FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ – FADIC
PRÓ-REITORIA DE GRADUAÇÃO
CURSO DE RELAÇÕES INTERNACIONAIS

GUILHERME ANTONIO GOMES CAVALCANTE

ATAQUES CIBERNÉTICOS E O CASO STUXNET: UM NOVO DESAFIO À SEGURANÇA INTERNACIONAL

RECIFE
2015

GUILHERME ANTONIO GOMES CAVALCANTE

ATAQUES CIBERNÉTICOS E O CASO STUXNET: UM NOVO DESAFIO À SEGURANÇA INTERNACIONAL:

Monografia apresentada à Faculdade Damas da Instrução Cristã - FADIC, como requisito para obtenção do título de Bacharel em Relações Internacionais.

ORIENTADOR: Prof. Antonio Henrique Lucena Silva

RECIFE

2015

Cavalcante, Guilherme Antonio Gomes.
Ataques cibernéticos e o caso stuxnet: um novo desafio à segurança internacional. / Guilherme Antonio Gomes Cavalcante. – Recife: O Autor, 2015.

66 f.

Orientador(a): Profª. Dr. Antonio Henrique Lucena Silva.
Monografia (graduação) – Faculdade Damas da Instrução Cristã. Trabalho de conclusão de curso, 2015.

Inclui bibliografia.

1. Relações Internacionais. 2. Segurança internacional. 3. Soberania estatal. 4. Guerra cibernética. 5. Guerra da informação. 6. Ataques cibernéticos. 7. Stuxnet

327	**CDU (2.ed.)**	**Faculdade Damas**
327	**CDD (22.ed.)**	**TCC 2015-548**

GUILHERME ANTONIO GOMES CAVALCANTE

ATAQUES CIBERNÉTICOS E O CASO STUXNET: UM NOVO DESAFIO À SEGURANÇA INTERNACIONAL

Monografia apresentada à Faculdade Damas da Instrução Cristã - FADIC, como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.

Aprovado em:____/____/_____

Nota: _____

BANCA EXAMINADORA

_____

Prof. Orientador: Antonio Henrique Lucena Silva
FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ – FADIC

_____

Prof.: Pedro Gustavo Cavalcanti Soares
FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ – FADIC

_____

Prof.: Luís Emmanuel Barbosa da Cunha
FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ – FADIC

SUMÁRIO

Lista de Ilustrações

Lista de Tabelas

Lista De Siglas

ARPANET – Rede da Agência de Investigação de Projetos Avançados dos Estados Unidos

AIEA – Agência Internacional de Energia Atômica

CD – Disco Compacto

CSNU – Conselho de Segurança das Nações Unidas

DDA – Departamento para Assuntos de Desarmamento

EUA – Estados Unidos da América

FBI – Agência Federal de Investigação dos Estados Unidos

HMI – Interface homem-máquina

IST – Iniciativa de Segurança Europeia

NIPC – Centro de Proteção da Infraestrutura Nacional dos Estados Unidos

NSA – Agência Nacional de Segurança dos Estados Unidos

ONU – Organização das Nações Unidas

OPEP – Organização dos Países Exportadores de Petróleo

PCCIP – Comissão Presidencial Para Proteção da Infraestrutura Crítica

SCADA – Sistemas de Supervisão e Aquisição de Dados

UNIDIR – Instituto para Pesquisa de Desarmamento

USB – Porta Serial Universal

ATAQUES CIBERNÉTICOS E A SEGURANÇA INTERNACIONAL:
O Caso do Stuxnet

Guilherme Antonio Gomes Cavalcante[*]

Resumo

Três décadas após o surgimento da Internet, a sociedade internacional depara-se com um novo desafio para a clássica agenda da segurança: os ataques cibernéticos. Ainda que em proporções menos graves do que as guerras tradicionais, os ataques cibernéticos constituem ameaça e desafio aos conceitos de segurança e soberania estatais por ocorrerem em um outro domínio, o ciberespaço, e pela rara identificação de seus autores, o que dificulta as possibilidades de defesa e coerção ao agressor. Nesse contexto, o presente trabalho busca identificar as mudanças que os ataques cibernéticos trazem ao cenário internacional, bem como descrever seus padrões e propor alternativas para a diminuição gradual de suas consequências para o sistema internacional. Para fins de análise, ao final deste trabalho apresenta-se um estudo de caso referente ao ataque ao programa nuclear iraniano através do malware Stuxnet.

Palavras-Chave: **Segurança Internacional, Soberania Estatal, Guerra Cibernética, Guerra da Informação, Ataques Cibernéticos, Stuxnet.**

[*] Estudante concluinte do curso de Relações Internacionais

Abstract

Three decades after the rise of the Internet, the international society is facing a new challenge for the classic security agenda: the cyber attacks. Although in minor proportions than traditional wars, cyber attacks constitute threat and challenge to State security and sovereignty concepts insofar as they occur on a different domain, cyberspace, and their authors are rarely identified, which hampers the possibilities for defense and coercion to the attacker. In this context, this paper seeks to identify the changes that cyber attacks bring to the international arena, as well as describe their patterns and propose alternatives for the gradual reduction of their consequences for the international system. For analysis purposes, the end of this paper presents a case study regarding the attack on the Iranian nuclear program through the Stuxnet malware.

Keywords: **International Security, State Sovereignty, Cyberwar, Information Warfare, Cyber Attacks, Stuxnet.**

Agradecimentos

Agradeço, primeiramente a Deus, fonte de toda a força, coragem, foco, persistência e confiança que me têm sido necessárias em cada passo da minha vida – neste caso, para a conclusão do curso de Relações Internacionais e para a feitura deste trabalho; pelo dom da vida, por minha família e amigos; por todas as oportunidades que me tem me dado; por ser a resposta para minhas vitórias.

Agradeço também aos meus pais, Graça e Rogério, e avós, Vilma e Zezito pelo apoio incondicional em todos os setores e momentos de minha vida, muitas vezes superando os próprios limites em nome do meu bem-estar. Agradeço por confiarem em minha decisão de mudar de cidade e estado a fim de estudar um curso até então pouco conhecido; por minha educação e valores; por compartilharem comigo minhas angústias e vitórias; por serem meus exemplos de trabalho duro, garra, fé e resiliência; pelo amor genuíno que sinto em cada momento que estamos juntos. São a razão maior para minha luta diária – não apenas por retribuição, mas por puro e verdadeiro amor.

Ademais, tenho enorme gratidão por todos os meus professores, desde o pré-escolar até a faculdade, por ir além da transmissão e facilitação de conhecimento: pela inspiração, pelo incentivo, pela dedicação; por acreditarem em mim, por formarem parte da minha personalidade.

Sou igualmente grato aos meus colegas da Faculdade Damas que estiveram comigo nessa agradável jornada do curso de Relações Internacionais – em especial a Daylhane, minha grande e admirável amiga, que me inspirou a fazer o curso de Relações Internacionais e tem estado comigo desde Maceió, passando pela faculdade e pela AIESEC; e a Isadora, pessoa maravilhosa, cuja companhia me propicia alegria, paz e conforto.

Prolongo minha gratidão aos meus superiores do estágio na Netmake, Márcia Araújo e Carlos Lacerda, pela compreensão e apoio no período da escrita deste trabalho. Foram fundamentais para esta realização. Um agradecimento especial a Márcia, por partilhar comigo seus conhecimentos acadêmicos e, além do âmbito do trabalho, me apoiar como amiga.

Por fim, agradeço ao Professor Antonio, meu orientador, por ter aceitado orientar-me e por todo o suporte, desde sugestão de tema e materiais de leitura, até pela paciência e compromisso.

E, de maneira geral, agradeço à vida, pela plenitude de poder finalizar minha graduação em Relações Internacionais com a certeza de que fiz a escolha certa. O curso permitiu-me o desenvolvimento não apenas acadêmica e profissionalmente, como também desenvolveu minha personalidade e me faz-me sentir hoje um cidadão do mundo. Insistir e persistir em fazer o que se ama vale muito à pena.

