UNESP Universidade Estadual Paulista
Faculdade de Filosofia e Ciências
– Campus de Marília –

GABRIELA CRISTINA ROCHA

CASO STUXNET: OS IMPACTOS DO ATAQUE CIBERNÉTICO AO PROGRAMA NUCLEAR DO IRÃ COM A PRIMEIRA ARMA CIBERNÉTICA À SEGURANÇA INTERNACIONAL (2009-2010)

MARÍLIA-SP
2022

GABRIELA CRISTINA ROCHA

CASO STUXNET: OS IMPACTOS DO ATAQUE CIBERNÉTICO AO PROGRAMA NUCLEAR DO IRÃ COM A PRIMEIRA ARMA CIBERNÉTICA À SEGURANÇA INTERNACIONAL (2009-2010)

Trabalho de Conclusão de Curso apresentado ao Conselho de Curso de Relações Internacionais da Faculdade de Filosofia e Ciências, da Universidade Estadual Paulista "Júlio de Mesquita Filho" – UNESP (Campus de Marília), para a obtenção do título de Bacharel em Relações Internacionais.
Orientador: Dr. Rafael Salatini de Almeida

MARÍLIA

2022

R672c

Rocha, Gabriela Cristina
CASO STUXNET: : OS IMPACTOS DO ATAQUE CIBERNÉTICO AO PROGRAMA NUCLEAR DO IRÃ COM A PRIMEIRA ARMA CIBERNÉTICA À SEGURANÇA INTERNACIONAL (2009-2010) / Gabriela Cristina Rocha. -- , 2022
57 p. : tabs.

Trabalho de conclusão de curso - Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, Marília
Orientador: Rafael Salatini de Almeida

1. cibersegurança. 2. Stuxnet. 3. segurança internacional. 4. Irã. 5. programa nuclear do Irã. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Filosofia e Ciências, Marília. Dados fornecidos pelo autor(a).

GABRIELA CRISTINA ROCHA

CASO STUXNET: OS IMPACTOS DO ATAQUE CIBERNÉTICO AO PROGRAMA NUCLEAR DO IRÃ COM A PRIMEIRA ARMA CIBERNÉTICA À SEGURANÇA INTERNACIONAL (2009-2010)

Trabalho de Conclusão de Curso para obtenção do título de Bacharel em Relações Internacionais, da Faculdade de Filosofia e Ciências, da Universidade Estadual Paulista "Júlio de Mesquita Filho"– UNESP (Campus de Marília).

BANCA EXAMINADORA

Orientador: _____

Dr. Rafael Salatini de Almeida (UNESP-Marília)

1º Examinadora: _____

Ma. Gabrielle Custódio Carinheno (UNESP-Marília)

2º Examinadora: _____

Ma. Raquel Torrecilha Spiri (UNESP-Marília)

Marília, SP, 19 de abril de 2022.

RESUMO: Utilizando-se do método qualitativo descritivo, com base bibliográfica, o presente trabalho tem como objetivo estudar os impactos da atuação do *worm* de computador Stuxnet no programa nuclear do Irã, entre os anos de 2009 e 2010, para a segurança internacional. Visto que o Stuxnet, declarado com a primeira arma cibernética já criada, se mostrou um código de alta complexidade e capacidade de destruição nunca antes registrada, voltada para uma infraestrutura essencial, como instalações nucleares para produção de energia elétrica. Fato pelo qual transformou a noção de ciberespaço dentro de um cenário de guerra, valorizando o campo da cibersegurança, decorrente da exposição da fragilidade de uma sociedade integrada na era digital, frente a ameaças cibernéticas, que, em razão da multissetorialidade, podem atingir diversas áreas de atuação, prejudicando um ou mais Estados, de forma abrangente, tanto na economia, na política e até mesmo na área saúde. Impulsionando mudanças na segurança tanto nacional quanto internacional, para comportar esse novo tipo de conflito.

PALAVRAS-CHAVE: cibersegurança; *Stuxnet*; segurança internacional; Irã; programa nuclear do Irã.

ABSTRACT: Using the descriptive qualitative method, based on literature, the present work aims to study the impacts of the Stuxnet computer worm on Iran's nuclear program, between 2009 and 2010, for international security. Whereas Stuxnet, declared to be the first cyber weapon ever created, proved to be a code of high complexity and never-before-recorded destruction capability, aimed at essential infrastructure, such as nuclear facilities for the production of electrical energy. This fact has transformed the notion of cyberspace within a scenario of war, valuing the field of cybersecurity, resulting from the exposure of the fragility of an integrated society in the digital age, in the face of cyber threats, which, due to multisectoral nature, can affect several areas. of action, harming one or more States, in a comprehensive way, both in the economy, in politics and even in the health area. Driving changes in both national and international security to accommodate this new type of conflict.

KEYWORDS: cybersecurity; Stuxnet; international security; Will; Iran’s nuclear program.

AGRADECIMENTOS

Primeiramente, à minha família, meus pais Marco e Márcia, meu irmão Lucas, meus avós Antônio e Maria, minhas tias Silvia e Fabiane, meu tio Marco e minhas primas Letícia, Larissa e Luisa, por sempre acreditarem em mim, estarem presentes sempre que eu precisava, pelo apoio que me deram, pelas palavras e incentivo. Só cheguei até aqui por vocês.

Às minhas amigas Paula e Thamires, pelas quais eu nem tenho palavras para descrever o tamanho da gratidão que eu tenho. Vocês fizeram cada ano da minha graduação valer a pena. Agradeço por cada vez que me senti insegura e fui acolhida por seus atos e palavras, por todas as vezes que nos encontramos para conversar e estudar, que saímos, cada momento e risada com vocês, todas as memórias que sempre vou carregar no meu coração.

A todos que eu amo e que nunca poderia esquecer de agradecer, que sempre me deram tanto apoio, carinho e torceram tanto pelas escolhas que eu fiz: Victória, Ana Claudia, Weslley e Tiffany, vocês fizeram parte dessa trajetória desde o começo.

A todos os professores que ajudaram na minha formação, desde os meus primeiros anos na escola, até hoje, em minha graduação. Vocês me inspiraram e ajudaram a construir a pessoa que sou hoje.

À Faculdade de Filosofia e Ciências da Universidade Estadual Paulista "Júlio de Mesquita Filho" (campus Marília), por proporcionar uma das experiências mais enriquecedoras de minha vida.

.

SUMÁRIO

INTRODUÇÃO

A tecnologia e a internet, nos dias atuais, são recursos indispensáveis para a sociedade. Todos os âmbitos da vida de uma pessoa estão integrados ao uso dessas ferramentas, exemplificado pelo fato de que, cada área de estudo, nomeia essa transformação de uma maneira conveniente para seus estudos; seja de Era da Informação, Era Digital ou afirmando o acontecimento da Quarta Revolução Industrial, todas se referem à mesma integração do cotidiano ao ciberespaço. Essa incorporação tem sido potencializada nos últimos anos, não unicamente pelos avanços tecnológicos, mas sofrendo também, aceleração, devido ao evento da pandemia do COVID-19, que criou a necessidade de adaptação de diversas atividades, para que essas persistissem no cenário de crise sanitária mundial.

E a área militar, como os demais setores, está sempre se atualizando, e, em muitos casos, foram dentro desses estudos que as tecnologias citadas anteriormente foram criadas, como a internet e o computador, com intuito de serem eficazes tanto atacando quanto se protegendo em conflitos. Analisando a história, percebe-se o uso tecnológico para mudar a forma como as guerras eram travadas. A inclusão de armas de fogo e de armas nucleares em divergências armadas foram pontos críticos de transformação para a segurança nacional e internacional dos países. Então, não seria diferente com o ciberespaço, desenvolvendo o tipo bélico de arma cibernética.

A primeira arma cibernética a ser criado, um *worm* de computador, que infectou as máquinas da instalação nuclear de Natanz, no Irã, e causou danos físicos nesta propriedade, trouxe aos holofotes internacionais, a necessidade de uma maior atenção para a cibersegurança, tendo em vista a periculosidade de um programa malicioso como este, capaz causar danos físicos para uma instalação, poderia ter para essa nova sociedade extremamente dependente da tecnologia.

O método qualitativo descritivo, de base bibliográfica, foi usado para fazer esse levantamento, com intuito de analisar quais foram os impactos causados na segurança internacional pelo Stuxnet, considerado como primeira arma cibernética usada para infiltrar nas máquinas de enriquecimento de urânio do Irã, na instalação de Natanz, entre os anos de 2009 e 2010, prejudicando a integridade das mesmas.

No primeiro capítulo, é discutida de uma forma breve a conceituação do termo "segurança", que foi se modificando para um termo com significado mais amplo até

chegar à significação dos dias atuais. Assim como ocorre com os grandes debates da Teoria de Relações Internacionais, que restringia a questão de segurança internacional apenas à área militar, até que, após a Segunda Guerra Mundial (1939-1945), por influência da Escola de Copenhague, admitiu-se que há uma pluralidade de setores envolvendo a segurança. E é nessa abrangência que o subcampo da cibersegurança pode ser mais bem estudado, tendo em vista que, no século XXI, com os avanços da tecnologia, os riscos para a segurança provindos do ciberespaço aumentaram. Principalmente após um ataque crítico a uma instalação nuclear do Irã (2009-2010).

O segundo capítulo apresenta um pouco da história do Irã e a sua relação com o cenário internacional, uma vez que o país foi o palco do ataque cibernético, entre 2009 e 2010, na instalação nuclear de Natanz. Através dessa exposição, fica claro quais são os países com que o governo iraniano não possui boas relações e por que seu programa nuclear é um assunto tão discutido. Promovendo, assim, um maior entendimento da questão política que permeia o ataque, quem seriam os responsáveis e a motivação deste.

O último capítulo expõe sobre o ataque cibernético de fato, a partir da construção do cenário anterior, teorizando sobre os responsáveis e a intenção de criação do que seria considerada a primeira arma cibernética, o *worm* de computador Stuxnet. Um código de programa de alta complexidade desenvolvido para prejudicar as centrífugas de enriquecimento de urânio iranianas, responsável pela percepção da importância da cibersegurança dentro da segurança internacional. Já que os ataques agora não se limitavam a atingir esferas militares, pois as principais infraestruturas dos países utilizam da integração ao ciberespaço para proporcionar facilidades aos usuários, colocando outras esferas da sociedade em risco.

CAPÍTULO 1. SEGURANÇA E AS TEORIAS DE RELAÇÕES INTERNACIONAIS

Antes de abordar o campo teórico de segurança internacional, necessita-se entender a historiografia do termo "segurança", compreendendo que o mesmo passou por numerosas transformações para alcançar a abrangência dos dias atuais, sendo então intrinsecamente ligada com as relações internacionais e um âmbito político nacional (SILVA; NUNES; SILVA, 2018). A percepção de sua significância possibilita assimilar qual o objeto de estudo do assunto no âmbito acadêmico, ao decorrer de suas transformações compreensivas.

Ainda que sem um conceito definido, a palavra já aparece no primeiro século antes de Cristo, aludindo uma conotação negativa, que se perpetuou até o período medieval, nunca assumindo um sentido totalmente positivo. Nos primórdios do absolutismo, um importante questionamento sobre a quem a segurança estava relacionada foi levantado, constatando a modificação que ocorreu de que antes era algo que fazia referência a um indivíduo e, a partir do momento em que os Estados modernos surgiram, estes assumem a responsabilidade principal para a segurança (SILVA; NUNES; SILVA, 2018).

Ao decorrer da história, diversos pensadores de grande renome, como Hobbes, Montesquieu e Adam Smith, teorizam sobre o termo, e, de forma gradual, uma noção comum foi formada, na qual o indivíduo é ligada à segurança, e o papel do Estado é o de defesa, garantindo a proteção tanto da violência interna da sociedade quanto de outras sociedades independentes (McSWEENEY, 1999). Contudo, o conceito não permaneceu estático, sua definição assumiu uma polissemia, adaptando-se às ocorrências da história humana e às necessidades do que segurança deveria abranger.

No século XVII, o termo sofreu influência do modo de produção capitalista da época, no qual a palavra "segurança" agora se relacionava com objetos de posse, como terras, propriedades e dinheiro. E as ações de defesa exercidas pelo Estado deveriam ser feitas através de fortificações e armas militares, assim sendo capaz de proteger o indivíduo. Com a Revolução Francesa e a nova Declaração dos Direitos do Homem e do Cidadão, datada de 1793, reforça-se essa visão do Estado como um meio para a

segurança. É nesse momento também, em razão das guerras revolucionárias e napoleônicas, que o conceito ganha um caráter mais coletivo, voltando-se mais para a sociedade, sobrepondo-se ao pensamento mais individualista. Entende-se então que, para que o indivíduo tenha segurança, seria imprescindível a segurança da nação (SILVA; NUNES; SILVA, 2018).

Com a antropomorfização do Estado, há o raciocínio de segurança como um processo político coletivo, percebendo a sociedade como algo único e indivisível. Baseando-se nesse pensamento, a noção de segurança nacional, que está ligada ao individual de cada Estado, agora visto como os indivíduos, deveria ser obtido através de processos coletivos, sendo estes relacionados com ações internacionais (AMARAL, 2008, p. 53). Essa lógica ganha reforço com o Congresso de Viena, de 1815. Logo, fica evidenciado que, no século XIX, a segurança do coletivo, do Estado, acaba sobrepondo a do indivíduo, conquanto a ideia de segurança seja mais correlacionada com o conceito de uma "paz doméstica" do que com assuntos internacionais. E, enquanto isso, os Estados estariam em busca da consolidação interna, pelo que mais tarde as nações de unificação mais recentes seriam protagonistas de disputas internacionais (SILVA; NUNES; SILVA, 2018).

O século XX apresenta um ponto crucial tanto para a significação de segurança quanto para seus objetos de estudo. Ambos sofrem por ampliações de suas delimitações, possibilitando nessa nova abrangência englobar assuntos até mesmo na atualidade. É nesse momento também que o estudo da segurança passa a ser relacionado com o âmbito das Relações Internacionais. Isso porque este período foi marcado por diversas guerras de escala mundial, que sustentaram a segurança em um pensamento internacional, sendo ela o meio de garantir os interesses de segurança nacional.

Devido a animosidades entre nações, em que muitos países estabeleceram relação de hostilidade, como os EUA e a URSS, a expressão "segurança internacional" ganha força e passa a fazer parte dos discursos internacionais. Entretanto, a nova expressão não minimiza a segurança nacional, mas apenas explicita que não há como pensar em segurança nacional sem envolvimento em assuntos internacionais (SILVA; NUNES; SILVA, 2018).

