. **Guerra Cibernética**: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport Livros e Multimídia, 2015. 241 p.

CLAUSEWITZ, Carl von. **Da guerra**. São Paulo: M. Fontes, Brasília: Ed. Univ. Brasilia, 1979. 787p.

COUTAU-BÉGARIE, Hervé. **Tratado de estratégia**. Rio de Janeiro: Diretoria do Patrimônio Histórico e Documentação da Marinha, 2010. 410p.

ESTADOS UNIDOS DA AMÉRICA. **JP 3-12: Cyberspace Operations.** Washington: Joint Chiefs of Staff, 2018.

FADOK, David S. **John Boyd and John Warden**: Air Power´s Quest for Strategic Paralysis. 61 f. Dissertação – USAF School of Advanced Airpower Studies, 1995. Disponível em: <https://media.defense.gov/2017/Dec/27/2001861508/-1/-1/0/T_0029_FADOK_BOYD_AND_WARDEN.PDF >. Acesso em: 10 jun. 2020.

FALLIERE, Nicolas; O´MURCHU, Liam; CHIEN, Eric. **W32 Stuxnet Dossier**. Cupertino: Symantec Corporation, 2011. 69 p. Relatório.

FRIESER, Karl-Heinz. **The Blitzkrieg Legend**: The 1940 Campaign in the West. Annapolis:

Naval Institute Press, 2013. 536 p.

GAZULA, Mohan B. **Cyber Warfare Conflict Analysis and Case Studies.** 2017. 100 f. Tese (Mestrado em Engenharia e Gerenciamento) – Boston University, Boston, 2017.

GERMER, André *et al*. **O Irã Nuclear.** *Coleção Meira Mattos – Revista de Ciências Militares.* Rio de Janeiro. n. 21, 2010. Disponível em: <http://ebrevistas.eb.mil.br/index.php/RMM/article/view/47/71>. Acesso em: 22 jul. 2020.

HOUAISS, Antonio. **Minidicionário Houaiss da língua portuguesa**. Rio de Janeiro: Objetiva, 2004. 976 p.

KERR, Paul K. **Iran´s Nuclear Program:** Status. *Congressional Research Service Report for Congress.* 2009. Disponível em: <https://fas.org/sgp/crs/nuke/RL34544.pdf>. Acesso em: 22 jul. 2020.

LIMA, Martonio M. B.; FREITAS, M. O. **Programa Nuclear do Irã e Panorama Internacional.** *Revista Jurídica*, Curitiba, v. 03, n. 44, p. 355-380, 2016. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/1920/1268>. Acesso em: 22 jul. 2020.

LOPES, Gills V.; OLIVEIRA, Carolina F. J. **Stuxnet e defesa cibernética estadunidense à luz da análise de política externa**. *Revista Brasileira de Estudos de Defesa,* v. 1, n. 1, p. 55-69, 2014. Disponível em: <https://rbed.abedef.org/rbed/article/view/39457/30874>. Acesso em: 20 jun. 2020.

OGÎGĂU-NEAMȚIU, Florin; MOGA, Horațiu. **A Cyber Threat Model of a Nation Cyber Infrastructure Based on Goel-Okumoto Port Approach.** *Land Forces Academy* Review, Sibiu, v. 23, n. 1, p 75-87, 2018.

OLSEN, John A. **John Warden and the Renaissance of American Air Power**. 1 ed. Washington, D.C. Potomac Books, Inc, 2007, 374 p.

PINTO, Pedro Miguel X. E. F. **Giulio Douhet e John Warden**: Aspectos Evolutivos da Teoria do Poder Aéreo. *IDN - Revista Nação e Defesa*. Lisboa, n. 106, p. 153-196, 2003. Disponível em: <https://comum.rcaap.pt/bitstream/10400.26/1372/1/NeD106_PedroMiguelXavierEstradaFontesPinto.pdf>. Acesso em: 14 abr. 2020.

SIQUEIRA, Mauro B. **A Eficácia do Poder Aéreo à luz das Estratégias da Paralisia e da Coerção**: Teorias de John Warden III e de Robert Pape. In: ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 1, 2007, São Carlos. Disponível em: <https://www.abedef.org/conteudo/view?ID_CONTEUDO=74 >. Acesso em: 25 mai. 2020.

SHAKARIAN, Paulo. **Stuxnet: Cyberwar Revolutions in Military Affairs**. *Small Wars Journal.* 14 abr.2011. Disponível em:<https://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs>. Acesso em: 22 jul. 2020.

WARDEN, John A. **The air campaign**: planning for combat. Washington, DC: National Defense University Press, 1988. 193 p.

WARDEN, John. A. **The enemy as a system**. *Airpower Journal*, Pensilvânia, EUA, v. 9. n. 1, p.41-55, primavera 1995. Disponível em: <https://www.airuniversity.af.edu/Portals/ 10/ASPJ/ journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf >. Acesso em: 22 mai. 2020.

WARDEN, John A., RUSSELL, Leland A. **Winning in FastTime**: Harness the Competitive Advantage of Prometheus in Business and Life, Montgomery, Venturist Inc; 7th Edition, 2001. 224 p.

ZETTER, Kim. **Contagem regressiva até zero day**: Stuxnet e o lançamento da primeira arma digital do mundo. Rio de Janeiro: 2017. [10979].