INTRODUÇÃO

Há bastante tempo, mais precisamente desde a Primeira Revolução Industrial, historiadores e cientistas sociais têm dissertado sobre como o mundo tem se transformado, tanto na esfera individual quanto global, a cada descoberta tecnológica ou científica. Não obstante, em meados da década de 1980, o mundo foi surpreendido com uma inovação tecnológica cujo impacto viria a transformar a humanidade em todas as suas instâncias: surgira a rede mundial de computadores, a Internet.

Devido principalmente a seu baixo custo e facilidade de acesso, a Internet popularizou-se ao longo das últimas décadas e trouxe impacto imediato a indivíduos, empresas e governos através do compartilhamento de conhecimento de maneira extremamente veloz, em âmbito global, ampliando as possibilidades de aprendizado; e facilitou a comunicação, uma vez que indivíduos e entidades de qualquer parte do globo podem comunicar-se em questão de segundos através da rede.

Em direção contrária ao impacto que a rede trouxe à esfera individual, o Estado foi impactado, tanto internamente quanto na relação com outros Estados, por um fenômeno resultante da popularização da Internet: a difusão de poder. Nas últimas décadas o cenário internacional tem mudado sua dinâmica com a participação de novos atores, notadamente indivíduos, agora capazes de interferir diretamente da esfera pública.

A despeito de todas as mudanças resultantes desse processo, como o protagonismo das redes sociais durante eleições em regimes democráticos, entre outras, o objetivo deste trabalho é compreender de que forma o conceito de segurança internacional tem sido ameaçado pela recente ascenção dos ataques cibernéticos e propor soluções para que os custos decorrentes de tais ataques sejam minimizados.

Nesse sentido, após a descrição da metodologia utilizada para a escrita do presente trabalho, o capítulo 1 inicia-se com alguns dos conceitos-chave da era informacional, visando à proporcionar melhor compreensão do que será discutido no capítulo seguinte. Define-se aí os conceitos de cibernética, infosfera, ciberespaço e poder cibernético.

Em seguida, apresenta-se uma perspectiva histórica da criação e desenvolvimento da Internet, desde a origem de sua precursora, a cibernética, até o que convencionou-se chamar de Revolução da Informação. Uma vez entendido o quão revolucionária foi a criação da rede mundial de computadores para a humanidade, nota-

se que a Internet poderia ser considerada, além de novo domínio de interação humana (além do espaço terrestre, aéreo, marítimo e espacial), um instrumento de poder. Partindo desse pressuposto, recorre-se ao conceito político de poder para, através de sua análise, responder ao questionamento anteriormente citado. Ainda, sabendo-se que o poder é objeto central das relações internacionais, juntamente ao interesse e à força, analisa-se se a Internet, enquanto nova forma de poder, poderia ser inserida na fórmula de poder internacional utilizada para calcular de maneira pragmática quão poderosos são os Estados.

O capítulo 1 traz, ainda, uma recapitulação de teorias das Relações Internacionais e aborda as conexões entre os principais conceitos de tais teorias e o surgimento da Internet como nova forma de poder e a transformação que esta trouxe para as relações entre os atores do cenário internacional.

Em suma, o Realismo/Neorrealismo forma a base para a compreensão de que os Estados continuam sendo os atores principais das Relações Internacionais, assim como a segurança permanece como prioridade nas agendas estatais. Ainda, tal teoria é coerente com o fato de que, apesar de ataques cibernéticos ameaçarem os Estados constantemente na contemporaneidade, o sistema internacional ainda tem como base a anarquia – ou seja, não há qualquer forma de regulamentação ou controle do uso na Internet no contexto transnacional.

A Teoria da Interdependência Complexa, por sua vez, demonstra-se coerente e atual quando notamos que a popularização da rede levou ao surgimento de novos atores no cenário internacional, originando a difusão de poder e interdependência que hoje observamos. Além disso, um dos autores de tal teoria contribui também para o entendimentos do "fenômeno Internet" com novos conceitos de poder (*hard* e *soft power*), podendo a rede ser utilizada de ambas as formas, conforme será visto no decorrer do capítulo.

No capítulo 2, chega-se ao tema central do trabalho: a segurança cibernética. A priori, aborda-se de forma sucinta os conflitos e guerras (quando já é utilizada a força a despeito da diplomacia), desde o período precedente à Internet até os dias atuais. Em seguida, questiona-se se o popular termo "guerra cibernética" seria apropriado ou não para definir os conflitos que ocorrem no ciberespaço, levando em consideração a gravidade das consequências dos ataques cibernéticos quando comparados com a gravidades e as consequências das guerras ocorridas ao longo da história.

A partir de então, como principal fator de ameaça à segurança cibernética internacional, os ataques cibernéticos são explorados a fundo ao longo do capítulo: exploram-se as bases para seu surgimento; os atores envolvidos; seus objetivos; suas consequências para o sistema internacional; e a forma como eles são percebidos/reconhecidos internacionalmente.

Por último, ao ser observada a gravidade dos ataques cibernéticos à segurança dos Estados, são apresentadas algumas propostas de cientistas políticos e outros teóricos visando à resolução desse tipo de conflito, de modo a garantir o interesse prioritário dos Estados – a segurança.

A título de exemplo e visando à compreensão aprofundada de um ataque cibernético, o capítulo 3 traz como estudo de caso o ataque da aliança Estados Unidos-Israel ao Irã, através da infecção, por meio do *malware*[1] Stuxnet, a algumas centrífugas enriquecedores de urânio daquele à país, com o intuito de boicotar o programa nuclear iraniano.

Antes de chegar ao ataque em si, o capítulo é iniciado com uma contextualização do Irã, ressaltando sua importância histórica, os motivos de obter grande atenção por parte das grandes potências e suas principais diretrizes para a política externa, com foco nas relações com Israel e os Estados Unidos. Na sequência, explica-se a origem do programa nuclear iraniano e sua repercussão internacional.

A parte seguinte do capítulo trata das ideias originais dos Estados Unidos para a criação do Stuxnet e a forma como tal *malware* age quando é inserido em um sistema eletrônico, contando com uma ilustração e um fluxograma para compreensão do processo. Nessa parte, os aspectos técnicos são evidentemente vistos de maneira superficial, uma vez que o presente trabalho tem como foco as reações que tal *malware* provocou para as relações interestatais, e não sua capacidade técnica.

Na sequência, o capítulo descreve a descoberta e a repercussão do ataque, chegando-se finalmente à hipótese do presente trabalho, aplicado ao caso do Stuxnet: este trabalho defende a hipótese de que os ataques cibernéticos ocorrem visando a manipular informações, de modo a confundir o alvo dos ataques e levá-lo a uma tomada de decisão que seja benéfica ao agressor. Tais ataques, porém, provam-se, além de antiéticos, ilegítimos, uma vez que ferem ao princípio básico da soberania estatal. Ao

[1] A ser definido no capítulo 3

final, soluções a curto, médio e longo prazo são apresentadas em referência aos ataques cibernéticos.

CAPÍTULO 1 – A Cibernética e sua Inserção nas Relações Internacionais

1.1 Problema e Metodologia

A origem da definição do tema para o presente trabalho encontrou-se na ideia de ligar fatos e teorias referentes às Relações Internacionais ao espaço cibernético, conceito bastante contemporâneo, uma vez que muitos dos temas estudados no curso ainda estão ligados a conceitos clássicos e historicamente replicados, como guerras, acordos de cooperação internacional, entre outros assuntos. No entanto, dada a demasiada amplitude do tema proposto inicialmente, deu-se a necessidade de delimitá-lo e chegou-se ao assunto dos *conflitos cibernéticos internacionais*, assim como definiu-se que sua estrutura seria baseada em referencial teórico, desenvolvimento e estudo de caso.