Tendo observado, introdutoriamente, a evolução da significância do termo "segurança" através da história, explicitando a abrangência adotada até mesmo na agenda de estudos e nos quesitos de possíveis ameaças, torna-se possível, dentro da área

de estudos da segurança internacional, estudar um termo relativamente novo, mas não menos nocivo para a segurança do Estado, e, consequentemente, do indivíduo: "cibersegurança".

A cibersegurança é um tema integrante dos estudos do ciberespaço, que nas últimas décadas têm ganhado muito destaque, devido, principalmente, ao crescimento exponencial de ataques e ameaças cibernéticas. Fomentando a necessidade de discussão sobre o assunto, até mesmo pelo Conselho de Segurança da ONU, e constantemente vigiado através da União Internacional de Telecomunicações (agência especializada da ONU). Essa nova fonte de preocupação da segurança internacional foi evoluindo juntamente com os desenvolvimentos tecnológicos que vêm transformando a humanidade (FONSECA, 2021).

Isso pois a sociedade passou a ser dependente dessas novas tecnologias nascidas no meios militares, que passaram a integrar o cotidiano do ser humano em virtude das facilidades trazidas, principalmente pela computação, começando o que foi chamado, por Klaus Schwab em sua obra, *A Quarta Revolução Industrial* como "Terceira Revolução Industrial", datando da década de 1960, quando tanto o computador quanto a internet se desenvolveram e difundiram. A partir desse momento, os processos econômicos, políticos e sociais sofreram uma reestruturação com maior dinamismo e complexidade, em função desses avanços tecnológicos. Essas modernizações não sofreram uma desaceleração, apenas se potencializaram, dando início ao termo que nomeou o livro, a chamada "Quarta Revolução Industrial", fase atual do século XXI.

Isso se deve também porque, nos anos 1990, foi desenvolvido a *World Wide Web* (WWW), um programa que criava uma interface visual, possibilitando que o usuário visualizasse as informações presentes na internet de forma mais fácil e clara. Observa-se, então, uma rápida evolução tecnológica, além de uma fusão das tecnologias e integração dos domínios físicos, biológicos e digitais (SCHWAB, 2016, p. 18). Ou seja, a tecnologia expandiu seus campos de atuação e se transformou para atender às necessidades das pessoas, independente da área. Com a internet sendo considerada uma rede global de computadores, que mudou significativamente a comunicação, surgindo dela a nomeada "sociedade digital", da qual hoje cerca de 60% da população mundial faz uso (FONSECA, 2021).

Com a pandemia da Covid-19, a necessidade e o uso de tais ferramentas foi de suma importância para que, mesmo com as atividades presenciais suspensas, as

empresas, escolas de ensino de todos os graus, prestações de serviços e outros tipos de estabelecimentos continuassem com suas atividades. Então, a transformação digital que já estava ocorrendo foi acelerada em razão do acontecimento, quando cada vez mais a rotina das pessoas foi infundida à tecnologia, através de redes sociais, *e-commerce*, aplicativos, *home office* e ensino à distância (EAD).

Até mesmo ações que antes necessitavam da presença física, como ir ao banco, foram adaptadas para essa nova era digital. E não se limitando apenas para o lado mais econômico, a tecnologia foi e é uma peça fundamental para o estudo da doença do coronavírus, auxiliando no desenvolvimento de vacinas em larga escala, produção de aparelhos hospitalares, além de outras medidas preventivas que foram criadas e disseminadas nesse período.

Perante o cenário atual apresentado, no qual diariamente milhões de dados transitam pela internet, entende-se a valorização do estudo do ciberespaço dentro das Relações Internacionais, percebendo que, apesar da internet ser um ponto principal da área, usando como nomeação, o termo criado pelo escritor americano-canadense de ficção, William Gibson, para seu livro de ficção, Fonseca afirma que:

> O ciberespaço configura-se como um universo sem fronteiras e multifacetado, por onde trafega uma infinidade de informações, podendo impactar várias áreas e estar suscetível a distintas abordagens, por meio de diversas perspectivas: política, sociológica, jurídica, tecnológica, entre outras. No que se refere às Relações Internacionais (RI), é inquestionável a capilaridade e as implicações do ciberespaço nas temáticas inerentes à área. (2021, s/p)

Ou seja, não é limitado apenas à internet, mas, antes disso, diversos sistemas já integravam o espaço cibernético, como as telecomunicações, tráfego aéreo e navegação marítima (FONSECA, 2021). Elementos dos quais os Estados já entendiam a necessidade de defesa e segurança. Pensando na influência que o ciberespaço em sua totalidade possui no âmbito das Relações Internacionais, autores como Lopes, Kremer e Müller instigam um debate acadêmico sobre o assunto, alegando até mesmo a criação de um subcampo científico intitulado de Relações Internacionais Cibernéticas (CiberRI), em que o foco seria estudar a interação do ciberespaço tanto na relações internacionais em si quanto no campo acadêmico, sugerido por Lopes (*apud* FONSECA, 2021).

Esse caráter interdisciplinar do ciberespaço possibilita que o mesmo seja um objeto de análise para vários campos integrantes das Relações Internacionais, como comércio exterior, cooperação internacional, economia, política, entre outros. Ou, neste

caso, no campo da segurança internacional, em que, devido a ser um espaço propício não apenas para novas oportunidades surgirem, mas também para novas ameaças para o cenário internacional, que devem avaliadas. Diante dessas mudanças, todo uma nova tipologia foi originada de incidentes cibernéticos, como se pode observar através do quadro 1.

QUADRO 1. TIPOLOGIA DE CONFLITOS CIBERNÉTICOS

Termo	Significado
Ciberdefesa	Tem a função de garantir a realização de missões de defesa.
Crime cibernético (cibercrime)	Desenvolvimento de ações ilícitas com o emprego de computadores e da internet.
Espionagem cibernética	Finalidade de se testar a configuração e os sistemas de defesa de um determinado computador, ou ganhar acesso a informações sigilosas
Guerra cibernética	Emprego de meios eletrônicos para atrapalhar as atividades de um inimigo, bem como atacar sistemas de comunicação, podendo corresponder também a incidentes cibernéticos de natureza política variada.
Guerra da informação	Pode ser definida como qualquer ação de negação, exploração, corrupção ou destruição das estruturas e funções de informação do adversário, ao mesmo tempo adotando condutas para contrariar essas ações quando provenientes dos adversários, e potenciando as próprias capacidades de gestão de informação.
Sabotagem cibernética	Criação de empecilhos ao desenvolvimento de processos e rotinas de trabalho nos setores público e privado a partir de meios eletrônicos.
Terrorismo cibernético	Ataques ilícitos contra computadores – e a informação neles armazenadas – e redes computacionais com o objetivo de intimidar ou coagir governos e/ou suas populações para o alcance de objetivos políticos. Dos ataques, deve decorrer a violência contra bens e pessoas, tanto quanto for necessária para se gerar o nível de medo adequado ao rótulo de "terrorismo cibernético".

Fonte: MILITÃO, 2014; MÖCKLY *apud* FONSECA, 2021.

No início dos anos 1990, segundo Hansen e Nissenbaum (*apud* FONSECA, 2021), a cibersegurança – também um novo termo que será analisado de forma separada dos demais nesse momento – estava ligada a questões de segurança referentes aos

computadores em rede, de uma maneira muito mais isolada e ligada ao pessoal. Contudo, os efeitos das ameaças cibernéticas não afetavam apenas as partes ligados à área técnica, mas eles se mostravam de grande periculosidade até mesmo nas áreas sociais. Com essa percepção, houve a necessidade ampliar seu estudo, agora sendo parte das agendas tanto da segurança nacional quanto da internacional e parte das funções estratégicas do Estado (FONSECA, 2021).

Assumindo uma caracterização que engloba essa nova agenda, a União Internacional das Telecomunicações definiu cibersegurança como um conjunto de políticas, diretrizes, ações, treinamentos, ferramentas, melhores práticas, análises de gestão de risco, proteções de segurança e tecnologias que podem ser aplicadas visando à proteção do ambiente cibernético e dos ativos da organização e dos usuários (*apud* FONSECA, 2021). Um importante ponto de vista exposto por Fonseca é que:

> A característica principal da cibersegurança é a sua transversalidade. Sua abrangência alcança diferentes áreas (política, econômica, social, segurança, militar) e segmentos (setores público e privado, sociedade civil, academia, etc.) de um país, logo, requer um conjunto de ações integradoras e multissetoriais. Em vista disso, a cibersegurança precisa ser compreendida como um ecossistema constituído de diversas variáveis […]. (2021, s/p)

A pluralidade evidenciada pelo trecho demonstra a seriedade com que o assunto deve ser tratado pelos Estados, pois as suas infraestruturas vitais, como sistemas de saúde, energia, bancos, abastecimento de água, portais de serviços voltados à população, etc. estão todos utilizando o ciberespaço, e, caso sofram de algum tipo de ataque ou paralisação, os prejuízos serão sentidos de maneira severa nas mais diversas áreas da sociedade (FONSECA, 2021). Por essa razão, o tema já se tornou pauta fixa dentro das discussões dos governos e organizações internacionais, sendo destaque na segurança internacional, no que foi considerado como segurança cibernética (LOPES, 2016, p. 16).

Uma complexidade dessa interdisciplinaridade do ciberespaço é que um ataque não precisa ser voltado para atividades ligadas aos governos para que os impactos sejam sentidos pelos mesmos, pois um *site* com dados pessoais ou uma rede social paralisada já podem abalar a segurança nacional e a economia de um país, e, nessa linha de raciocínio, a cibersegurança requer o mesmo alcance.

Tendo discorrido sobre segurança e cibersegurança e entendido a problemática que as cerca, foi demonstrado de forma introdutória a ligação entre os termos e o campo de Relações Internacionais, não se aprofundando de maneira considerável no papel dos

debates teóricos da área de estudo nas mudanças em segurança, mesmo tendo sido mencionado que, ao final da Guerra Fria (1945-1991), a palavra tenha adquirido um caráter holístico.

As discussões acerca das relações entre diferentes comunidades políticas não é novidade, contudo a institucionalização da disciplina de Relações Internacionais só obteve maior destaque com o fim da Primeira Guerra Mundial (1914-1919), com o viés idealista político, surgido da necessidade de entender o acontecimento da guerra, com intuito de evitar que ocorrências como tais se repetissem no futuro. Nas duas décadas que se seguiram, a política internacional assumiu juntamente uma influência do realismo político (SILVA; NUNES; SILVA, 2018), estabelecendo então o que ficou conhecido como "primeiro grande debate das relações internacionais", entre o realismo, que acreditava na anarquia do sistema internacional, na qual a soberania do Estado prevalecia, e o idealismo, que se pautava na possibilidade da existência de um órgão soberano acima aos Estados (VIGNESWARAN, 2004, p. 05).

Esse debate intelectual durou até o final da Segunda Guerra Mundial (1939-1945), ocorrendo a partir de então uma predominância dos pensamentos realista, reflexo do mau desempenho dos mecanismos de segurança propostos pelos liberais após a então chamada Grande Guerra, que sugeriam uma redução do poder militar de cada Estado-nação em favor do fortalecimento de uma força militar comandada pela comunidade internacional *(SILVA; NUNES; SILVA, 2018)*

Com esse cenário em que o realismo se mostrou dominante e com as perspectivas de paz pós-Segunda Guerra Mundial, Amaral escreve sobre um entendimento prevalecente na época, afirmando que "pensar em Relações Internacionais implicava pensar a guerra", assim como "pensar a guerra era pensar a violência" e "pensar a violência nos levaria a pensar a segurança" (2008, s/p). E por essa razão que há uma semelhança entre a composição teórica de Relações Internacionais e o estudo voltado para a subárea de segurança, sofrendo com a marginalização de pensamentos que se diferem do estabelecido pelo de maior domínio. Amaral aponta ainda que até mesmo o conceito de segurança sofre com isso, sendo consagrada pelo realismo como "ausência de ameaças militares de origem externa à sobrevivência ou à soberania do Estado-nação em um sistema internacional anárquico" (2008, s/p). Tanto a disciplina quanto a subárea adotaram esse conceito por um considerável tempo, sem que houvesse questionamentos da academia (AMARAL, 2008).

Essa hegemonia do pensamento realista é percebida na base teórica de Relações Internacionais, sendo formada no período entre-guerras, com a sistematização do realismo clássico por estudiosos da área. Um desses teóricos é Edward Carr, autor de grande renome dentro deste campo disciplinar, que levantara um ponto extremamente relevante nessa perspectiva, que é o fato que as noções liberais possuem ausência da variável "poder". Afirmando ainda mais o discurso do realismo político.

É com Hans Morgenthau que se inicia o processo de criar uma teoria realística sobre a política internacional, na qual os pontos principais são "poder" e "interesse nacional", argumentando ainda que não existe uma grande diferença entre política interna de um Estado e a internacional, a não ser pelo fato da primeira seguir a legislação interna e a última permanecer anárquica, em que o poder era visto através das ações individuais voltadas para o interesse de cada Estado.

Em contrapartida, Raymond Aron alegava que existia sim uma diferenciação entre as políticas internas e internacionais, ainda que as mesmas tenham como objetivo comum a sobrevivência. Mas ele concorda com a importância imposta ao Estado em relação à segurança, afirmando que o cerne das relações internacionais são as relações interestatais (SILVA; NUNES; SILVA, 2018).

Nesse cenário, com o interesse sendo a principal motivação de um Estado, as forças armadas se tornam uma peça fundamental para a estratégia da balança de poder (SILVA; NUNES; SILVA, 2018), pois, com elas, o Estado garante seu território, defendendo-o, e consegue exercer um domínio sob aqueles que possuem as forças armadas mais fracas ou mesmo não possuem as mesmas. Sendo esse um estratagema para equilibrar o poder dentro de um sistema internacional anárquico.

A partir desse momento, várias noções realistas, que assumiam um caráter mais individual e material, pautando que o Estado seria o ator racional, utilizando estratégias de forma que tragam sucesso para a política externa, influenciaram o desenvolvimento de teorias sobre a questão de segurança internacional, como o dilema de segurança de Herz.