O procedimento seguinte para a feitura desta monografia foi a identificação do problema e da hipótese, juntamente à delimitação temporal e espacial. Definir tempo e espaço para o tema proposto não foi tarefa árdua, visto que, apesar de muitos participantes no processo, há um consenso para a data de criação da Internet (1985), continuando seus impactos até os dias de hoje, e seu uso pode ser identificado na imensa maior parte do globo terrestre.

O problema, por sua vez, foi observado como a vulnerabilidade dos atores internacionais, principalmente os Estados, frente a uma nova forma de conflito internacional, os ataques cibernéticos. Devido à ausência de um sistema de governança capaz de conter tais ataques, caracteriza-se um novo desafio para os estudos de segurança internacional. Seguiu-se, naturalmente, a hipótese de que, a fim de defender-se, os atores internacionais afetados – sejam eles Estados, corporações ou indivíduos, devem criar soluções a curto prazo, como o uso de sistemas eletrônicos mais robustos e, ao mesmo tempo, ter como estratégia de defesa a longo prazo a criação de leis internacionais acordadas entre a maioria e que funcionem em termos de normatividade, julgamento e coerção dos crimes cibernéticos.

O desenvolvimento do trabalho seguiu-se através de pesquisa bibliográfica de livros e artigos científicos. Cabe a observação de que, a cada nova obra pesquisada, a (micro) estrutura do trabalho modificava-se. Para o capítulo 1, por exemplo, percebeu-se a necessidade de, além de resumir teorias clássicas das Relações Internacionais e sua

relação com o tema, incluir antes a presente metodologia e posteriormente um breve histórico da Internet, assim como seus conceitos-chave, que antes estariam no capítulo 2. Ademais, também foi percebida a necessidade de incluir no primeiro capítulo a definição de poder, um dos eixos primordiais das Relações Internacionais.

O capítulo 2, por sua vez, tinha como estrutura inicial o conceito de guerra, sua perspectiva histórica e, em seguida, características da chamada *guerra cibernética*. Entretanto, no decorrer da pesquisa bibliográfica, notou-se que a nomenclatura *guerra cibernética* para classificar os conflitos internacionais ocorridos dentro e através do ciberespaço, ainda é alvo de controvérsias sobre sua adequação, uma vez que o conceito clássico de guerra sempre esteve ligado a confrontos físicos, o que não ocorre no ciberespaço. Por esse motivo, sempre baseado em pesquisa bibliográfica, chegou-se a estrutura final do capítulo: tratar sobre as origens, os atores, as formas de conflito, seu reconhecimento internacional e, por fim, as possíveis soluções para constranger os atores de ataques cibernéticos.

Para o estudo de caso apresentado no capítulo 3 deste trabalho, definiu-se o aprofundamento no caso do uso do vírus Stuxnet, uma demonstração clássica da relevância de ataques cibernéticos para as relações entre os Estados. A escrita do capítulo deu-se por uma perspectiva histórica em paralelo a referências conceituais apresentadas nos capítulos anteriores.

Dessa forma, os métodos de pesquisa utilizados no presente trabalho são dois: o método histórico e o método monográfico. O primeiro método será utilizado para a contextualização temporal do surgimento da cibernética, da Internet e posteriormente dos ataques cibernéticos. Mais adiante, no capítulo 2, declarações feitas em determinados períodos históricos demonstram a relevância que autoridades de governos nacionais e de órgãos supranacionais têm dado à segurança cibernética. O método também é usado no capítulo 3, quando é descrita uma perspectiva histórica do Irã, anteriormente ao ataque cibernético do Stuxnet, e do ataque em si, abrangendo sua origem, prática, descoberta e consequências.

Finalmente, e em paralelo ao método histórico, o método monográfico é utilizado quando, através de um estudo de caso sobre a utilização do vírus Stuxnet pela aliança Estados Unidos-Israel contra o Irã, explica-se a origem, o desenvolvimento, as causas e consequências, a título de exemplo de ataques cibernéticos em geral.

1.2 Conceitos-chave

1.2.1 Cibernética

O termo cibernética foi cunhado pela primeira vez em 1948 pelo matemático estadunidense Norbert Wiener (1894-1964) em sua publicação *Cybernetics: or the Control and Communication in the Animal and the Machine*, em que, junto a colaboradores, desenvolveu o conceito de que, de maneira geral, o sistema de processamento de informações, assim como seu controle e certas funções seriam equivalentes matemáticos em seres vivos e em máquinas[2]. Esse campo de pesquisa foi, então, designado na língua inglesa como *cybernetics*, uma derivação do grego *kubernetes* (timoneiro, piloto de barco), trazendo o sentido de controle para o termo[3]. Cibernética seria, então, uma derivação natural para a língua portuguesa do termo cunhado em inglês, sendo definida como a ciência do controle e da comunicação entre os seres vivos e as máquinas.

1.2.2 Infosfera

Sheldon[4], em seu capítulo *The Rise of Cyberpower* para o livro *Strategy in the Comtemporary World* (2013) define o que seria a infosfera. Também conhecida como ambiente ou domínio informacional, é um lugar no espaço e tempo onde a informação existe e flui[5]. A informação encontrada na infosfera flui no ciberespaço e o uso dessa informação para conquistar objetivos políticos é o poder cibernético – ambos os conceitos serão definido a seguir.

A informação – como é criada, armazenada, comunicada e manipulada – é um produto da infosfera. O ciberespaço é apenas um subconjunto da infosfera, apesar de ser cada vez mais significante. Sob o ponto de vista de Sheldon, o ciberespaço estaria rapidamente preenchendo várias funções da infosfera, citando como exemplo o fato de que os jovens de hoje prefeririam enviar mensagens de texto do que conversar pessoalmente.

---

[2]KIM, Joon Ho. Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. **Horizontes Antropológicos**. Porto Alegre, vol.10, no.21, jan./jun.
[3]KIM apud WIENER 1948, p. 19; 1984, p. 15.
[4]SHELDON, John B. The Rise of Cyberpower, p. 309. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. (Ed.). **Strategy in the Contemporary World.** Nova Iorque: Oxford University, 2013. P. 309.
[5]SHELDON, p. 309 apud Lonsdale 2004:181.

1.2.3 Ciberespaço

Posteriormente ao surgimento da cibernética, com o desenvolvimento de cada vez mais dispositivos eletrônicos e sua presença no cotidiano de indivíduos de todo o mundo – tais como o telefone, o computador e depois a Internet, surgiu o termo *ciberespaço*. Citado pela primeira vez em 1982 pelo escritor estadunidense de ficção científica William Gibson em sua obra *Burning Chrome* e popularizado dois anos depois na obra *Neuromancer*, o significado de ciberespaço vem a ser definido por seu compatriota e também escritor Bruce Sterling, considerado um dos criadores da literatura *cyberpunk*. Sterling define ciberespaço em sua obra de não-ficção *The Hacker Crackdown - Law and Disorder on the Electronic Frontier*:

> Mas o território em questão, a fronteira eletrônica, tem cerca de 130 anos. Ciberespaço é o "lugar" onde a conversação telefônica parece ocorrer. Não dentro do seu telefone real, o dispositivo de plástico sobre sua mesa. [...] [Mas] O espaço entre os telefones. O lugar indefinido fora daqui, onde dois de vocês, dois seres humanos, realmente se encontram e se comunicam. [...] Apesar de não ser exatamente "real", o "ciberespaço" é um lugar genuíno. Coisas acontecem lá e têm consequências muito genuínas. [...] Este obscuro submundo elétrico tornou-se uma vasta e florescente paisagem eletrônica. Desde os anos 60, o mundo do telefone tem se cruzado com os computadores e a televisão, e [...] isso tem uma estranha espécie de fisicalidade agora. Faz sentido hoje falar do ciberespaço como um lugar em si próprio. [...] Porque as pessoas vivem nele agora. Não apenas um punhado de pessoas [...] mas milhares de pessoas, pessoas tipicamente normais. [...] Ciberespaço é hoje uma "Rede", uma "Matriz", internacional no escopo e crescendo rapidamente e constantemente.[6]

Mais contemporaneamente, Nye[7], por sua vez, define o ciberespaço como o conjunto de recursos relacionados à criação, controle e comunicação de informações eletrônicas e computacionais; e não apenas os computadores estariam inclusos, mas também intranets, celulares e comunicações espaciais.

---

[6]KIM, op. cit., apud STERLING, 1992, pp. 11-12.
[7]NYE JR., Joseph Samuel. **The Future of Power**. Nova Iorque: Public Affaris, 2011, p. 168

O ciberespaço é, portanto, um conceito real, com consequências reais para o espaço físico e sua existência está intimamente relacionada ao desenvolvimento da Internet, uma vez que, se não houvesse interligação ou interconexão, os computadores seriam meras máquinas, como tantas outras, e o conceito de ciberespaço não teria ganho força e sentido.

1.2.4 Poder cibernético

Ainda de acordo com Sheldon[8], o poder cibernético seria o processo de conversão da informação existente na infosfera para efeito estratégico dentro e a partir do ciberespaço, seja em períodos de paz, crise ou guerra.

A definição de Sheldon é coerente com a de Nye, uma vez que este afirma que poder cibernético seria "a habilidade de obter resultados desejados através do uso de recursos de informação do domínio cibernético interconectados eletronicamente". Ainda de acordo com Nye, o poder cibernético pode ser usado para produzir resultados desejados *dentro* do ciberespaço ou pode utilizar instrumentos cibernéticos para produzir resultados desejados em outros domínios, *fora* do ciberespaço.

1.3 A Internet e a Revolução da Informação

Conforme pode ser observado pelos conceitos acima apresentados, a cibernética viria a ser apenas o primeiro passo para a criação de uma ferramenta que viria a revolucionar a humanidade no final do século XX: a Internet. Por ser, ao mesmo tempo, o cenário e o próprio instrumento dos conflitos cibernéticos estudados no presente trabalho, é de fundamental importância compreender como se deu seu surgimento e quais foram as principais mudanças que ela trouxe para a humanidade; notadamente a revolução informacional.

Vale salientar que a história da Internet, assim como a do computador – máquina que a antecedeu e possibilitou primariamente a sua utilização, possui protagonistas múltiplos, que ao longo de muitas décadas contribuíram, na teoria ou na prática, para o que resultou em uma das maiores invenções da humanidade. Nesse sentido, o objetivo do início deste capítulo não é de aprofundar-se na história da Internet, mas sim

[8] SHELDON, op. cit., p. 306.

apresentar seu surgimento de forma introdutória, bem como explicitar brevemente a forma como a Internet revolucionou a maneira como o homem lida com a informação.

1.3.1 Precedentes históricos da Internet

Máquina pioneira para utilização da Internet, o computador nasce muito anteriormente a ela. Os registros mais remotos sobre sua existência relatam que o primeiro computador digital[9], desenvolvido por Charles Babbage (1791-1871) em 1839, foi projetado para a resolução de problemas matemáticos. Apesar das progressivas modificações nessa máquina ao longo das décadas seguintes, deixando de ser um equipamento de enormes proporções para tornar-se o *laptop* ("em cima do colo", em tradução livre do inglês) que conhecemos hoje, pode-se dizer que o computador apenas tornou-se relevante para toda a humanidade após o surgimento da rede mundial de computadores, a Internet, em meados da década de 1980.

A ideias iniciais do que viria a ser a Internet surgiram na década de 1960, em plena Guerra Fria, quando as Forças Armadas dos Estados Unidos encomendaram um estudo a partir do qual fosse possível descobrir uma estrutura para que suas linhas se comunicação pudessem ficar imunes a qualquer ataque da União Soviética. Deu-se assim o surgimento da ARPANET, a Rede da Agência de Investigação de Projetos Avançados dos Estados Unidos[10].

Desenvolvida nas universidades estadunidenses, a *net* passou a ser utilizada também para fins acadêmicos, em paralelo aos fins de defesa nacional idealizados pelo governo daquele país. Compreendida como forma de compartilhamento e armazenamento de informação, em seus primórdios essa tecnologia foi largamente utilizada por professores, pesquisadores universitários e funcionários do governo estadunidense, estimando-se cerca de dois mil usuários em 1975[11].

Não demorou para que a Internet deixasse de ser recurso desse seleto grupo de acadêmicos e funcionários do Departamento de Defesa dos Estados Unidos. Em 1979, ao perceber o potencial dessa tecnologia para o comércio, foi criado o CompuServe, primeiro provedor de serviços comerciais online, ainda nos Estados Unidos. Em seguida, o novo negócio despertou interesse de grupos alemães e franceses, que

---

9 KIM, op. cit. *apud* WINEGRAD; AKERA, 1996.
[10]ABREU, Karen Cristina Kraemer. História e usos da Internet. **Biblioteca on-line de Ciência da Comunicação.** v. 12, p. 05-09, 2009 apud TURNER; MUÑOZ (2002, p. 27)
[11]ABREU, op. cit.

ligaram-se à American On-Line (AOL), o segundo provedor comercial a ser criado[12]. Rapidamente outros provedores surgiram e, à medida que os investidores recrutavam assinantes, a Internet passou a ser usada também para fins de entretenimento, popularizando-se nos anos seguintes de maneira extremamente veloz.

Foi nesse contexto que Tim Berners-Lee, pesquisador inglês, imaginou o que chamaria de *World Wide Web*, em 1989[13]. Tal conceito consiste no que reconhecemos hoje como Internet: uma rede mundial de computadores, controlados por usuários, cujas informações armazenadas estão mundialmente interligadas.

Como pode-se observar pelo resumo histórico acima descrito, a razão para o surgimento da Internet enquanto estrutura ou sistema foi a manipulação e a segurança de um conceito que vem a ser palavra-chave para os desdobramentos posteriores do presente trabalho – a *informação*. Seja no campo da educação, do entretenimento ou da política, a Internet tomou espaço por ser uma ferramenta preciosa para a troca e o armazenamento de informações. As relações estabelecidas pelos homens entre si e com o mundo não foram mais as mesmas após o surgimento da Internet; e as mudanças consequentes desse episódio serão explicitadas no tópico seguinte.

1.3.2 A Revolução da Informação

A comunicação entre os homens, isto é, a troca de informações entre si, tem sido, ao decorrer da História, mola propulsora para o desenvolvimento da humanidade. A título de exemplo das grandes mudanças geradas pela interação entre os homens, podem ser citadas a invenção da escrita (aproximadamente 6000 a.C.), que possibilitou a transmissão de conhecimento de uma geração para a seguinte; o desenvolvimento dos transportes (estradas, ferrovias, navegação e aviação), possibilitando a troca de conhecimento entre povos de regiões longínquas; e, mais recentemente, o surgimento da Internet, que encurtou absolutamente o tempo e a distância entre as pessoas. A Internet tornou possível que, hoje, indivíduos de todas as partes do globo comuniquem-se e troquem informações instantaneamente através de websites, e-mails, redes sociais e programas conectados à rede.

Dadas as enormes mudanças originárias da Internet e testemunhadas contemporaneamente, alguns historiadores caracterizam o período entre o final do

[12] ABREU, op. cit.
[13] Idem apud BRIGGS; BURKE 2006, p. 302.

século XX até os dias atuais como Revolução da Informação – em comparação com a Revolução Agrícola e a Revolução Industrial, também fenômenos de grandes transformações para a humanidade. Em razão de ser especialmente recente e de sermos testemunhas de tal revolução, a Revolução da Informação é uma teoria ainda em construção, podendo ser denominada também como Revolução Técnico-Científica-Informacional, Terceira Revolução Industrial (por considerar-se a Internet uma continuação do desenvolvimento tecnológico originado das duas revoluções anteriores)[14] e ainda há quem afirme que a criação da *World Wide Web* não foi a primeira revolução da informação, mas apenas a quarta, uma vez que, anteriormente a esta, houve a invenção da escrita, a invenção do livro escrito (1300 a.C.) e a invenção da impressão (1450)[15]. A título de padronização para o presente trabalho e coerência com o que será posteriormente apresentado, tal revolução será doravante chamada de Revolução da Informação.