Entretanto, seria o trabalho de Kenneth Waltz que ganharia destaque pelo impacto causado nas Relações Internacionais, sua proposta chegando a fomentar o surgimento do chamado "terceiro debate das relações internacionais". Apesar de ainda se pautar em uma qualidade do realismo citado anteriormente, Waltz apresenta uma análise sistêmica da política internacional mais abrangente do que a abordada pelo

individualismo. Para Waltz, nesse sistema anárquico, os Estados que priorizem a segurança poderiam se beneficiar de duas estratégias, uma focada no mecanismo de ajuda, sendo feito através em uma ampliação do seu poder, e a outra voltada para o balanço do poder, que, ao invés de investir em sua própria força, estabelece alianças que contrabalancem com o poder de outros Estados. O comportamento dos Estados dentro dessa teoria seria reacionário, pelo que Waltz fora considerado um realista defensivo (SILVA; NUNES; SILVA, 2018).

Diversos críticos, até mesmo de outras vertentes de pensamento internacionalista, expressaram opiniões sobre o trabalho de Waltz. Inclusive a corrente neoliberal, que voltava a ganhar espaço nas discussões internacionalistas e se reestruturou com base na teoria de interdependência complexa, composta por Robert Keohane e Joseph Nye. Essa teoria buscava demonstrar que os Estados não eram pautados por ações individualistas, além de afirmar que poderia haver uma cooperação entre os Estados, construindo um regime internacional, mesmo com aqueles Estados mais racionais e egoístas.

Esse ideal foi o outro adversário do "terceiro debate das relações internacionais". É de comum acordo para muitos críticos da teoria internacionalista que uma das maiores falhas de Waltz foi a falta de atenção para a interação internacional, devido ao que diversos trabalhos construídos utilizando sua teoria como base também não priorizaram esse ponto, incapacitando a explicação das mudanças estruturais. Segundo Jatobá:

> Waltz considera a possibilidade de mudança de sistema quando o princípio ordenador é modificado. Porém, sendo a anarquia considerada uma constante, passou a considerar essencialmente as mudanças dentro do sistema, derivadas das distribuições das capacidades, o que corresponde as condições de unipolaridade, bipolaridade e multipolaridade. (SILVA, NUNES, SILVA, 2018, p. 11)

Essa consideração dominante e restrita que compõe o realismo não permite a apreciação de outros atores que interagem com o sistema internacional. Por isso, há a necessidade de uma compreensão mais holística dos estudos que discorrem sobre o campo da segurança, conciliando com a mesma abertura sociológica das Relações Internacionais. Essa demanda é datada em um cenário pós-Guerra Fria, em que outras esferas, como a economia, o social, o ambiental e o político, se mostraram mais proeminentes (SILVA; NUNES; SILVA, 2018).

Após conflito entre EUA e URSS, principalmente na primeira metade da década de 1980, o debate internacionalista foi marcado por críticas de teorias que construíram um terreno fértil para o amadurecimento de um debate mais amplo nessa área do conhecimento, e com ele também a diversificação do conceito antes estático de segurança. É então que o "quarto debate das relações internacionais" se desenrola, sendo a maior questão discutida a epistemologia da disciplina. A conjuntura se mostrou propícia para o desenvolvimento de estudos mais inclusivos, principalmente na área de segurança, em Relações Internacionais.

Com isso, em 1985, o Copenhagen Peace Research Institute (COPRI), comumente conhecido apenas como Escola de Copenhague, é fundado. O Instituto busca responder a nova demanda de questionamentos que surge na ciência das Relações Internacionais, com intuito de uma consideração de segurança e paz que ultrapasse a visão tradicionalista. Então, os teóricos participantes dessa escola assumem a missão de analisar e estruturar o conceito que se encaixe nos panoramas atuais, sem estabelecer algo restringente, mas passando a ser disseminado como algo intersubjetivo, que não se foca em um único objeto de referência, que nesse caso era representado pela figura do Estado, agora considerando a sociedade na qual a soberania e identidade estatal são baseadas (SILVA; NUNES; SILVA, 2018).

Barry Buzan é um nome de destaque dentro dessa nova exploração hermenêutica de segurança, notando a diversidade e multiplicidade do termo, que o mesmo já tinha proclamado como um "conceito essencialmente contestado" (*apud* AMARAL, 2008). Ele, juntamente com Ole Wæver e Jaap de Wilde, em 1998, sintetizam as ideias principais da Escola de Copenhague, que apresenta o conceito de segurança como uma condição defensiva, na qual, quando uma ameaça existencial é detectada, justifica-se o uso de todos os recursos para impedi-la. Aplicando essa lógica em um sistema internacional, o Estado, quando ameaçado, assume um papel mais central no poder, utilizando a força para neutralizar o problema.

Nessa proposta de Buzan, Wæver e Wilde (1998), há uma análise sobre a ameaça existencial, entendendo qual seu objeto de referência e em qual setor vai ser considerado: por exemplo, pode ser uma questão militar, ambiental, política ou econômica. E em cada esfera citada um diferente objeto de referência é atingido. Essa abertura não estagnou a significação da segurança, observando que uma ameaça pode

ser direcionada para um âmbito fora do militar, como anteriormente era considerado (SILVA; NUNES; SILVA, 2018).

Essa tese ficou conhecido como teoria de securitização, sendo o termo definido como "a possibilidade de um determinado tema passar a ser visto como ameaça à existência do Estado que desencadeará uma ação estatal emergencial, pontual e localizada fora da política comum e quotidiana de governo" (SILVA & PEREIRA, 2018, s/p). A teoria é considerada uma das principais contribuições do Copenhagen Peace Research Institute.

Segundo esses teóricos, que são considerados os líderes da Escola de Copenhague, em seus momentos iniciais, há três relevantes diferenças que podem ser vistas na evolução do assunto de segurança internacional. A primeira, já exposta anteriormente, é o fato da "chave de segurança" não ser unicamente ligada à defesa, mas considerar questões de cunho político e sociais. Já a segunda consideração surge com as tecnologias desenvolvidas na guerra, nesse caso as armas nucleares. Com impactos de grande magnitude é impossível entender o uso de tais armas apenas por meios militares. Com poder bélico tão potente, a estratégia seria evitar as guerras sem que a área militar fosse afetada. E, por fim, da natureza das questões de segurança não mais se limitarem à questão militar, agora considerando também outras óticas (SILVA & PEREIRA, 2018).

Sem aprofundar no que discorre a teoria em seus pormenores, e focando na percepção de que a Escola de Copenhague foi o ponto inicial para uma consideração mais abrangente seja com o objeto de referência ou mesmo com a natureza da questão de segurança, assim possibilitando que futuramente as questões como cibersegurança fizessem parte do estudo da disciplina. Possibilitando um maior entendimento da segurança internacional e dos Estados de como lidar com o impasse, quais medidas e providências poderiam ser tomadas. Apesar dessa teoria já estarem inserida no entendimento de Relações Internacionais, e garantir um olhar mais crítico para as situações de ameaças, algo tão atual quanto a tecnologia podendo ser um risco como é hoje, não foi previsto. Na realidade, apenas na última década, com os ataques cibernéticos mais frequentes e afetando mais do que os computadores domésticos, foi identificado um risco para a segurança do Estado.

Montando uma linearidade cronológica dos ataques cibernéticos que mais tiveram impacto no cenário internacional, o primeiro caso ocorreu em 2007, na Estônia. O ataque consiste em um grande número de solicitações em um pequeno espaço de

tempo, fazendo assim com que a rede sofra com queda ou congestionamento e impossibilitando o funcionamento do serviço. Esse tipo de ataque é chamado de Distribuído de Negação de Serviço (DDoS). Nesse dia, diversos serviços como redes de telefone, serviço de internet, cartão de crédito, banco, comércio e comunicação ficaram paralisados, o que, para um país com alto índice de conexão como a Estônia, é extremamente prejudicial e preocupante. Em 2008, o mesmo tipo de ataque cibernético ocorreu na Geórgia, tendo como alvo sites do governo. Para evitar maiores danos, todo o setor bancário foi desligado, sendo que os sistemas de cartões de crédito e telefonia móvel foram afetados (FONSECA, 2021).

Em 2010, aconteceu o caso que será analisado no presente trabalho como um marco relevante para segurança internacional, pois foi considerado por múltiplos estudiosos como um dos primeiros ataques de uma guerra cibernética. Um *worm* de computador, que é um programa que se autorreplica no sistema infectado, conhecido como *Stuxnet*, atingiu uma usina nuclear de enriquecimento de urânio no Irã, fazendo com que as centrífugas nucleares fossem danificadas no processo e impedindo o progresso do programa nuclear do país (FONSECA, 2021).

Ainda no ano de 2010, aconteceu a polêmica do *Wikileaks*, em que Julian Assange, um ativista político australiano, montou um polêmico portal na internet, responsável pela divulgação de documentos confidenciais que denunciavam diversas empresas e governos em questões de guerras, sistemas de corrupção e de espionagem. Os EUA foram um dos mais citados, principalmente com informações sobre a guerra travada contra o Afeganistão. Até o Brasil chegou a ser citado pela organização sem fins lucrativos, denunciando a espionagem da Agência Nacional de Segurança dos EUA a alguns líderes políticos da época.

Três anos depois, em 2013, uma situação parecida aconteceu, em que Edward Snowden, um ex-funcionário da Agência Nacional de Segurança dos EUA, revelou um sistema de monitoramento de dados do governo estadunidense, que espionava a comunicação até mesmo de países amigos e suas populações. O fato ficou conhecido como Caso Snowden e foi um grande destaque internacional da época (FONSECA, 2021).

Apesar deste ataque cibernético datar o ano de 2017, situações similares acontecem até os dias de hoje, principalmente com o maior consumo de redes sociais e aplicativos durante o período pandêmico. O *Wannacry* é caracterizado por um sequestro

de informações da vítima, exigindo resgates monetários virtuais para devolução desses dados. Atualmente, esse ataque *ransomware* também acontece para aplicação de golpes financeiros, em que redes sociais são tomadas e são mandadas mensagens para doação e/ou venda de produtos para os amigos da vítima, utilizando da imagem da pessoa para aplicar a fraude.

O grande problema desse tipo de ataque é o seu amplo alcance. No ano de 2017, diversos governos e empresas de setores importantes da sociedade, como banco, energia, saúde e telecomunicações, sofreram consequências do *Wannacry*. E, em 2020, ambientado no Brasil, foi registrado um aumento de cerca de 715% no número de casos de *ransomware*, atingindo até mesmo o Superior Tribunal de Justiça, paralisando por vários dias os serviços desse órgão público nacional (FONSECA, 2021).

Por fim, mais recentemente, dois casos de grande repercussão aconteceram no Brasil e nos EUA. Em território nacional, um vazamento de dados expôs o CPF de cerca de 223 milhões de cidadãos, além de outras informações de caráter confidencial. E, nas terras estadunidenses, um ataque cibernético parou a maior rede de gasoduto do país, algo tão extremo que aquele governo decretou situação de emergência em alguns locais. Todos esses casos citados tornam possível entender a complexidade do ciberespaço, por ser algo que atinge tanto atores estatais quanto não-estatais do sistema internacional, tornando-se uma grande preocupação devido os diferentes ataques que podem ser aplicados, a rapidez e o tamanho do impacto (FONSECA, 2021).

Para dar continuidade nessa discussão, será analisado um dos ataques supracitados, em que seu acontecimento foi um grande marco dentro da cibersegurança, pois pode ser observado de diversos ângulos dentro dessa nova tipologia de estudos. O acontecimento também chama atenção porque seus impactos não se restringem apenas ao ciberespaço, mas foram sentidos de forma física no alvo do ataque. Então, o ataque na usina nuclear do Irã, que ocorreu no ano de 2010, "abriu os olhos" para inúmeros problemas que um mundo mais integrado poderia ter.

CAPÍTULO 2. IRÃ

2.1. História

Para uma maior compreensão do acontecimento principal em que o presente trabalho se foca, será feita uma contextualização do cenário de uma forma geral, permitindo a avaliação perante diversos ângulos do ataque. Para isso, será discutido neste capítulo o Irã, abordando de uma forma breve sua história e explorando a questão do Programa Nuclear Iraniano, fator de grande relevância para essa conjuntura.

O país localizado no sudoeste da Ásia é, em grande parte, um planalto desértico, ladeado por altas cadeias de montanhas, no qual uma parcela significativa da população vive às margens (AFARY, MOSTOFI, AVARY, 2022). Devido a essa formação geográfica, com os desertos de temperaturas extremas, clima árido e um cerco montanhoso, o Irã se estabelece como uma fortaleza no território asiático, impossibilitando a chegada de inimigos por meios terrestres. Um fato benéfico para a nação, já que é o cruzamento entre Sul, Centro e Ocidente da Ásia, além de ter vastas reservas de combustíveis fósseis, como gás natural e petróleo. A maior cidade é Teerã, a capital, por onde passa toda a cultura e economia do país (AFARY, MOSTOFI, AVARY, 2022).

O território iraniano tem uma vasta história, de uma cultura e etnia excepcionalmente rica, com diversos impérios, conquistas e dinastias em seu rastro. Em face a essa densa cronologia, um recorte temporal será feito para expor os últimos cem anos, tempo esse em que o país teve maior contato com o Ocidente e que seria mais necessário nesta análise (AFARY, MOSTOFI, AVARY, 2022).

Antes mesmo de 1925, o país, que até este momento era conhecido como Pérsia, já passava por influência ocidentais, predominantemente da Grã-Bretanha e da Rússia, sendo que as duas se envolveram com o Irã por questões comerciais. Desde então, a predominância sob a nação foi crescendo chegando mesmo a ter uma Convenção Anglo-Russa, no ano de 1907, em que esses dois países receberam diferentes campos que ficariam responsável.

A presença da Europa foi cada vez mais sentida, principalmente nos sistemas de transporte que ligavam Europa e Oriente Médio, impactando na forma de vida dos iranianos, que antes era mais rural. O país chegou a prestar um serviço semelhante ao das semi-colônias da coroa britânica, suprindo a necessidade de determinados produtos e contando ainda com a presença Russa. Mas foi nesse ano que Reza Pahlavi chega ao poder. O xá (título dado aos soberanos iranianos) começou a dinastia que perdurou no poder até 1979, quando foi deposto através de uma revolução (AFARY, MOSTOFI, AVARY, 2022).