A fim de compreender de que forma a Internet possibilitou a Revolução da Informação, o cientista político Joseph Nye aponta em sua obra *O Futuro do Poder* as causas prováveis para as grandes mudanças ocorridas nos últimos tempos. De acordo com ele, a principal característica da Internet que viria a proporcionar a Revolução da Informação não teria sido apenas a *rapidez* da comunicação entre as pessoas (o telégrafo possibilitou comunicação instantânea entre os ricos por mais de 130 anos), mas sim a rápida e extrema redução dos custos para buscar, criar, processar e transmitir informações – argumentando que o custo para exercer tais atividades era, no início do século XXI, apenas um milésimo do que custaria da década de 1970[16]. Nenhuma outra tecnologia teria tido tão rápida redução de custos e, por isso, o acesso à rede tornara-se tão popular.

Ainda segundo Nye, tamanha redução dos custos para uso da Internet, aliada à diminuição dos aparelhos com acesso à rede, levou a uma espécie de descentralização da informação, que antes permanecia restrita a governos e empresários de grandes sistemas de informação, como redes de televisão, rádio e jornais. Além disso, se antes as informações eram passadas no sentido de um para muitos (rede de comunicação para a população), a popularização da Internet possibilitou a difusão da informação de todas

[14] MOREIRA, Ruy. Sociabilidade e espaço: as formas de organização geográfica das sociedades na era da Terceira Revolução Industrial-um estudo de tendências. **Agrária**, São Paulo, n. 2, p. 93-108, 2005.
[15] AMARAL, Luis Mira. A sociedade da informação. **JD Coelho, A sociedade da informação-O percurso português**, p. 85-92, 2007.
[16] NYE JR., Joseph Samuel. **The Future of Power**. Nova Iorque: Public Affaris, 2011. p. 85.

as formas: de um para um (email), de um para muitos (websites e blogs), de muitos para um (Wikipedia) e de muitos para muitos (redes sociais)[17].

Por haver originado tamanhas mudanças para a humanidade, a ponto de serem definidas como *revolução*, poder-se-ia considerar a Internet não apenas como o espaço em que as grandes mudanças têm ocorrido, como também o instrumento através do qual as mudanças ocorrem. Nesse sentido, por seu protagonismo nas três décadas recentes, poder-se-ia também interpretar a Internet como uma nova forma de poder. É partindo de tal pressuposto que investigamos, a seguir, se a Internet pode ser interpretada de fato como forma de poder no sistema internacional.

1.4 Um novo instrumento de poder

Para chegarmos a uma definição de poder, recorremos a uma das obras políticas mais respeitadas na academia brasileira, o Dicionário de Política de Norberto Bobbio[18]. Segundo o autor, o poder é caracterizado por uma tríade composta por um indivíduo (A) que exerce o poder; uma fonte de poder através da qual o poder é exercido; e outro indivíduo (B), sobre o qual A exerce poder. O exercício do poder acontece, então, quando B tem seu comportamento alterado conforme o interesse de A.

O mesmo autor define, ainda, algumas características relacionadas ao conceito de poder, frente as quais, no quadro a seguir, buscamos inserir a Internet e analisar a possibilidade de correspondência com as características do poder.

Tabela 1 – Características do poder segundo Bobbio

Características do poder, segundo Bobbio:	**Internet:**
Pode ser *potencial*, quando não existe ação, mas suas consequências estão implícitas; ou *atual*, quando há ação de fato por parte de A, através utilização	Atualmente a Internet não é totalmente vista como poder em potencial, mas enquadra-se como poder atual quando se atenta para ataques, invasões,

[17] NYE, op. cit., p. 86.
[18]BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. **Dicionário de Política (A-Z)**. Brasília- UNB, 1998. Pp. 933-942.

do instrumento de poder.	espionagem e outros crimes já noticiados pela mídia internacional.[19]
Só existe de fato quando há, em B, expectativa ou previsão do que poderá ocorrer caso não aja conforme o interesse de A.	O reconhecimento do poder de outrem e previsão dos riscos que se correm podem ser comprovados pelas inúmeras estratégias adotadas visando à segurança *online*.[20]
Pode ser exercido de forma explícita ou implícita, desde que o comportamento de B resulte de certo interesse de A.	Uma vez que vários países destinam parte de suas reservas para realizar segurança preventiva antes mesmo de sofrer qualquer ataque, este tópico também caracteriza poder para a Internet.[21]
Não é eterno, ou seja, restringe-se a determinado período de tempo.	Os "crimes virtuais" costumam ser pontuais, de curta duração.[22]

Fontes: Portal Tecnologia da Informação e Comunicação; European Union Agency for Network and Information Security; International Business Times; Martin Libicki: Conquest in Cyberspace.

Nesse sentido, podemos ratificar a ideia de que a Internet é, de fato, uma nova forma de poder – em qualquer instância, dada a sua onipresença na vida contemporânea, inclusive no cenário internacional, em que inúmeros casos de demonstração de poder têm ocorrido.

Trazendo efetivamente o conceito de poder para o campo das Relações Internacionais, em junção à força e ao interesse, o poder forma a tríade pela qual o sistema internacional é regido – sistema esse que caracteriza-se pela ausência de isonomia, ou seja, não há igualdade de forças, poderes, nem interesses entre seus atores.[23]

---

[19] Top 13 dos ataques cibernéticos de 2014. Alcyon Junior. **Portal TIC**. Disponível em: <http://portaltic.com/84-alcyon-junior/496-top-13-dos-ataques-ciberneticos-de-2014.html>. Acesso em: 09 jun. 2015.

[20] National Cybersecurity Strategies in the World. **Enisa**. Disponível em: < https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>. Acesso em: 09 jun. 2015.

[21] US Investment in Cyber-security Equal to Nuclear Strategy. Edward Smith. International Business Times. Disponível em: <http://www.ibtimes.co.uk/cyber-security-nuclear-budget-china-attacks-congress-467232>. Acesso em: 09 jun. 2015.

[22] LIBICKI, Martin C. **Conquest in Cyberspace**. Nova Iorque: Cambridge University, 2007, p. 37.

[23] CASTRO, Thales Cavalcanti. **Elementos de Política Internacional**. Curitiba: Juruá, 2005. P. 53

Outrossim, dado seu recente surgimento, podemos inferir que, no contexto do presente trabalho, a Internet é considerada um novo instrumento de poder a ser exercido pelos atores no sistema internacional que, em nosso ponto de vista, poderia complementar a fórmula de cálculo de poder apresentada por Castro[24]:

$$P_1=\sum P_{pd}, P_{ef}, P_c, P_m, P_g.$$

Em que:

- P_{pd} representa o poder político-diplomático;
- P_{ef} representa o poder econômico-financeiro;
- P_c representa o poder cultural;
- P_m representa o poder militar;
- P_g representa o poder geodemográfico.

Nota-se que a Internet, se considerada como instrumento de poder, não consta na fórmula apresentada por Castro e nem poderia estar enquadrada em qualquer das formas de poder inclusas. Sob outras óticas, por exemplo, a Internet poderia não ser considerada poder, mas sim um recurso facilitador do poder militar, aéreo ou marítimo. Dessa forma, podemos considerar que a definição de poder, tanto de Castro quanto te outros autores, permanecem abertas a discussões e novas abordagens.