Pahlavi era a favor da modernização do seu governo, por meio de uma ocidentalização, e a independência do território, que em 1935, recebeu o nome na comunidade internacional de Irã, em resposta ao pedido do xá. O modelo seguido para a modernização proposto pelo xá foi muito parecido com o de Kemal Atatürk, que comandava as terras vizinhas da Turquia, em que um código civil de moldes europeus foi estabelecido, em que o sistema de educação se distanciava dos valores religiosos e aboliu o uso das vestimentas obrigatórias, tanto para mulheres quanto para os homens. A inserção das mulheres em diversos âmbitos, como governo, negócio, academia e esportes, também foi incentivada (MORETÃO, 2017).

Apesar das mudanças que foram realizadas, inclusive em seu sistema judiciário, a administração de Pahlavi tinha características ditatoriais, controlando a manifestação da política e da imprensa. Outro ponto que causou discórdia nesse governo e por diversas décadas que viriam a seguir foram as negociações das concessões de petróleo (AFARY, MOSTOFI, AVARY, 2022).

Diferentemente da Primeira Guerra Mundial, quando o país foi palco para disputas entre as forças britânicas, russas, turcas e alemãs, na Segunda Guerra Mundial, o Irã permaneceu neutro, negando pedidos para uso do território como base logística dos EUA. Essa atitude, combinada com o fato de que o Irã mantinha relações comerciais com a Alemanha nazista, como uma forma de fugir do controle das rotas terrestres pela Grã-Bretanha e a Rússia, levou esses países a deporem o xá, substituindo-o por seu filho Mohammad Reza Pahlavi, no ano de 1941, por meio de uma invasão.

Não tendo tanta autoridade quanto seu pai, com uma proximidade ainda maior com o Ocidente e com o saldo de uma guerra, que prejudicou sua economia e sua política, as medidas mais restritivas instauradas pelo xá anterior acabaram por se flexibilizar, permitindo uma liberdade tanto para imprensa, quanto para questões

políticas, quando então partidos políticos foram formados, entre eles o *National Will*, com uma orientação pró-britânica, e o pró-soviético *Tūdeh*.

Essa liberdade, juntamente com os novos partidos e as forças conservadoras, prestaram apoio ao Mohammad Mosaddegh, um político e advogado iraniano, que visava a diminuição da influência monárquica e do clérigo no país. Além desses valores, o político buscava a retomada do poder sob os recursos naturais iranianos. Inclusive, essa foi uma das suas primeiras medidas quando se tornou primeiro-ministro, em 1951, nacionalizando a indústria de petróleo, fato esse que incomodou a Grã-Bretanha, que detinha grande monopólio das concessões iranianas de petróleo. Ela chegou a apresentar embargos econômicos ao Irã e pedir consideração do caso pela Corte Internacional de Justiça, que tomou a decisão de não interferir (AFARY, MOSTOFI, AVARY, 2022).

Entretanto, essa decisão acabou não durando tanto, quando alguns anos depois de chegar ao cargo de primeiro-ministro, Mosaddegh foi deposto devido às fortes pressões internas alinhadas de um golpe financiado pela Agência Central de Inteligência dos EUA (CIA), apoiado pela Grã-Bretanha. Com isso, um consórcio com o Ocidente foi feito, estabelecido entre várias multinacionais da área, com destaque para a liderança de *British Petroleum*, com intuito de desenvolver as petrolíferas iranianas (AFARY, MOSTOFI, AVARY, 2022).

A partir desse golpe político, o xá contou da ajuda da Sāzmān-e Amniyyat va Ettelaʿāt-e Keshvār (SAVAK), uma organização de segurança e informações nacionais, sua polícia secreta, para exercer maior controle sobre a população. A opressão política, a questão econômica e as reformas feitas iniciaram o descontentamento dos iranianos, culminando na Revolução Iraniana, que aconteceu em 1979 (MORETÃO, 2017).

Esse movimento foi responsável por unir diversas áreas da sociedade, tanto religiosas, quanto políticas, como nacionalistas, esquerdistas e sindicalistas, em um único propósito, que era derrubar o governo de Mohammad Reza Pahlavi, que se mostrava corrupto e opressor. Com a saída do xá do poder, o primeiro-ministro ficou responsável por administrar um país que se mostrava em disputa política para decidir quem comandaria. Foi então que o aiatolá Rhollah Khomeini (um título dado a uma pessoa do alto escalão entre os mulçumanos xiitas, segundo o dicionário de língua portuguesa (PRIBERAM, 2022)) chamou um referendo para instaurar a República Islâmica (MORETÃO, 2017).

A nova república deixou de seguir o sistema político do secularismo, para adotar a lei de *Sharia*, que se refere ao direito islâmico (também sob consulta do dicionário (PRIBERAM, 2022)). Além dessa mudança, Khomeini implementou medidas que limitassem o contato do país com o Ocidente, o que estremeceu muito as relações principalmente com os EUA, que tiveram até mesmo suas embaixadas atacadas, e retomou atitudes que antecederam a dinastia de Reza Pahlavi, que incluía determinações realmente limitantes para as mulheres, proibindo-as de participar em espaços que anteriormente eram incentivadas a participar, como o cenário político. Apesar dessa coibição, muitas mulheres já trabalhavam com seus garantidos e se recusaram a acatar essa medida, decisão que foi reforçada pela guerra que aconteceria no ano seguinte, quando o mercado de trabalho viu a necessidade de manter as trabalhadoras. Além dessas restrições morais, aconteceu a censura a todos aqueles que não concordassem com o governo (MORETÃO, 2017).

Em 1980, o Irã entra em uma guerra de oito anos com o Iraque, iniciada por questões de disputas territoriais, em que o presidente iraquiano Saddam Hussein, identificando uma maior vulnerabilidade das forças armadas iranianas, devido à deposição do xá, tentou invadir uma das mais importante províncias produtoras de petróleo do país. Apesar de enfraquecida, a armada iraniana deteve a ocupação. A guerra foi custosa para a população de ambos os países, sofrendo com troca de bombardeios em áreas residenciais e industriais e as mortes decorrentes de uma disputa (AFARY, MOSTOFI, AVARY, 2022).

Outro ponto de preocupação internacional era o Golfo Pérsico, mar raso do Oceano Índico, localizado entre a Península Árabe e o sudoeste do Irã, ponto de valorização em razão ao seus vastos recursos petrolíferos (EVANS, 2021), que tiveram suas atividades reduzidas em face à guerra Irã-Iraque, chegando a ter navios escoltados pelos navios de guerras estadunidenses ancorados na área. O conflito acabou em 1988, após o Irã aceitar uma resolução das Nações Unidas que decretava que ambos os países deveriam voltar às suas respectivas fronteiras e um cessar-fogo. O Irã resultante da guerra era permeado pela disputa entre dois blocos principais sobre a economia, a política tanto nacional quanto internacional e a parte social (AFARY, MOSTOFI, AVARY, 2022).

Com o óbito de Khomeini, em 1989, o povo iraniano começa a ir às urnas para decidir os próximos presidentes do país. Os governos dos anos que se seguem são

marcados por políticos mais moderados. Ali Akbar Hashemi Rafsanjani, o presidente eleito após o falecimento do antigo líder, visava a reconstrução da economia após o período de guerra, para o que suas políticas defendiam uma liberação econômica, aproveitando de uma reconciliação com países do Ocidente para encorajar investimentos estrangeiros no país, e a privatização de suas indústrias.

A partir da abertura dada por esse governo, cada vez medidas mais progressistas eram decretadas e de defesa dos direitos, tanto das mulheres, dos direitos humanos, quanto de uma sociedade civil mais democrática. As novas formas de comunicação possibilitaram à população mais contato com informações e com o mundo ocidental. Mas essas mudanças não vieram sem o antagonismo dos partidos conservadores do país, que provocou copiosos protestos durante os anos. E, apenas em 2005, os conservadores conseguem voltar ao poder com Mahmoud Ahmadinejad, que administra por dois mandatos e que acaba sendo muito prejudicado pelo cenário econômico e recebe duras críticas, principalmente por sua postura diante do programa nuclear iraniano (AFARY, MOSTOFI, AVARY, 2022).

As dificuldades econômicas perduraram até as eleições de 2013, quando Hassan Rouhani assumiu o poder, garantindo um crescimento econômico resultante da reinserção do Irã na economia global, quando assinou um acordo limitante de seu programa nuclear. Entretanto, no seu segundo mandato, a questão econômica voltou a ser um problema, quando parte desse benefício da reintegração que refletia no Produto Interno Bruto lentamente não beneficiava o resto da população. E essa foi a conjuntura em que as votações presidenciais em 2021, agravada com os impactos do COVID-19, aconteceram, registrando o menor número de votantes desde a instauração da República Islâmica (AFARY, MOSTOFI, AVARY, 2022).

2.2. Economia

Segundo *World Bank*, a economia iraniana é caracterizada por atender os setores de combustíveis fósseis, também chamado de hidrocarbonetos, da agricultura e dos serviços, com o Estado participando na manufatura e nos serviços financeiros. Na primeira categoria, o Irã ganha posições de destaque mundialmente por suas reservas, ocupando o segundo lugar na questão de gás natural, e quarto na de petróleo bruto. Ainda que sua economia seja diversificada, tanto as atividades com fins econômicos

quanto as receitas governamentais, mostram dependência do petróleo (WORLD BANK, 2022).

A economia iraniana, mesmo que com notáveis recursos, como os combustíveis fósseis, acaba sendo afetada pelo isolamento para com a comunidade internacional. Isso resultou em problemas para o mercado interno, no curto e no longo prazo, dificultando o crescimento e o acesso às tecnologias de ponta, prejudicando com isso o investimento estrangeiro no Irã. A reclusão iraniana é efeito de dois fato:, o medo interno dos políticos das vertentes mais conservadoras dos pós-imperialistas no país, e as sanções impostas pelos Estados Unidos, com a alegação que o Irã apoiava o terrorismo internacional. Sendo determinada pelas Leis de Sanções do Irã e da Líbia, acordadas em 1996. Segundo uma matéria da Folha de S.Paulo do ano do ocorrido, esse projeto de lei do governo estadunidense de Bill Clinton tem como objetivo punir empresas de outros países que invistam ou exportem para Líbia ou Irã (SILVA, 1996).

Considerando que as empresas estadunidenses seguem o mesmo tipo de restrição. O alvo principal das sanções é o campo petrolífero, mas também prejudica a área de tecnologia e até mesmo limita a importação de produtos iranianos diversos. Apesar dos políticos do Irã com ideias reformistas apresentarem projetos para uma abertura ao investimento estrangeiro, o retorno apresentado foi limitado (AFARY, MOSTOFI, AVARY, 2022).

Contudo, em 2018, o EUA, que tinha firmado acordo nuclear com o Irã, com o intuito de progressivamente ter mais acesso com o relaxamento das sanções, resolveu sair do tratado e revisar as medidas punitivas. Em fevereiro de 2022, o atual presidente estadunidense, Joe Biden, está em negociação para a volta para o tratado quebrado pelo ex-presidente Donald Trump, além de restaurar as isenções de sanções contra o Irã, a fim que isso possibilite projetos de cooperação nuclear internacional (R7, 2022).

Desde a Revolução Islâmica, em 1979, os objetivos de longo prazo do país envolvem a independência econômica, possibilitando aos cidadãos empregos e um padrão de vida confortável. Porém, esse plano econômico passou por alguns e empecilhos no final do século XX e começo do séculos XXI. Isso porque a população do Irã teve um aumento demográfico significativo, uma queda na produção agrícola, sendo que o país era rural e agrário, e uma migração para as maiores cidades iranianas com os problemas econômicos. Ainda que o Irã mantenha as taxas de alfabetização e

expectativa de vida em alta, o mesmo acontece com os índices negativos, como o de desemprego e inflação.

Como citado anteriormente, as atividades econômicas iranianas estão centradas na indústria de combustíveis fósseis, o que restringe as oportunidades de trabalho para a população mais jovem e com maior nível de escolaridade. Na tentativa de melhorar as condições da economia, o governo investiu na infraestrutura voltada para a comunicação, transporte, com o foco desses dois primeiros serem integrados em seus Estados fronteiriços, e na fabricação e produção energética, considerando a energia nuclear (AFARY, MOSTOFI, AVARY, 2022).

No campo petrolífero, o Irã é responsável pela extração e o processamento do combustível, e, através de sua empresa estatal, a *National Iranian Oil Company* (NIOC), o produto é exportado e utilizado para consumo interno. As exportações são feitas por meio de um gasoduto para uma ilha no Golfo Pérsico, onde um navio-tanque escoa a produção para os compradores por todo o mundo. Das refinadoras saem o combustível para aeronaves, para o aquecimento das casas e para a indústria de transporte. O país também possui uma indústria petroquímica, que produz amônia, fosfato, enxofre, gás líquido e óleo leve.

Na questão do gás natural, as reservas iranianas constituem um décimo do todo mundial, a distribuição é realizada por dois gasodutos estatais, considerados os maiores do Oriente Médio, abastecendo a Rússia, Europa Oriental, Paquistão, Turquia e Índia. Outra indústria notável são as mineradoras de carvão, e, apesar de terem uma exploração relativamente mais recente, de lá saem chumbo, zinco, urânio, ouro, refratária, giz, cal, gesso, ocre e caulim (AFARY, MOSTOFI, AVARY, 2022).

2.3. Relações Exteriores

Dentro do Oriente Médio, o Irã é uma das nações mais importantes. A política de projeção de poder, exercida pelo Irã nas últimas décadas, colocou o país em holofote na comunidade internacional. Aliado ao fato que o país já mostrou um avanço tecnológico, sendo este de seu próprio desenvolvimento e produção, contando com, em 2009, o lançamento de satélites, foguetes e mísseis balísticos, repercutindo em sua política externa, com foco na segurança regional e internacional. Quando considerado as relações exteriores, necessita-se lembrar que, no Irã, a política e a religião estão

entrelaçadas, assim influindo na maneira como é feita sua inserção no meio internacional e na política externa. Os iranianos são, assim como o povo árabe em geral, islâmicos, porém de uma vertente diferente, seguindo o xiismo. Compreendendo que essa vertente decreta certas restrições na atuação regional do país (FILHO, 2009).

Essa influência é percebida pelo distanciamento imposto ao mundo ocidental, causado pelas ideologias dos políticos iranianos. Analisando a história do Irã nos últimos cem anos, é notável a influência britânica, russa e estadunidense no território, tanto em relações benéficas quanto em situações em que os países mostravam certa controvérsia entre si. Durante o mandato de Rafsanjani, foi tentado estabelecer uma restauração do relacionamento econômico entre países ocidentais e o Irã, mas, mesmo com essa intenção, o Estado não integrou as forças montadas pela ONU para movimentos contra o Kuwait e se opôs à pacificação israelense-palestina, sendo que nem mesmo reconhece o Estado de Israel desde sua revolução em 1979.

Essas e outras ações controversas iranianas foram responsáveis por dificuldades, tendo até mesmo relações diplomáticas e comerciais cortadas. Como a Alemanha, que em 1997, após investigações, as autoridades constataram que o ataque ocorrido em 1992 no país, onde quatro pessoas foram mortas, sendo uma delas do Partido Democrático do Curdistão Iraniano, foi indiretamente ligado ao presidente e o aiatolá iranianos da época (AFARY, MOSTOFI, AVARY, 2022).

Com a revolução de 1979, o Irã assumiu uma frente mais desafiadora, principalmente aos EUA, almejando uma inserção nos cenários internacionais e regionais de forma mais independente, seguindo os princípios fundamentalistas que a revolução assumiu. Internamente, como citado anteriormente, a sociedade foi fortemente reprimida. No âmbito internacional, nos primeiros dias de regime, uma invasão à embaixada estadunidense, localizada no Teerã, ocorreu, fazendo dos diplomatas e funcionários reféns do governo, declarando dessa forma um desafio aos EUA. A guerra iraniana contra Iraque marcou a década de 1980, em que a política externa teve que assumir um caráter mais agressivo e radical, visto que esse conflito contra um aliado dos EUA foi um desastre custoso não só para economia do país, mas na qual mais de 300 mil pessoas perderam suas vidas (FILHO, 2009).

A tranquilidade que a década de 1990 passou, voltando-se para os assuntos internos, acabou quando, em 2005, Mahmoud Ahmadinejad assumiu a presidência, retomando uma política mais marcante contra as percepções ocidentais difundidas pelos

EUA. Reativando a polêmica política nuclear iraniana e novamente tendo um tom mais desafiador perante as provocações estadunidenses.

O Irã é considerado nessa época como um oponente para a política externa dos Estados Unidos, aparentando uma capacidade tanto tecnológica quanto militar em crescimento. Esse aspecto, mesmo que mais brando, em favor de ampliar a sua política para o Oriente Médio, mantinha o presidente Barack Obama observando o Irã. O que em parte também ocorria devido a uma tensão entre Israel, sendo temido um ataque pelos mesmos à instalações nucleares iranianas, que levaria a uma situação de apreensão (FILHO, 2009). Mais tarde, um ciberataque ocorreria realmente a uma usina nuclear no Irã, contudo o autor considerado não foi Israel, mas sim os próprios EUA.

A situação com o país norte-americano até os dias atuais é complicada, sendo que, durante a última década, um acordo entre os dois Estados foi assinado, visando melhorar o campo político e econômico com o Ocidente, já que a tensão foi a responsável por uma perda econômica significativa pelas sanções aplicadas contra o Irã. E, ainda neste ano, sob o comando de Joe Biden, o atual presidente dos EUA, o tratado está sendo renegociado, após a abrupta saída estadunidense e as novas sanções decretadas durante a presidência de Donald Trump.

2.4. Programa Nuclear

A história do Irã com a energia nuclear começa com uma iniciativa dos EUA. Em 1953, o presidente estadunidense Dwight Eisenhower levanta em discurso a preocupação do uso da tecnologia nuclear para propósitos bélicos, diante da Assembleia Geral da ONU. Para reduzir o risco de mais países usarem essa tecnologia para esse fim, Eisenhower propôs algumas medidas, na intenção em transformar esse conhecimento em algo benéfico para a humanidade.

Uma das sugestões foi a criação de uma agência de energia atômica, comandada pela ONU, responsável pelos materiais nucleares, garantindo que seu uso fosse sempre voltado para um propósito pacífico, como a medicina ou mesmo o fornecimento de eletricidade para regiões sem acesso à mesma. Essa foi a premissa para criação da Agência Internacional de Energia Atômica (IAEA). A outra iniciativa foi nomeada como "Átomos para a Paz", em que o conhecimento e tecnologia para o desenvolvimento da energia atômica pacífico seria disponibilizado pelos EUA.

No ano de 1957, Eisenhower e o xá iraniano, Mohammad Reza Pahlevi, assinam um acordo para o uso pacífico da energia atômica, através do projeto "Átomos para a Paz". Apenas dez anos depois, um reator nuclear de 5 megawatts, com fins de pesquisa, chegaria ao Irã, juntamente com uma quantidade limitada de urânio altamente enriquecido. Para evitar o uso para o desenvolvimento bélico, foi criado o Tratado de Não Proliferação Nuclear (TNP), em 1970, tendo em vista que uma guerra nuclear causaria sérios danos para toda a humanidade, afirmando que os países signatários, usassem os recursos para pesquisas e conhecimento, seguindo as diretrizes da IAEA.

Apesar do Irã ser um dos signatários do tratado para a não-criação de armas nucleares, o xá não dispensou totalmente esse pensamento, o que declara Akbar Etemad, o presidente da Organização Iraniana de Energia Atômica (AEOI) da época, em entrevista para a BBC em 2013 (G1, 2021).

Para que esse programa funcionasse no país, foi investido na educação para formação de especialistas qualificados, com acordos entre EUA e Irã, tendo até mesmo um com o Instituto de Tecnologia de Massachusetts (MIT), que treinaria os engenheiros nucleares iranianos. A primeira grande instalação nuclear iraniana construída foi o Centro de Pesquisa Nuclear do Teerã (TNRC), em 1967, com administração da Organização Iraniana de Energia Atômica e localizado na Universidade de Teerã. Essa instalação continha o reator dado pelos EUA, produzindo cerca de 600 gramas de plutônio por ano (SAHIMI, 2003).

O plano de Pahlevi era, nos próximos 20 anos, a construção de 23 instalações de energia atômica com capacidade de gerar cerca de 23 mil megawatts de energia, além de desenvolver todo o ciclo de produção de combustível nuclear no país (G1, 2021). Para concluir esse projeto, o xá contratou a Kraftwerk Union, da Alemanha Ocidental, por quantia bilionária, para construção de dois reatores nucleares Siemens de 1200 megawatts, na província de Bushehr. Outro Centro de Tecnologia Nuclear foi fundado em Esfahan, com assistência da França, para o treinamento da equipe que trabalharia em Bushehr, atuando com quatro reatores nucleares de pequena dimensão, fornecidos pela China (SAHIMI, 2003).

Contudo, todo o programa foi desativado com a Revolução Islâmica de 1979, sendo que os reatores Bushehr-1 e Bushehr-2 já se encontravam parcialmente construídos (SAHIMI, 2003). Isso porque a opinião popular sobre o projeto era extremamente antinuclear nos primeiros anos. Essa opinião não permaneceu por muito

tempo, pois, logo que foi percebida a magnitude da tecnologia nuclear, o governo tenta trazer de volta todos os especialistas que deixaram o Irã frente à reação inicial da revolução iraniana, para que pudesse montar o próprio programa atômico secreto (G1, 2021).

Por vários anos, o governo iraniano tentou reativar o programa para terminar o projeto da Bushehr através de parcerias já existentes e novas propostas, mas os EUA acabaram aplicando pressão contra esses países, frustrando assim os planos do Irã. Após muita negociação, a Rússia assumiu um acordo para terminar o primeiro projeto e construir mais dois reatores. O que foi muito mal visto pelos EUA e por Israel, temerosos de que, com essa tecnologia e conhecimento, o país iraniano passasse a fabricar armas nucleares (SAHIMI, 2003).

Essa desconfiança do programa nuclear iraniano não diminuiu nem mesmo quando, em 1997, entrou em vigor a Convenção sobre as Armas Químicas (CWC), o primeiro acordo multilateral do mundo sobre desarmamento que propõe a eliminação de todo tipo de armas de destruição em massa com um prazo definido. Para fiscalizar o cumprimento desse mandato, nasceu o regime internacional de desarmamento de armas químicas chefiado pela Organização para a Proibição de Armas Químicas (OPAQ). A OPAQ confere o desenvolvimento, produção, armazenamento, transferência e uso de armas químicas com intuito de evitar a guerra química. O Irã é signatário desde a criação da Convenção sobre as Armas Químicas, concordando com os termos segundo os quais relatórios deveriam ser enviados anualmente para a Secretaria Técnica do órgão responsável (OPAQ, 2022).

Essa pressuposição de que o Irã tinha intenção de construção de armas nucleares ganha força quando, em 2003, o então presidente iraniano, Mohammad Khatami, anunciou publicamente a instalação de Natanz, que até então permanecia em sigilo, e aproveitou para convidar a Agência Internacional de Energia Atômica para fazer uma inspeção no local. No mesmo mês que o anúncio foi feito, o chefe da Agência Internacional de Energia Atômica, Dr. Mohammad El Baradei, acompanhado de um time de inspetores e especialistas, visitou a instalação nuclear mais de uma vez. Dois relatórios foram emitidos a partir dessas inspeções, um preliminar em junho e um de acompanhamento em agosto.

O país recebeu então um ultimato da agência para que revelasse toda a atividade do seu programa nuclear até uma data no mesmo ano. Destacando que, como

participante do Tratado de Não Proliferação Nuclear, o Irã precisaria avisar a Agência Internacional de Energia Atômica, 180 dias antes de introduzir qualquer material nuclear, o que ocorre, de modo que o governo iraniano não violou os acordos estabelecidos (SAHIMI, 2003). No site da Agência Internacional de Energia Atômica, é possível encontrar todos os relatórios publicados desde 2003 até os dias atuais, constando a situação das instalações nucleares (IAEA, 2022).

É nesse cenário que o Irã sofre acusações, principalmente dos EUA, de que seu programa teria a intenção de enriquecer urânio com fins militares. Isso porque, para gerar energia elétrica, o urânio precisa ser enriquecido apenas em percentuais que variam de 3% a 5%, e o programa iraniano passou a enriquecer a níveis de 20%, ainda dentro do limite para uso civil, não sendo suficiente para a fabricação de armas nucleares, que precisam de percentuais de 90%. Mas gerando desconfiança, pois o país pode chegar nos níveis necessários para o uso bélico (CAETANO, 2014).

Diante desse fato, o Conselho de Segurança das Nações Unidas, do qual as cadeiras de membros permanentes são preenchidas pelos Estados que dispõem da maior parte do poderio bélico nuclear, adotou medidas para impedir o desenvolvimento do programa nuclear do Irã. Sendo a primeira feita através da Resolução de 1696, em 2006, que requisitava ao governo iraniano acatar as determinações da Agência Internacional de Energia Atômica, comprovando os fins pacíficos do programa. Afirmando também que seria necessário uma paralisação temporária do enriquecimento de urânio (CAETANO, 2014, p. 10).

Quando o Irã não cumpriu essa resolução, o Conselho de Segurança das Nações Unidas passou a instituir sanções na tentativa de atrasar o projeto nuclear iraniano. Devido ao não-obedecimento iraniano, quatro rodadas de sanções foram definidas nos anos que se seguiram, conforme o avanço no programa nuclear iraniano. Cada rodada apresentava medidas mais rigorosas que as anteriores.

A chamada Primeira Rodada, referente à Resolução 1737, de 2006, bloqueou a exportação de materiais e equipamentos nucleares, além de congelar financeiramente as pessoas ou organizações com algum envolvimento das atividades nucleares iranianas (UNSC *apud* CAETANO, 2014, p. 10).

Assim como a anterior, a Segunda Rodada, da Resolução 1747, se voltou para prejudicar a exportação e o congelamento financeiro. Então, em 2007, foram afetadas as exportações de armas para o Irã e somou nos grupos já prejudicados mais 28 grupos,

seja de empresas ou indivíduos, dessa vez também considerando as atividades que envolviam a construção de mísseis balísticos (UNSC *apud* CAETANO, 2014, p. 10).

A Terceira Rodada, lançada pela Resolução 1803, em 2008, teve como alvo autoridades iranianas, sancionando a proibição de viagens internacionais para cinco autoridades do Irã, e novamente utilizou de congelamento financeiro no exterior, atingindo agora 13 companhias e mais 13 autoridades. A medida anterior já tinha vetado a questão bélica, agora proibindo até mesmo itens considerados com "uso duplo", ou seja, usados tanto para fins pacíficos quanto para militares (UNSC *apud* CAETANO, 2014, p. 10).

No 31º aniversário da Revolução Islâmica, o presidente Mahmud Ahmadinejad afirmou que o Irã tinha capacidade para enriquecer o urânio em até 80%, mas o interesse do país nesse momento era produzir ao nível civil de 20% (G1, 2010). Contrapondo-se à resolução do Conselho de Segurança das Nações Unidas, que ordenava que o país suspendesse o enriquecimento de urânio e outras atividades envolvidas com materiais nucleares até que o programa nuclear fosse analisado e de fato provasse suas intenções pacíficas. Porém, o Irã se recusa a parar seu enriquecimento, já que está dentro do que foi previsto no Tratado de Não-Proliferação Nuclear, produzindo a quantidade necessária para o uso em energia civil (BBC, 2010).

E, por fim, a última sanção, da Resolução 1929, datada de 2010, colocou a Quarta Rodada em vigor, ainda focando nos armamentos, proibindo o comércio de armamentos considerados pesados, como helicópteros de ataque, mísseis e navios de guerra. Mais 40 empresas foram prejudicadas com o congelamento de seus ativos financeiros. E, para garantir que as cargas não contivessem itens que foram sancionados, foi solicitado que um sistema de inspeção de cargas fosse criado (UNSC *apud* CAETANO, 2014, p. 11).

Lembrando que, enquanto essas rodadas eram feitas, o Irã sofria de sanções de forma isolada, como os EUA, que, segundo o Departamento de Tesouro dos EUA (USDT), desde 1979, decretava ordens executivas que proibiam e bloqueavam certas atividades com o país. Um exemplo é a Ordem Executiva 12.957, que proibia certas transições relacionadas com o desenvolvimento de recursos petrolíferos iranianos, em uma tradução livre do título, que entrou em vigência em 1995 (USDT, 2022).

Tantas restrições contra o Irã não só afetaram o programa nuclear, mas abalaram de forma notável a economia iraniana, já que não só os alvos das sanções sofreram

restrições no mercado internacional. O petróleo, produto de maior exportação do país, chegando a ser 80% de suas exportações nesse período, não era bem recebido no mercado internacional. Fato que, apesar dos esforços para não afetar a população, abalou a economia iraniana (CAETANO, 2014). Mas, ainda sim, em 2011, o país anunciou o funcionamento da usina nuclear de Bushehr.