Como poderemos ver no tópico a seguir, as teorias das Relações Internacionais apresentam grande dinamismo e discussão teórica, uma vez que novos elementos – como a *web*, alteram constantemente a lógica de todo o sistema internacional. Nesse sentido, o próximo tópico faz um resumo de algumas das principais teorias das Relações Internacionais e busca aplicá-las aos fatos recentes relacionados aos conflitos cibernéticos.

1.5 Internet sob a ótica das Teorias das Relações Internacionais

1.5.1 O Realismo Clássico e o Neorrealismo

A busca de poder pelo homem e as consequências de sua aplicação são objetos de observação e dissertação de pensadores desde a Antiguidade Clássica, sendo

[24] CASTRO, op. cit., p. 58.

destacadas as contribuições de Tucídides (460 a.C – 395 a.C.) e de Nicolau Maquiavel (1469-1527). Mais adiante na História, Thomas Hobbes (1588-1679) teve contribuição fundamental para o entendimento mais profundo de poder e política, quando, em sua obra *O Leviatã* (1651), assinalou que o homem é possuidor de um *estado de natureza*, que teria como base o medo da morte precoce devido a ação alheia, a busca constante pelo prestígio através do poder e a ambição.

Tal premissa é considerada por muitos como o marco definitivo para o estudo da política e das Relações Internacionais, dada a explicação contundente do conceito de Estado e razão de sua criação. Segundo Hobbes, os diferentes interesses colocariam os homens em constante conflito e, a fim de prevenir a morte precoce, o conceito de Estado surgira, através de um contrato social, como meio de impor regras e garantir a segurança da população. Ainda de acordo com o mesmo autor, em sua obra supracitada, as ações estatais seriam reflexo do próprio estado de natureza do homem; porém, no âmbito internacional, diferentemente do que ocorre em escopo nacional, não haveria qualquer tipo de sistema de coerção que garantisse a segurança das unidades nacionais.[25]

A ideia de que o Estado teria como fim principal a garantia de segurança de sua população, seja por meio da harmonização interna ou da prevenção de ataques externos, e o conceito de que o sistema internacional é anárquico são as premissas fundamentais do Realismo, teoria clássica do estudo das Relações Internacionais.

João Pontes Nogueira e Nizar Messari resumem as ideias centrais desses pensadores:

> Portanto, a leitura que os realistas fazem destes três pensadores, Tucídides, Maquiavel e Hobbes, destaca os elementos de sobrevivência, poder, medo e anarquia internacional que representam as premissas centrais do realismo nas Relações Internacionais. (NOGUEIRA; MESSARI, 2005, p. 23)

Os mesmos autores esclarecem, na mesma obra, o significado da chamada *anarquia internacional*: "O que se entende por anarquia não seria propriamente o caos, mas sim a ausência de uma autoridade suprema, legítima e indiscutível que possa ditar as regras, interpretá-las, implementá-las e castigar quem não as obedece."[26]

No contexto de anarquia internacional, o Estado estaria isento de moralidade e seu papel seria basicamente o de garantir segurança para seu povo, sendo todos os

[25] NOGUEIRA, João Pontes; MESSARI, Nizar. **Teoria das Relações Internacionais.** Rio de Janeiro-Elsevier, 2005. P. 24.
[26] Ibidem, p. 26

outros interesses – bem-estar, liberdade, ou prosperidade, secundários. Visando a garantir segurança no cenário internacional, os Estados, então, estariam em constante busca de poder.[27]

Séculos mais tarde, o Realismo ganhou força no século XX com as contribuições de teóricos como Hans Morgenthau (1904-1980) e Kenneth Waltz (1924-2013). Esses autores resgatam o antigo conceito realista de *Balança de Poder*, argumento que justifica que "o poder é central. Atores se juntam ao poder ou se juntam contra o poder"[28]. Tal balança, que, segundo Kenneth Waltz pode ser bipolar ou multipolar, mas nunca unipolar[29], levaria à redução de conflitos, uma vez que os Estados temeriam o confronto com um conjunto forte de países. Segundo Morgenthau, "só o poder limita o poder"[30].

Além de estabelecer pontos chaves do Realismo ao retomar pensamentos de autores clássicos, Morgenthau contribui com a ideia de que, a política pode ter por objetivo manter o poder (status quo), aumentar o poder (expansão) ou demonstrar o poder (prestígio) – complementando o que se havia sido dito por teóricos anteriores. O sucesso de um Estado seria alcançado no cenário internacional a partir de quando seu prestígio fosse suficiente para que outros Estados se sentissem ameaçados e cedessem ao primeiro, tornando o uso da força desnecessário[31].

Apesar de ter enfrentado crise teórica na década de 1970 (a ser detalhada no tópico seguinte), o Realismo conseguiu ser reinventado através do Neorrealismo, ao constatar que, apesar do surgimento de novos atores e organismos supranacionais, como a Organização das Nações Unidas e o Tribunal Penal Internacional, e sua autonomia, a guerra e a anarquia internacional continuavam presentes nas relações entre os Estados. Entre os autores do chamado Neorrealismo, destaca-se novamente Kenneth Waltz, que afirmou em sua obra *Teoria da Política Internacional* (1979), que "a anarquia internacional, premissa básica do Realismo, responde à pergunta central das relações internacionais: o porquê de sempre ter havido guerra"[32]. Apesar de todas as mudanças do final do século XX, os Estados Nacionais continuavam em estado permanente de desconfiança e insegurança.

---

[27] NOGUEIRA; MESSARI, op. cit., p. 49
[28]Ibidem, p. 29.
[29]NOGUEIRA;MESSARI apud WALTZ, Kennedy. **Theory of International Politics**. Nova York-Mac Graw Hill, 1979, p.18.
[30] NOGUEIRA; MESSARI, op. cit., p.30
[31] Ibidem, p.35
[32] NOGUEIRA; MESSARI apud WALTZ, op. cit., p. 118.

O Realismo foi positivamente reconhecido durante vários séculos por explicar de forma coerente os fenômenos históricos que haviam ocorrido no passado. Durante todos esses séculos, indivíduos e Estados, por inúmeras vezes, entraram em conflito ao defender seus próprios interesses. Guerras eram, em sua maioria, iniciadas objetivando a conquista de poder – através de territórios ou recursos diversos, e eram finalizadas pela demonstração de maior poder da parte vencedora.

Nesse sentido, o Realismo, apesar da crise que enfrentou na década de 1970 e que culminou com a transição para o Neorrealismo, mostra-se atual e bem sucedido ao notarmos que a Internet é um dos principais instrumentos de poder exercidos na contemporaneidade. Indo mais além, o Neorrealismo é coerente à este trabalho ao analisarmos que, apesar de tamanho impacto que pode causar nas mais diversas esferas, a Internet ainda não conta com nenhuma legislação internacional que limite seu uso através da coerção. Sendo assim, apesar de a segurança cibernética estar frequentemente presente nas agendas internacionais, ainda falta autoridade suprema capaz ditar regras e implementá-las. Chegamos, então, à premissa clássica do Realismo e do Neorrealismo: a anarquia internacional, ainda presente no cenário internacional contemporâneo.

1.5.2 Novas abordagens: Interdependência Complexa e Soft Power

A criação do que podemos chamar hoje de Internet na década de 1970, assim como fatos históricos da década – a saber, a internacionalização do sistema financeiro, a formação do cartel da OPEP (Organização dos Países Exportadores de Petróleo), a desvalorização do dólar e a primeira crise nos Estados Unidos enquanto superpotência – levou o Realismo a uma crise de credibilidade. O surgimento de novos atores, como as organizações governamentais e multinacionais com grande força econômica, política e tecnológica, contradiziam à ideia realista de que os Estados eram os únicos atores relevantes no cenário internacional.

Nesse contexto, destaca-se um importante autor do estudo moderno das Relações Internacionais: o estadunidense Joseph Nye (1937). Nye iniciou sua contribuição mais relevante para as teorias das relações entre os Estados quando criou, juntamente com o também estadunidense Robert Keohane (1941) o conceito que ficou conhecido como *Interdependência Complexa* (Poder e Interdependência, 1977).

Tal teoria consistia em afirmar que atores não-estatais estavam, cada vez mais, tomando decisões relevantes em investimentos, tecnologias, mídia etc, o que

enfraqueceria o poder absoluto dos Estados e tornaria o mundo cada vez mais interdependente. Para esses observadores, os novos atores deveriam ser inclusos nos estudos de poder.

Nogueira e Messari nos ajudam a compreender melhor a definição de Interdependência:

> [..]Interdependência, na definição de Keohane e Nye, deve ser entendida como uma relação entre dois (ou mais) países na qual processos e decisões tomadas em cada um têm efeitos recíprocos, ou seja, atingem de alguma forma suas respectivas economias e sociedades. (NOGUEIRA; MESSARI, 2005, p. 83)

Nesse novo contexto de interdependência econômica, política e tecnológica, os Estados perdem os referenciais clássicos de poder que haviam sido antes colocados como fórmula matemática para atingir maior segurança. Esse novo contexto da sociedade internacional, tendo a Internet como um de seus protagonistas, tornou o poder mais difuso entre os atores transnacionais e reduziu relativamente as disparidades de poder entre eles – ainda que os Estados ainda possuam mais poder quando comparado aos outros atores.[33]

Essa teoria faz sentido quando nos deparamos com a realidade mencionada no início do capítulo, em que Estados muito poderosos, como os Estados Unidos da América, superpotência atual, têm seu sistema de defesa atingido por hackers no escândalo do Wikileaks.

Mais adiante, Nye observou que, além da difusão de poder e maior força dos novos atores, a própria forma de poder já não era mais a mesma, sendo essa a premissa para a criação do conceito de *Soft Power*[34]. Segue definição, extraída de livro mais recente, *O Futuro do Poder*.

> Fully defined, soft power is the ability to affect others through the co-optive means of framing the agenda, persuading and eliciting positive attraction in order to obtain preferred outcomes. (NYE, 2011, p. 44)

Em contraponto ao *Soft Power*, Nye conceitua o *Hard Power*, que seria a habilidade de conseguir resultados desejáveis através da coerção e punição[35]. Nesse sentido, no ponto de vista de Nye, se um ator tivesse de escolher entre *soft* e *hard*

[33] NYE JR., Joseph Samuel. **The Future of Power**. Nova Iorque: Public Affaris, 2011. p. 64.
[34] Idem apud NYE JR., Joseph S. **Soft Power: The Means To Success In World Politics**. Public Affaris, 2004
[35] NYE JR., op. cit, p.38

power, o *hard power* certamente seria a opção mais certeira[36]. No entanto, a forma ideal de poder a ser buscada por um Estado contemporaneamente seria o que chamou de *Smart Power*, conceito criado apenas em 2004, cuja definição seria "[..] the combination of hard power of coercion and payment with the soft power of persuasion and attraction" (NYE, 2011, p. 16).

Cabe-nos entender que a criação da Internet corresponde a ambos os conceitos de *soft power* e *hard power*, na medida em que pode ser instrumento de ataque direto (como no estudo de caso a ser apresentado adiante), mas também um instrumento com potencial de ser utilizado para propagação de ideias. Nye reconhece a relevância do poder da Internet (*cyberpower*) em sua obra, dedicando um capítulo inteiro a esse tema (capítulo 5 – *Diffusion and Cyberpower*, O Futuro do Poder, 2011). No mesmo capítulo[37], o autor apresenta alguns exemplos quando se refere a possibilidades de um ator exercer o poder virtual, dividindo-o em *soft* e *hard power*.

Como exemplos de *hard power* no espaço virtual, Nye cita ataques a Sistemas de Supervisão e Aquisição de Dados (SCADA), assim como o uso de roteadores de bombas e corte de cabos de transmissão de dados. Em contrapartida, os meios de utilização de *soft power* dentro do domínio virtual poderiam ser a criação de softwares para ajudas ativistas pelos direitos humanos ou campanhas diplomáticas públicas para influenciar a opinião pública.[38]

Com a Teoria da Interdependência Complexa e os conceitos de *Soft Power*, *Hard Power* e *Smart Power*, Joseph Nye tem ganhando reconhecimento global como principal observador contemporâneo para os fenômenos de poder no que se refere às relações entre atores internacionais. Sua contribuição nos ajuda a compreender de forma mais clara os movimentos políticos mais recentes do planeta, cuja velocidade do surgimento de novas tecnologias e disseminação da informação impressiona dia após dia.

[36] NYE JR., op. cit., p.48
[37] Ibidem, p. 173
[38] Ibidem, p. 173

CAPÍTULO 2 - Ataques Cibernéticos Internacionais: uma Nova Ameaça à Segurança Estatal

2.1 – Os conflitos internacionais

O estudo dos conflitos entre povos é um dos temas centrais das Relações Internacionais, uma vez que, conforme mencionado no capítulo anterior, a segurança tende a ser busca prioritária dos Estados; e estes, juntamente aos outros atores internacionais, são tradicionalmente regidos pela tríade força-poder-interesse[39], tendo suas ações sempre guiadas pelo viés racional, a despeito de valores ou julgamentos morais. Por tradição, a forma primária pela qual os Estados agem visando ao alcance de seus interesses (entre eles a defesa de seu território) é a diplomacia. No entanto, quando contrariados, tais interesses tendem a ser defendidos através do uso da força – levando aos conflitos internacionais, majoritariamente guerras, em que, ao final, apenas um de seus participantes tende a ser vencedor.

Ao longo da história, as guerras caracterizam-se como forma clássica de conflito internacional, sendo bastante conhecidas e estudadas. Resquícios de guerras estão presentes nos mais primitivos registros históricos e, portanto, os fenômenos bélicos confundem-se com o desenvolvimento da tecnologia: as guerras passaram a ter características diferentes devido às novas tecnologias, assim como novas tecnologias foram criadas sob origem dos esforços de guerra.

Ironicamente, foi no contexto da Segunda Grande Guerra, considerada a mais destruidora da História em relação a número de mortos, que surgiram os estudos antecedentes do que viria a ser chamado de *cibernética*, devido a esforços para o desenvolvimento de máquinas ordenadoras e com mecanismos de controle para artilharia aérea.[40]

Assim como ocorre com a tecnologia, o acesso e o domínio da informação foi e ainda é fator determinante em todas as guerras e outros tipos de conflitos internacionais da história. A informação é fator fundamental para tomadas de decisões e consequente estabelecimento de estratégias no momento e no lugar certo visando à submissão do inimigo. No entanto, se levarmos em consideração a guerra como principal conflito internacional ao longo dos séculos, anteriormente a informação era apenas um meio

[39]CASTRO, Thales Cavalcanti. **Elementos de Política Internacional**. Curitiba: Juruá, 2005. P. 53.
[40]KIM, op. cit.

para que se chegasse a ações posteriores de combate e enfraquecimento de outro combatente, enquanto, hoje, podemos dizer que o acesso à informação e os ataques *online* que temos presenciado nos últimos anos são o fim em si mesmo dos conflitos. Nesse sentido, paralelamente ao surgimento recente dos termos definidos no Capítulo 1 deste trabalho, tais como infosfera, ciberespaço e poder cibernético, nas últimas décadas, com intenção de caracterizar os conflitos internacionais que ocorrem dentro e a partir do ciberespaço, surgiu também o conceito de *guerra cibernética*, que, apesar das inúmeras controvérsias em torno de sua nomenclatura, relaciona-se aos diversos conflitos cibernéticos internacionais que são contemporaneamente noticiados.