Em 2013, os EUA e o Irã entraram em contato e uma negociação foi iniciada. Anos mais tarde, em 2015, o Irã e as grandes potências mundiais assinaram um tratado nuclear, em Viena, na Áustria. O acordo visava limitar o programa nuclear iraniano, garantindo que esse não seja utilizado para fins bélicos, mas apenas para fins pacíficos. Em contrapartida, as sanções internacionais definidas pelo Conselho de Segurança das Nações Unidas seriam retiradas. Os chefes diplomáticos do grupo P5+1 (integrados pelos membros permanentes Estados Unidos, China, França, Reino Unidos e Rússia, contando também com a Alemanha) se reuniram junto ao Irã, no palácio de Coburg, na capital austríaca, por um período de 17 dias, para essa decisão. A decisão foi muito comemorada pelo então presidente estadunidense Barack Obama e por Hassan Rohani, do governo iraniano (G1, 2015).

O acordo, que foi nomeado de Plano de Ação Conjunto Global (JCPOA), trazia uma série de ações iranianas, em que a Agência Internacional de Energia Atômica ficaria responsável pela fiscalização e o relatório constatando o cumprimento ou não das medidas e em troca os congelamentos e sanções aplicadas, que afetaram até mesmo o campo petrolífero. Até o ano de 2018, todos os países seguiram suas partes no contrato; contudo, nesse mesmo ano, Donald Trump, o presidente estadunidense da época, anunciou a saída unilateral do acordo, assim tendo liberdade para, no período de dois anos, encerrar todas as isenções das sanções de cooperação com o projeto nuclear. Como resposta a esse comportamento, mesmo sem rescindir o contrato, passou a violar alguns pontos do trato, alegando que o intuito da assinatura foi o alívio das sanções que assolavam o país. A condição para voltar a cumprir o compromisso era a volta das isenções (ARMS CONTROL ASSOCIATION, 2022).

No ano de 2020, o governo Trump, através do então secretário estadunidense, Michael Pompeo, enviou uma carta ao Secretário-Geral da ONU, Antonio Guterres, e para o embaixador da Indonésia na ONU, que geriu o Conselho de Segurança desse órgão, citando uma resolução presente no texto do acordo que permitia que os países signatários voltassem com sanções ao Irã. Contudo, o pedido foi rejeitado tanto por

Antonio Guterres quanto pelos demais Estados assinantes, argumentando ainda que, como os EUA se retiraram do acordo, não poderiam mais reivindicar resoluções constatadas no mesmo para restabelecer as sanções internacionais ao Irã. Em dezembro do mesmo ano, o Irã emite uma nova legislação, contendo a Nova Lei Nuclear do Irã, que obriga a Organização de Energia Atômica do Irã a ter um aumento considerável das atividades nucleares nos próximos meses (ARMS CONTROL ASSOCIATION, 2022).

O governo de Joe Biden, presidente eleito em 2021 nos EUA, retirou o pedido da administração anterior formalmente (ARMS CONTROL ASSOCIATION, 2022). E, nesse ano, voltou a renegociar o acordo, e, em fevereiro, o país reimplantou as isenções das sanções. Considerando que o Irã afirma, que os inspetores da Agência Internacional de Energia Atômica só poderão analisar as instalações nucleares depois da adesão dos EUA no acordo (CNN, 2021).

2.5. Instalações Nucleares

Para o Ciclo de Combustível Nuclear é necessário algumas instalações com diferentes atividades. Atualmente, o Irã conta com três reatores, sendo que apenas um deles é usado em uma usina nuclear. O ciclo inicia em Sagand com a mineração do urânio, que é enviado para os locais de enriquecimento de urânio em Natanz ou Ghom, depois enviados para a Usina Nuclear de Bushehr, para serem usados em seu núcleo. Os reatores em Teerã e Arak tem finalidade de estudo, assim como o centro em Isfahan (INB, 2022).

A Usina de Bushehr começou a funcionar em agosto de 2011, com supervisão interna da Organização de Energia Atômica do Irã, e, devido ao Plano de Ação Conjunto Global, de 2015, avaliado também pela Agência Internacional de Energia Atômica, garantindo a conformidade tanto na usina em si, quanto nos locais de enriquecimento de urânio, assegurando que os percentuais do urânio enriquecido não passem do necessário para uso civil. Assim, respeitando o acordo estabelecido, para o uso dos materiais nucleares para fins pacíficos.

CAPÍTULO 3. ATAQUE AO PROGRAMA NUCLEAR DO IRÃ

Desde a Revolução Islâmica em 1979, o Irã assumiu uma postura forte diante das intervenções externas. Mesmo para aqueles países com que antes mantinha boas relações, o governo agora expressava de forma aberta características de repúdio, principalmente aos países do Ocidente, como o EUA, mas também afetando nações próximas, como Israel. Essa postura, juntamente com a falta de informações sobre o programa nuclear iraniano, causaram a desconfiança dos EUA e da União Europeia para com as verdadeiras intenções do Irã com o desenvolvimento de energia nuclear, tendo em vista que em seu território são registradas notáveis reservas petrolíferas (LOPES, OLIVEIRA, 2014, p. 58).

Foi durante o governo de G.W. Bush nos EUA que uma medida foi tomada considerando que o desenvolvimento do programa nuclear iraniano era algo urgente. As perspectivas de invasão do território iraniano ou deixar que o país progredisse com a suposta construção de bombas nucleares não eram favoráveis para o então presidente estadunidense. Sanger afirma que uma terceira alternativa foi proposta, a intervenção de forma cibernética, atacando o Irã (*apud* LOPES & OLIVEIRA, 2014, p. 59). Esse tipo de abordagem era inédito e tinha o objetivo de atrasar o programa nuclear iraniano. Para isso, os EUA iniciaram um programa secreto:

> [...] o *Olympic Games* [...], o qual possui dois objetivos políticos: sabotar, ainda que temporariamente, o programa nuclear iraniano e convencer Israel de que há uma maneira mais eficaz e menos custosa de lidar com o problema nuclear iraniano do que lançar ataques aéreos [...]. Em tese, o projeto se mostrou eficaz, mas, na prática, não havia garantias de que *de facto* funcionasse. Mesmo assim, Washington e Tel Aviv consideraram essa a melhor opção. (SANGER *apud* LOPES & OLIVEIRA, 2014, p. 60)

O convencimento de Israel para essa alternativa foi de grande importância, pois o desenvolvimento e aperfeiçoamento do *software* que seria usado no ataque ao Irã, que foi elaborado a partir das fraquezas identificadas pelos agentes israelenses no processo computadorizado da instalação nuclear, e a forma como o mesmo seria introduzido ao alvo seriam de responsabilidade dos israelenses (LOPES & OLIVEIRA, 2014, p. 60).

A jornalista investigativa estadunidense, Kim Zetter, que publicou numerosos artigos sobre cibersegurança e segurança nacional estadunidense, descreve em *Countdown to zero day* o incidente. Segundo seu relato, em janeiro de 2010, os oficiais da Agência Internacional de Energia Atômica, responsáveis pelo monitoramento do programa nuclear iraniano na instalação de Natanz, notaram acontecimentos incomuns. Em um curto período de tempo, uma grande quantidade de centrífugas usadas no enriquecimento de urânio foi substituída e as mesmas estavam rodando em alta velocidade. O local que abrigava cerca de 8.700 centrífugas em 2009, onde cerca de anualmente 10% delas eram trocadas, apresentou um aumento anormal nesse número em um espaço de tempo menor que o usual (ZETTER, 2014, p. 10).

Para melhor compreensão da importância desse equipamento e o papel dentro do processo de energia atômica, uma breve explicação da utilidade das centrífugas de enriquecimento de urânio, com base nas informações disponíveis pela Indústrias Nucleares do Brasil (INB) sobre o assunto, parece importante. O átomo de urânio obtido na natureza possui diferentes números de variações, nomeadas de isótopos. Nesse átomo, a variante U-238 apresenta uma concentração de 99,27% contra o U-235, isótopo usado para produção nuclear, desde energia até armas de destruição em massa, com concentração de apenas 0,72%. Para gerar energia, é preciso aumentar a concentração de U-235, ou seja, enriquecer o urânio para níveis de até 5%. Para obter esse elemento, é feita uma separação dos dois isótopos, que se encontram em estado gasoso, através da força centrípeta. O gás girado em altas velocidades separa os átomos de diferentes pesos, enriquecendo assim o urânio. Permitindo que o átomo de urânio libere calor e gere energia posteriormente (INB, 2022). Danificar esse equipamento pararia uma usina nuclear, visto que, sem o elemento correto, não há como gerar energia.

Nesse momento, nem a Agência Internacional de Energia Atômica ou os operadores de Natanz sabiam o que estava levando os equipamentos a falhar. Os números de centrífugas quebradas variam entre 900 e 2.000 substituições. E, apesar das claras falhas ocorrendo, as máquinas de supervisão dos processos no enriquecimento não apresentavam nenhum erro aparente. O que estava ocorrendo na instalação iraniana só foi descoberto depois de quase um ano do incidente, após a verificação de um computador de Natanz que apresentava um defeito, que aparentava ser uma questão simples, mas que levou vários especialistas em segurança de computador a fazerem uma

análise detalhada do vírus, para realmente descobrir o que estava então acontecendo (ZETTER, 2014).

3.1. Stuxnet

Em julho de 2010, Sergey Ulasen, chefe da divisão de antivírus de uma pequena empresa de segurança de computadores, sediada na cidade de Minsk, na Bielorússia, chamada Virus-BlockAda, juntamente com seu colega de trabalho, Oleg Kupreev, descobriram um avançado vírus em uma das máquinas do Irã, que foi analisada remotamente pelos técnicos da empresa, após o computador apresentar um problema em que se reiniciava em *looping*. O que parecia algo simples, como uma incompatibilidade de sistema, se mostrou muito mais complexo, quando mais computadores apresentavam os mesmos arquivos suspeitos, em que se localizava o código. Após uma análise de código, que durou dias com vários trabalhadores dessa empresa de antivírus, é que foi entendido a estrutura de funcionamento desse intrincado *malware* (ZETTER, 2014).

Segundo a empresa Avast Software, uma das maiores empresas de antivírus atuais, a primeira diferença que esse código apresenta é que ele se caracteriza como um *worm* de computador, diferenciando de um vírus. Apesar de ambos causarem danos às máquinas infectadas e apresentarem uma rápida replicação, sua principal diferença está na forma como iniciam esse processo. Enquanto um vírus precisa que o usuário daquele sistema "desperte" através de alguma ação essa contaminação que está no arquivo hospedeiro, o *worm* não necessita dessa assistência, sendo um programa autossuficiente, que se replica e propaga de forma automática e muito mais rápida que o vírus (LATTO, 2020).

O *worm* de computador Stuxnet, nomeação que recebeu após uma combinação dos títulos de arquivos que apareciam constantemente no código, ".stub" e "MrxNet.sys" (ZETTER, 2011), é um código malicioso de computador, que foi programado para atacar o Sistema de Supervisão e Aquisição de Dados (SCADA) da empresa Siemens. Esse sistema é usado para gerenciar o funcionamento de equipamentos industriais, como os presentes nas centrífugas de enriquecimento de urânio no Irã. O Stuxnet infecta o Controlador Lógico Programável (CLP), responsável na automação dos processos eletromecânicos que são usados para controlar tanto as

máquinas quanto rotinas industriais completas. Esse *worm* de computador foi projetado para explorar falhas dentro do sistema operacional Windows (PATIL, SHINDE, BANERJEE, 2021, p. 01), conhecidas como *Zero-Day*, sendo eles:

> *Exploits zero-day*, entretanto, não são *exploits* comuns, mas a propriedade mais preciosa no mundo dos *hackers*, pois atacam brechas que ainda são desconhecidas pelos fabricantes de *software* e pelos fornecedores de antivírus – o que significa que ainda não há assinaturas de antivírus para detectar tal *exploit* e nem atualizações disponíveis para reparar as brechas que eles atacam. (ZETTER *apud* PEREIRA, 2018, p. 39)

Em sua obra, Zetter afirma que o uso desse tipo de vulnerabilidade não é comum, pois geralmente os *malwares* usam de falhas antigas para invadir as máquinas. A jornalista menciona que, anualmente, cerca de 12 milhões de vírus e arquivos maliciosos são detectados pelos antivírus, e, destes, apenas cerca de uma dúzia deles utilizam *zero days*. O código de Stuxnet apresentou quatro desse tipo de *exploits* (ZETTER, 2014, p. 11).

O *worm* de computador se espalhou por meio de um dispositivo *pen drive* infectado, inserido nas máquinas de sistema operacional *Windows*, com programas SCADA, que controlam as centrífugas de enriquecimento de urânio do Irã. O uso dessa forma de infecção é devido ao fato que essa instalação não possui nenhuma ligação com a internet, por onde normalmente os computadores acabam contraindo vírus. O Stuxnet, depois de instaurado, passa por algumas fases: primeiro, o *malware* executa o código principal; então as cópias propagadas se executam de forma automática; logo o serviço usa uma certificação digital legítima, conseguida através de informações internas prévias da instalação, para que não seja detectada pelo antivírus; e, por fim, o *rootkit* oculta os códigos e processos maliciosos para contornar os mecanismos de detecção; o que fazia com que as máquinas não demonstrassem nenhuma alteração nos processos; mesmo que as velocidades fossem mais altas, os relatórios apresentados aos técnicos não constavam nenhuma mudança (PATIL, SHINDE, BANERJEE, 2021).

Resultando em uma falha no funcionamento das centrífugas de enriquecimento de urânio, fazendo com que estas fossem prejudicadas pela rapidez com que eram infligidas, precisando de um maior número de trocas dos equipamentos, sendo algo custoso para o governo iraniano e que atrasou o programa, considerando que os ataques, apesar de serem muito mais significativo em Natanz, também atingiram os programas

da Usina Nuclear de Bushehr, que estava perto de sua inauguração (LOPES & OLIVEIRA, 2014).

Então, o que foi idealizado pelos engenheiros especialistas em computação e física nuclear dos EUA e de Israel, o complexo código malicioso conseguiu, através das vulnerabilidades encontradas nas máquinas do Irã, interferir em seu programa nuclear, de uma forma discreta e que demorou para que fosse identificada como um evento causado por um *malware*, destinado a prejudicar as centrífugas, parecendo aos técnicos que era apenas um problema de mau funcionamento (LOPES & OLIVEIRA, 2014).

Essa solução aplacou o desenvolvimento nuclear iraniano, que era a maior preocupação de G.W. Bush e do governo israelense. Essa alternativa de resolução, além de ser muito menos custosa do que o uso da força militar, se mostrou com menor impacto político do que outros feitos, pois, apesar de diversas referências bibliográficas apontarem os dois Estados que demonstravam maior apreensão com as evoluções tecnológica nuclear do Irã como os culpados pelo Stuxnet, não há declaração oficial dos governos assumindo a responsabilidade pelo ataque ou pela criação do *malware* (LOPES & OLIVEIRA, 2014). E é difícil identificar o local exato onde foi desenvolvido um vírus, devido à complexidade. Diferente de uma arma física, que vai requerer um local para produção, investimento, material, transporte, que poderia ser rastreado até a organização ou país, por trás da fabricação bélica. Já um código malicioso pode ser escrito de forma remota, necessitando apenas de conexão com internet e computadores capazes.

Apesar de muito bem elaborado, os criadores do *malware* não esperavam um comportamento incomum do *worm*. O que antes foi criado com alvo específico, o programa nuclear iraniano, acabou, em 2010, redirecionando os ataques para outros países, atingindo instalações nucleares na Indonésia, Índia, Azerbaijão e até mesmo usinas nos EUA e no Brasil. Isso porque um erro no código do Stuxnet permitiu sua circulação na Internet. Clarke e Knake (2012) falam sobre a postura dos EUA e do posterior presidente estadunidense Barack Obama, após o "isolamento" desse *worm*. Tendo em vista que um ataque cibernético a outro país faria com que a credibilidade estadunidense no cenário internacional fosse afetada, para evitar conflitos, os EUA se alinharam a outros Estados soberanos (LOPES & OLIVEIRA, 2014, pp. 61- 62).

Então, apesar do ataque cibernético ter afetado seu programa nuclear, isso não parou os avanços do Irã, causando apenas um atraso temporário nos planos. O

vazamento do código do *worm* ocasionou uma consequência inesperada, pois agora não só o país-alvo, mas todas as outras soberanias, inclusive os próprios EUA, estavam vulneráveis a ataques aos alicerces mais importantes de um governo, como instalações de energia, como foi feito, ou outras infraestruturas (LOPES & OLIVEIRA, 2014, p. 62).

3.2. Impactos da Primeira Arma Cibernética

O Stuxnet pode ser um dos *worms* de computador mais conhecidos do mundo. Sua codificação sofisticada, construída com diferentes tipos de linguagens de programação, usando uma sequência de recursos como *zero-days* e *rootkit*, para causar estragos sem ser identificado, nem pelas máquinas nem pelos técnicos, tanto os que trabalhavam na própria instalação nuclear de Natanz, quanto os responsáveis pela manutenção das máquinas, que, para desvendarem a totalidade desse *worm*, analisaram-no por numerosos dias, em equipes associadas de várias empresas especializadas em antivírus. Um dos primeiros impactos, ainda que não ligados à segurança internacional, está na inovação tecnológica do Stuxnet, trazendo à luz a possibilidade de *malwares* utilizarem de diferentes recursos de programação, causando estragos antes inimagináveis, como danos em meios físicos (PEREIRA, 2018).

Mas seu destaque não está unicamente em sua complexa estrutura, ou mesmo pelo alvo do ataque ser o programa nuclear do Irã, este que, sempre foi muito discutido e repercutido nos meios midiáticos, devido ao seu desenvolvimento, e pelo conflito que causava entre os países que estavam receosos de que essa tecnologia fosse usada para armas químicas. Esse *malware* explicitou como a questão cibernética é desafiadora (LOPES & OLIVEIRA, 2014). Nesse caso, focando no âmbito militar, o Stuxnet é o primeiro ato de uma guerra cibernética, materializando o que foi apenas teorizado, como Clarke e Knake relatam nesta passagem:

> [...] quando o termo guerra cibernética surge, é tido como algo meramente teórico. Em outras palavras, era difícil de se calcular, no início dos anos 1990, um ataque utilizando um *software* que causasse danos a *hardware* de alguma infraestrutura crítica estatal. Essa opção surge, para o caso iraniano, de dentro do U.S. *Strategic Command* (USSTRATCOM), que há muito tempo se ocupava em aperfeiçoar o potencial bélico dos EUA. (CLARKE & KNAKE *apud* LOPES & OLIVEIRA, 2014, p. 59)

Apesar de se terem relatos de outros ataques cibernéticos anteriores ao ocorrido em 2010, que são considerados parte da história da ciberguerra, o Stuxnet é o primeiro que, através de códigos maliciosos, conseguiu prejudicar algo fisicamente, forçando o Irã a substituir mais de 900 centrífugas de enriquecimento de urânio. O que anteriormente era limitado a ataques em sites e serviços dos governos, o que já gerava transtornos e impactos econômicos, passou a ter novas proporções, quando infraestruturas essenciais puderam ser prejudicadas com vírus como esse (LOPES & OLIVEIRA, 2014).

Algo para ser notado é que, entendendo o ciberespaço como algo amplo, que engloba não só as redes de comunicação, *software* e *hardware*, e a internet, mas também um meio que contém milhões de informações, seja do campo corporativo, comercial, financeiro, governamental, ou, como visto agora, da esfera militar e industrial, que transitam diariamente esse espaço. Justamente essa abrangência traz uma complexidade para assuntos ligados ao ciberespaço, como, por exemplo, a dificuldade em identificar culpados de crimes cibernéticos, a constituição de leis e penas e a prisão de fato de criminosos desse âmbito. Uma guerra usando esse mesmo cenário assume essa mesma característica intrincada. Motivo pelo qual, até nos dias de hoje, nenhum país foi oficialmente considerado culpado e recebeu pena pelo uso de *worm* de alta tecnologia para invadir uma infraestrutura de outro país soberano (PEREIRA, 2018).

E é nesta circunstância que surge uma nova capacidade bélica, adaptada para as transformações tecnológicas do presente momento, utilizando o ciberespaço para atingir as necessidades políticas e militares de um governo. Zetter, que no próprio título de uma de suas obras, assim como outros jornalistas, pensadores e teóricos envolvidos com a temática da guerra e tecnologia, concordaram que o Stuxnet era a primeira arma cibernética criada e executada, caracteriza o artifício como:

> De modo geral, pode-se afirmar que as armas cibernéticas (*cyber weapons*) são aplicações da tecnologia de informações que buscam criar efeitos negativos na disponibilidade, integridade e\ou confidencialidade nos dados de um computador individual ou de sistemas complexos de comunicação. (LIN *apud* ASSIS, BITTENCOURT, TAVARES, 2020, p. 137)

O impacto dessa arma não permaneceu só no campo militar. Com uma criação, com códigos tão sofisticados, que atacavam vulnerabilidades ainda desconhecidas de *softwares* e não era identificada por programas, demonstrando normalidade nos

processos produtivos das máquinas, sendo usado em uma infraestrutura como a de energia, Zetter afirma que essa arma cibernética iniciou uma nova era de guerras. O Stuxnet serviria de exemplo para a elaboração e aperfeiçoamento de outras armas cibernéticas, que, de maneira remota, silenciosa, anônima, rápida e sem todas as questões políticas e diplomáticas envolvidas em um conflito, poderiam prejudicar outra soberania. Sendo que os responsáveis por esses ataques poderiam ser agentes do Estado ou não (PEREIRA, 2018), podendo ser planejado por associações, como o famoso grupo de *hackers Anonymous*.

Examinando as possibilidades de cenários ocasionado por *malwares* como esse, é compreensível por que se torna um motivo de apreensão para todos os países. O Stuxnet foi criado para causar um dano controlado, para ser confundido com falhas comuns dentro de um processo de produção. Mas, com poucas mudanças, o código poderia atingir estruturas críticas, e, gerando um desastre semelhante ao da Usina de Chernobyl (Ucrânia), uma tragédia que prejudicaria a população, o meio ambiente e a economia iraniana.

Muitos portais de notícias de 2011 acabaram apontando esse fato, após um pronunciamento da Rússia comparando as situações (FOREIGN POLICY, 2011). Claramente, não seria interessante para a diplomacia de nenhum Estado ser o responsável por tal ataque, mas esse tipo de arma não mais se limita apenas aos ataques de governos. Os ataques não se limitam às instalações nucleares, também podendo atingir o abastecimento de água, gás e internet. Em uma conjuntura sem conflitos, esse tipo de ação poderia ocasionar perda de milhares de dólares e problemática para as populações da área, sendo que efeitos semelhantes podem ser observados por situações em que, por algum motivo sem ser ciberataques, esses serviços param de funcionar. Já em um cenário de guerra, um país pode usar como meio de isolar o seu rival dos seus recursos mais vitais.

Visando essa problemática, os países sentiram urgência em se proteger desse tipo de ataque e de investir no aprimoramento das capacidades ofensivas cibernéticas (PEREIRA, 2018). Muitos Estados instauraram departamentos especializados, órgãos de inteligência, acolhimento da pauta dentro da segurança nacional nos anos subsequentes, com intuito de trabalhar com esse potencial cibernético (LOPES & OLIVEIRA, 2014, p. 60). O Instituto de Defesa Nacional de Portugal (IND) chegou até a publicar um *working paper* relatando as preocupações com a cibersegurança e quais

medidas o país deveria tomar para evitar que ataques dessa magnitude afetem a população portuguesa (IND, 2013).

Durante os anos subsequentes da descoberta do Stuxnet, pode-se observar um avanço na segurança internacional. Como campo teórico, influenciado pelas contribuições da Escola de Copenhague, com conceitos multissetoriais, teorizando que a securitização de um país alcança outros quatro setores além do militar, considerando também os setores: político, social, econômico e ambiental. Admite-se então o estudo da cibersegurança como parte da segurança internacional (FONSECA, 2021).

Esse campo teórico passa a ser mais valorizado, sofrendo uma ampliação em sua agenda, em razão do impacto das armas e da guerra cibernética, que agora podem ter significativos efeitos sociais (FONSECA, 2021), como danos físicos e mortes (PEREIRA, 2018, p. 58). Segundo Hansen e Nissebaum, a cibersegurança deveria ser pauta para segurança nacional, internacional e vista como uma estratégia de Estado (*apud* FONSECA, 2021), assim como foi para os EUA e Israel o uso de uma arma cibernética para seus objetivos. O estudo da área permite que a multiplicidade de áreas e de variáveis, que requer ações colaborativas, seja considerada, propiciando a compreensão do ecossistema formado, como explicado e ilustrado por Fonseca com a Figura 2, apresentada a seguir:

FIGURA 2 - ECOSSISTEMA DO CIBERESPAÇO

Fonte: FONSECA, 2021.

Observando que a cibersegurança precisa de uma estrutura que a apóie, através de instituições, políticas, estratégias e a legislação de proteção contra cibercrimes, para ordenar as ações mais internas, como a pesquisa e desenvolvimento, e cooperação tanto nacionais quanto internacionais, entre outras atividades envolvendo o ciberespaço (FONSECA, 2021). Uma questão interessante dos avanços no estudo desta área é, como já citado anteriormente, que, para abranger as necessidades linguísticas para se referenciar aos acontecimentos ligados ao ciberespaço, uma novo vocabulário foi sendo adotado.

No campo da segurança internacional, como parte do cenário internacional, medidas foram tomadas para a proteção global, como consequência do perigoso *worm* de computador analisado. A União Internacional de Telecomunicações, que foi fundada em 1865 para facilitar a conectividade internacional das redes de comunicação, realocando espectro de rádio global e órbita de satélites, e sempre progredindo nos padrões técnicos para oferecer a interconexão de redes e tecnologias, segundo o próprio *website* dessa agência internacional. A associação global conta com mais de 193 Estados-membros, além de empresas, universidades e outras organizações internacionais e regionais (UIT, 2021). Desde 2015, a União Internacional de Telecomunicações realiza um diagnóstico analisando a cibersegurança mundial, com base no Índice de Cibersegurança Global (GCI), mapeando os países mais comprometidos com a questão. Esse indicador é determinado por:

> Como a segurança cibernética tem um amplo campo de aplicação, abrangendo muitas indústrias e vários setores, o nível de desenvolvimento ou engajamento de cada país é avaliado em cinco pilares – (i) medidas legais, (ii) medidas técnicas, (iii) medidas organizacionais, (iv) desenvolvimento de capacidades e (v) cooperação – e então agregados em uma pontuação geral. (UIT, 2022, tradução nossa)

Esse instrumento de avaliação possibilita que os países observem suas proteções cibernéticas em relação aos outros Estados, incentivando a melhora, conforme uma pluralidade de pilares que compõem o índice. Para que o diagnóstico seja feito, os países participantes respondem a um questionário, com perguntas pertinentes aos pilares apresentados, através de cujas respostas um cálculo é feito e um *ranking* correspondente à pontuação de cada país é apresentado (FONSECA, 2021).

No ano de 2020, o Índice de Cibersegurança Global completou sua quarta edição, em meio ao cenário pandêmico, registrando significativo aumento no tráfego da

internet, tendo em vista que seu uso foi indispensável para o funcionamento de distintas áreas de atuação da sociedade. Essa elevação de 30% no uso da rede, consequentemente, foi recebida com um aumento dos riscos de crimes cibernéticos. Mesmo com esses desafios, o Índice de Cibersegurança Global de 2020 confirmou que muitos países conseguiram aprimorar a questão de cibersegurança em seus territórios, fosse com a criação de leis ou com investimentos nas pesquisas. No *ranking* mundial divulgado no ano de 2020, os líderes são países desenvolvidos, com capacidade de investimento nas áreas que abrangem a cibersegurança, como EUA e Grã-Bretanha, os primeiros da lista com pontuação de 100 ou milésimos de pontos perto disso (FONSECA, 2021).

O Stuxnet foi um estopim para percepções que a influência do ciberespaço não estava presente apenas na integração do cotidiano às tecnologias oferecidas pela era da informação. O campo da segurança internacional agora também englobava o multissetorial ciberespaço, que exigia que o cenário internacional se atentasse às questões de cibersegurança, investindo para entender e aprimorar essa área. Sendo esse seu maior impacto de fato, que resultou na integração do assunto nas agendas nacionais e internacionais de segurança. E que, desde então, vem sendo cada vez mais discutido pelos países e organizações internacionais, como o Conselho de Segurança das Nações Unidas, que, no ano de 2021, se reuniu para um debate sobre cibersegurança, tendo em vista as preocupações crescentes e a necessidade de cooperação entre os países para combater ataques cibernético e estruturar programas de ação diante do assunto (R7, 2021).

3.3. Legado do Stuxnet

Como previsto, o Stuxnet foi a primeira arma cibernética, que serviria como base para o aprimoramento de outros *worms* e vírus, tão perigosos quanto o primeiro. O que de fato aconteceu, quando dois outros vírus analisados mostraram semelhanças que indicavam que ou os mesmos programadores que codificaram o Stuxnet desenvolveram esses novos *malwares* ou que exerceram certa influência. Os dois foram descobertos na mesma época, no ano de 2012, e receberam o nome de vírus DuQu e vírus Flame (PEREIRA, 2018, p. 59).

O primeiro a ser descoberto foi o DuQu, nome que recebeu devido à nomenclatura "DQ" que os arquivos infectados recebiam. As máquinas de uma empresa apresentavam um arquivo estranho, e, para analisar esse arquivo, contataram os responsáveis pela segurança do sistema. O *malware* se tratava de um vírus de espionagem, que tinha como objetivo copiar senhas e registros presentes do computador e gravar dados dos dispositivos que interagissem com a máquina infectada. Para não levantar suspeitas de suas ações, o vírus armazenava em um arquivo temporário na máquina hospedeira, esperando um determinado período de tempo para compartilhar essas informações com os atacantes (ZETTER *apud* PEREIRA, 2018, p. 60).

Apesar de aparentar ser um vírus comum de espionagem, o código do DuQu possuía certas semelhanças com o Stuxnet, como o uso de um certificado digital roubado da máquina, para que não seja identificado a presença do mesmo pelo antivírus, o que não era muito comum em outros vírus. E o *driver* usado nas máquinas tinha a mesma datação dos que surgiram nas máquinas em Natanz (Irã), em 2009. Quando comparados os códigos dos *drivers* de ambos os *malwares*, notou-se uma grande semelhança entre eles. Além disso, o DuQu também explorou as vulnerabilidades desconhecidas em um sistema, os *exploits zero-day*. Concluindo-se que deveriam ser os mesmos autores do Stuxnet ou pessoas com acesso a esse código (PEREIRA, 2018, p. 60).

Uma diferença entre esses códigos maliciosos é que o DuQu teve uma infecção de máquinas controladas, com vítimas específicas, diferentemente do Stuxnet, que afetou centenas de máquinas, facilitando sua descoberta. As vítimas desse vírus eram empresas e pessoas envolvidas de alguma forma com o Irã, geralmente fabricantes de equipamentos industriais ou programas que poderiam fornecer informações para ataques cibernéticos, como o próprio *worm*, ou ataques físicos através de plantas de construção. Tornando isso, mais que um cibercrime, um risco para a segurança nacional desse país (PEREIRA, 2018, p. 60).

O segundo vírus, o Flame, descoberto após o DuQu, ainda que no mesmo ano, assim como o outro, compartilha várias semelhanças com o Stuxnet, mas seu código tem mais linhas de programação que o *worm* e é muito mais nocivo que o vírus anterior. Originalmente, o vírus era conhecido como "Wiper", coligando o significado do termo em inglês "limpador" com as ações provocadas por esse *malware* (PEREIRA, 2018, p. 61).

Os alvos desse ataque foram os computadores do Ministério do Petróleo Iraniano e da Companhia Nacional de Petróleo Iraniano. O Flame infectava as máquinas, limpando arquivos essenciais presentes nos discos rígidos dos sistemas com que entrava em contato. O vírus não só limpava os dados do ataque, mas também apagava seu código dos computadores infectados, deixando apenas um arquivo temporário chamado "~DF78.tmp", que era deletado do sistema eventualmente. As investigações sobre o Flame foram significativamente dificultadas por essa limpeza. Para que fosse descoberto algo sobre o vírus, os especialistas analisaram máquinas que ainda não demonstravam nenhum sinal de limpeza nos dados, sendo neles encontrados um arquivo que permanecia ali até que fosse ativado e prejudicasse o computador alvo (PEREIRA, 2018, p. 62).

O arquivo "~DEB93D.tmp" apresentou traços de ser também um vírus de espionagem, assim como o DuQu. A extensão do código do Flame era maior que a do Stuxnet, pois garantia que o vírus deletasse informações importantes e seus próprios rastros das máquinas infectadas e permitia também a obtenção dos dados circulados naquele computador. Zetter explica com mais detalhes como o Flame funcionava:

> Dentre elas estava um módulo que extraía documentos de máquinas infectadas e outro que gravava as teclas digitadas e capturava telas a cada intervalo de 15 a sessenta segundos. Um terceiro módulo se apropriava clandestinamente do microfone interno dos computadores infectados para espionar conversas nas imediações. Um quarto módulo usava a função Bluetooth do computador para roubar dados de quaisquer *smartphones* detectáveis e outros dispositivos Bluetooth na área. (*apud* PEREIRA, 2018, p. 62)

Ela ainda afirma que os meios de espionagem não se limitavam a esses acima mencionados, quando identificadas máquinas com mais informações ou com dados de maior relevância, arquivos complementares eram enviados, potencializando o vírus. Os alvos para esses roubos de informações, em grande maioria, pertenciam ao Irã. O que, devido ao Stuxnet, cujo envolvimento do governo dos EUA e de Israel era afirmado, aqui esses Estados se tornam também os principais suspeitos por esse novo ataque cibernético. As vítimas escolhidas cuidadosamente para controlar a proliferação e encontrar os dados mais valiosos (PEREIRA, 2018, p. 62).

Em sua estrutura, o Flame tem semelhanças com o DuQu, buscando o mesmo programa de arquitetura, acrescentada a uma busca por documentos de texto e tabelas do sistema operacional *Windows*. Usava *exploit zero-day* presente no código do Stuxnet,

o que, em razão da raridade do uso desse tipo de ferramenta, aponta que podem ser os mesmo responsáveis ou pessoas com o acesso ao *worm*. Um dos *exploits* que compunham o programa era novo, designado para atingir o sistema *Windows Update* para contaminar em outros computadores da rede (PEREIRA, 2018, p. 63).

Apesar de ambos não se caracterizarem como um ato de guerra cibernética, não deixam de ser menos preocupantes, já que através desses crimes cibernéticos, conhecimentos necessários para a criação de armas cibernéticas, tão ou mais perigosas que o Stuxnet, chegam ao poder de pessoas capacitadas para isso. Uma verdadeira preocupação para a segurança nacional de cada país e do debate de defesa cibernética no cenário internacional (PEREIRA, 2018, p. 63).

CONSIDERAÇÕES FINAIS

Por tanto, o *worm* de computador Stuxnet impactou a segurança internacional, pela valorização do campo da cibersegurança. Tendo em vista que mudou de forma significativa a área diretamente militar, com inclusão de um novo tipo de arma e guerra, a qual, devido à ligação com o ciberespaço, se torna multissetorial, não limitando seus danos ao campo de guerra. Mas, possibilitando atingir as infraestruturas essenciais para qualquer sociedade, causando prejuízos econômicos, sociais e ambientais. Como um reflexo desse desenvolvimento, os países estabeleceram medidas de segurança nacional, para estudar as tecnologias do campo cibernético, aprimorando-o para potenciais ataques ou defesas. E, na segurança internacional, maneiras de avaliar a cibersegurança e conter esse tipo de ataques, estão sendo discutidos.

De uma forma mais isolada, a criação do Stuxnet constituiu a primeira arma cibernética, considerando que, anteriormente, nenhum *malware* foi capaz de ter o mesmo impacto que esse, devido à sofisticação que lhe permitiu rodar em máquinas na instalação nuclear Natanz por meses antes de ser descoberto. Isso abriu precedências para que vírus de alta complexidade, de grande potencial de danos e extremamente perigosos pudessem ser criados. Essa arma trouxe para realidade algo que era apenas uma teoria dentro da significação de guerra cibernética: um *software* atingindo um *hardware* e gerando prejuízos físicos.

Em nossa opinião, foi de grande importância essa valorização da cibersegurança após os ataques cibernéticos, em principal o do Stuxnet. Pois essa área de estudos conseguiu se aprimorar, impedindo que *malwares* com objetivos mais sérios e prejudiciais fossem criados e criando maneiras de prevenir os ataques. Um exemplo é que mesmo o Stuxnet poderia causar danos parecidos com o que ocorreu em Chernobyl (Ucrânia). E, cada vez mais, tanto a segurança nacional dos países quanto a segurança internacional estão investindo na área de conhecimento.

REFERÊNCIAS BIBLIOGRÁFICAS

AFARY, Janet; AVERY, Peter William; MOSTOFI, Khosrow. "Iran". **Encyclopedia Britannica**. Disponível em: https://www.britannica.com/place/Iran. Acesso em: 7 fev. 2022.

ARMS CONTROL ASSOCIATION. **Official proposals on the Iranian nuclear issue**. **2003-2013**. 03/01/2022. Disponível em: https://www.armscontrol.org/factsheets/Iran_Nuclear_Proposals. Acesso em: 18 jan. 2022.

ASSIS, Ana Carolina; BITTENCOURT, Nathalia; TAVARES, Sandra. "Armas inteligentes no ciberespaço: Oportunidades inovadoras e desafios prementes". **Revista Brasileira de Estudos de Defesa**, ano 02, v. 07, jul. 2020, pp. 133-157.

ATWOOD, Kylie. "Irã diz que só enviará imagens de usinas nucleares à ONU após acordo com EUA". **CNN Internacional**, 03/06/2021. Disponível em: https://www.cnnbrasil.com.br/internacional/ira-diz-que-so-enviara-imagens-de-usinas-nucleares-a-onu-apos-acordo-com-eua/.Acesso em: 18 jan. 2022.

BCC. Entenda a polêmica envolvendo o programa nuclear do Irã. **BBC News** , 17 maio 2010. Disponível em: https://www.bbc.com/portuguese/noticias/2010/05/100517_entenda_ira_nuclear_mv. Acesso em: 10 jan. 2022.

CAETANO, Karizia Ribeiro Pereira. **O programa nuclear iraniano**: Ameaça internacional ou busca pela segurança do país. Monografia de Graduação em Relações Internacionais. Universidade de Brasília. 2014. Disponível em: https://bdm.unb.br/bitstream/10483/8290/1/2014_KariziaRibeiroPereiraCaetano.pdf. Acesso em: 18 jan. 2022.

FONSECA, Leila Oliveira da. "A cibersegurança sob o prisma das Relações Internacionais". **Revista Relações Exteriores**, 20/10/2021. Disponível em: https://relacoesexteriores.com.br/ciberseguranca-relacoes-internacionais/. Acesso em: 3 jan. 2022.

FOREIGN POLICY. **2011**. 29 dez. 2011. Disponível em: https://foreignpolicy.com/2011/. Acesso em: 3 jan. 2022.

GLOBO. "Presidente do Irã diz que país já tem capacidade para produzir urânio a 80%". **G1**, 11/02/2010. Disponível em: https://g1.globo.com/Noticias/Mundo/0,,MUL1485942-5602,00-PRESIDENTE+DO+IRA+DIZ+QUE+PAIS+JA+TEM+CAPACIDADE+PARA+PRODUZIR+URANIO+A.html. Acesso em: 18 jan. 2022.

IAEA. **Treaties**. 03/01/2022. Disponível em: https://www.iaea.org/resources/legal/treaties. Acesso em: 18 jan. 2022.

Irã e potências mundiais chegam a acordo nuclear. **G1** , São Paulo, 14 jul. 2015. Disponível em: https://g1.globo.com/mundo/noticia/2015/07/reuniao-fecha-acordo-sobre-programa-nuclear-do-ira-dizem-agencias.html. Acesso em: 15 jan. 2022.

Irã aceita retomar negociações sobre acordo nuclear. **G1** , São Paulo, p. 1, 27 out. 2021. Disponível em: https://g1.globo.com/mundo/noticia/2021/10/27/ira-aceita-retomar-negociacoes-em-viena-sobre-acordo-nuclear.ghtml. Acesso em: 4 jan. 2022.

IRAN Sanctions. *In*: U.S. DEPARTMENT OF THE TREASURY. **Islamic Republic of Iran**. 2022. Disponível em: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/iran-sanctions. Acesso em: 9 jan. 2022

LOPES, Gill & OLIVEIRA, Carolina. "Stuxnet e defesa cibernética estadunidense à luz da análise de política externa". **Revista Brasileira de Estudos de Defesa,** ano 01, v. 01, 07/072014, pp. 55-69.
MCSWEENEY, Bill. **Security, Identity and Interests**. 1. ed. Cambridge: Cambridge University Press, 1998. 255 p.

MORETÃO, Amanda. "A posição da mulher no Irã antes e depois da Revolução Iraniana em comparação com a Turquia". **Islamic Republic of Iran**, 2017, pp. 01-12. Disponível em: http://www.en.wwc2017.eventos.dype.com.br/resources/anais/1499195277_ARQUIVO_TextocompletoAmandaStinghen-AposicaodamulhermuculmananoIraenaTurquia.pdf. Acesso em: 7 fev. 2022.

PEREIRA, Bruno. **Stuxnet**: O impacto do ataque cibernético na segurança internacional. Trabalho de Conclusão de Curso em Relações Internacionais. Universidade Estadual Paulista "Júlio de Mesquita Filho" (Campus de Marília). 2018.

ROHR, Altieres. "Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia". **G1**. 02/10/2010. Disponível em: http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.htm. Acesso em: 10 out. 2021.

SCHWAB, K. **A quarta revolução industrial**. São Paulo: Edipro, 2016.

SILVA, Mayane Bento; NUNES, Thainá Penha Baima Viana; SILVA, Tienay Picanço Costa da. "A evolução do conceito de segurança e sua inserção nas Relações Internacionais". **Encontro Nacional da Associação Brasileira de Estudos de Defesa**, 2018, pp. 01-20.

THE WORLD BANK. **Islamic Republic of Iran**. 2022. Disponível em: https://www.worldbank.org/en/country/iran. Acesso em: 7 fev. 2022.

U.S. DEPARTMENT OF THE TREASURY. **Iran Sanctions**. 03/01/2022. Disponível em: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/iran-sanctions. Acesso em: 18 jan. 2022.

WORLD BANK. **Islamic Republic of Iran**. 2022. Disponível em: https://www.worldbank.org/en/country/iran. Acesso em: 7 jan. 2022.

ZETTER, Kim. **Countdown to zero day**: Stuxnet and the launch of the world's first digital weapon. New York: Crown Publishers, 2014.