2.1.1 – O termo "Guerra Cibernética"

Segundo Sheldon[41], a guerra cibernética ou o conflito cibernético seria "uma gama de atividades abomináveis que acontecem no ciberespaço todos os dias". Tais atividades podem ser extremamente variadas em sua natureza, sendo as mais comuns os ataques de hackers[42] tendo como motivação o que o autor chama de "hacktivismo" (tradução nossa), uma forma de protesto e divergência política online, espionagem ou até atividades que corresponderiam a crimes no mundo real, como o roubo, por exemplo.

Em seu artigo, Sheldon questiona se de fato tais ataques caracterizariam uma guerra – os clássicos conflitos armados com grande derramamento de sangue, alto número de mortos e consequências desastrosas que durariam décadas, conforme estamos acostumados a ler em livros de História. Sheldon afirma que pouquíssimos dos ataques virtuais podem ser considerados realmente sérios, a ponto de causar danos significativos à segurança nacional de um Estado.

Outros autores discordam, no entanto, ao afirmar que o surgimento do ciberespaço mudou as características da guerra de maneira significativa, transformando em um novo conceito de guerra qualquer incidente cibernético conduzido por um ator, seja ele indivíduo, organização ou governo, contra um Estado ou sua sociedade ou economia, de modo a coagir aquele alvo e sujeitá-lo a seu objetivo político[43].

---

[41] SHELDON, op. cit., p. 307.
[42] Hacker ou ciberpirata é a pessoa com com profundos conhecimentos de informática que eventualmente os utiliza para violar sistemas ou exercer outras atividades ilegais; pirata eletrônico.
[43] Ibidem, p. 308.

Partindo do princípio de que o poder cibernético seria um instrumento a ser usado como estratégia para o alcance de determinado objetivo político, Sheldon propõe que seja talvez mais adequado falar em "poder cibernético em guerra" ou "guerra por meios cibernéticos", ao invés do, segundo ele, "ilusório termo *guerra cibernética*"[44].

Dado o surgimento recente de tudo aquilo que se refere à cibernética, podemos dizer que tanto os conceitos de ciberespaço e poder cibernético, como também o conceito de guerra cibernética estão ainda em estado embrionário, em processo de amadurecimento conforme a tecnologia toma cada vez mais espaço em nossas vidas. Por esse motivo, convém esclarecer neste início de capítulo que o termo "guerra cibernética", apesar de seu uso constante, continua a ser questionado por diversos acadêmicos e não nos cabe, neste trabalho, trazer um veredicto se os conflitos virtuais devem, ou não, serem classificados como uma nova forma de guerra no sistema internacional. O que pretendemos no presente capítulo é, portanto, sistematizar os tão recentes conflitos cibernéticos, sem maiores preocupações com sua epistemologia.

2.2 – Ataques cibernéticos internacionais

2.2.1 –Precedentes

É quase unanimidade entre acadêmicos contemporâneos a ideia de que os conflitos cibernéticos só puderam ocorrer e serem tão popularizados a partir de certas características básicas da cibernética, que podem ser interpretadas como a origem ou as causas para o surgimento dos conflitos. Nesse sentido, antes que possamos entender como os conflitos cibernéticos acontecem e quais são os atores que os operacionalizam, precisamos entender a base de seu surgimento, a partir da análise de algumas das características do ciberespaço e do poder cibernético que foram definidas sistematicamente por Sheldon[45], mas também presentes em outras literaturas importantes quando se trata dos conflitos cibernéticos, como *The Future of Power*[46], já citada anteriormente, e *Cyberwar, Netwar and the Revolution in Military Affairs*[47].

[44] SHELDON, op. cit., p. 308.
[45]Ibidem, p. 208
[46] NYE JR., op. cit.
[47]HALPIN, Edward; TREVORROW, Philippa; WEBB, David; WRIGHT, Steve. (Ed.). **Cyberwar, Netwar and the Revolution in Military Affairs.** Nova Iorque: Palgrave McMillan, 2006.

Sendo assim, tais são as características do ciberespaço que formam a base para os ataques cibernéticos:

- Baixo custo de entrada: os recursos e o conhecimento necessários para entrar e explorar o ciberespaço são extremamente modestos quando comparados aos custos e ao conhecimento necessários para explorar terra, ar, mar ou espaço;
- Múltiplos atores: o baixo custo de entrada leva ao aumento da quantidade e variedade de atores capazes de operar no ciberespaço e potencialmente gerar efeitos estratégicos. Indivíduos, organizações e atores não-estatais, assim como os próprios Estados, participam no ciberespaço;
- O ciberespaço se baseia no espectro eletromagnético: o espectro eletromagnético é o fator que possibilita que milhões de informações e tecnologias sejam capazes de comunicar-se entre si de maneira extremamente rápida;
- O ciberespaço pode ser constantemente replicado: não existe fim dentro do ciberespaço. Ao contrário do que acontece em terra, ar ou espaço, no ciberespaço a matéria não consegue ser completamente destruída; ela é constantemente reconstituída e replicada;
- O ciberespaço é quase instantâneo: a informação atravessa o ciberespaço em uma velocidade através da qual as informações podem ser movidas em qualquer parte da rede, a qualquer tempo.

Além das características do ciberespaço acima listadas, há também uma característica importante do poder cibernético que facilitou o surgimento dos ataques cibernéticos: a dissimulação, ou seja, os conflitos podem ocorrer sem que o criminoso corra grandes riscos de ser descoberto e condenado.

Dessa forma, podemos inferir que, dentre todas as características do ciberespaço e do poder cibernético, a "porta de entrada" para a chamada Revolução da Informação e, posteriormente, para os ataques cibernéticos em escala internacional, seria o baixo custo e o pouco conhecimento técnico necessário para inserção e atuação no domínio cibernético. Naturalmente, a principal consequência disso foi a emergência de diversos outros atores, que não apenas os Estados, no cenário internacional.

2.2.2 – Atores

No novo sistema internacional pós-Internet, há uma vasta gama de novos atores, que aqui ficarão restritos aos que diretamente desempenham ataques cibernéticos a Estados ou grandes instituições. No livro *Cyberwar, Netwar and the Revolution in Military Affairs*[48], seus editores descrevem os diversos tipos de *hackers*, como são popularmente conhecidos os atores diretamente responsáveis pelos ataques cibernéticos contemporaneamente.

O primeiro grupo seria o dos *hackers* amadores, pessoas que passam horas em frente à tela do computador invadindo sistemas eletrônicos sem nenhuma intenção explícita de malevolência, mas motivados pelo puro prazer pessoal de desafiarem os sistemas cibernéticos de segurança.

O segundo grupo incluiria *hackers* profissionais, que, geralmente motivados por interesses pecuniários, estariam envolvidos em casos de espionagem industrial, econômica ou corporativa. De acordo com os autores, esse grupo pode representar ameaça significativa a organizações.

O terceiro grupo consiste em *hackers* que agem individualmente ou dentro de organizações, tendo como alvo, por exemplo, o acesso a informações financeira de outras instituições. Também motivados por pecúnia, esses criminosos poderiam agir, por exemplo, conforme o interesse de certas empresas em descobrir segredos de comércio de seus competidores.

Finalmente, há também os *hackers* motivados por questões políticas, que vão desde entidades governamentais, como agências de inteligência ou unidades militares, até a grupos terroristas. Seus objetivos podem incluir coleta de informações, propaganda, vigilância, censura e sabotagem.

Sobre esse último grupo, também conhecido como *ciberativistas*, Nye observa que:

> Muitos desses atores transnacionais afirmam agir como uma "consciência global" representando interesses públicos amplos, além do alcance dos Estados individuais. Apesar de não terem sido eleitos democraticamente, esses atores às vezes ajudam a desenvolver novas normas diretamente por pressionar governos e líderes de negócios a mudar políticas e, indiretamente, por alterar as percepções públicas de legitimidade e do que governos e empresas deveriam estar fazendo. Em termos de recursos de poder, esses grupos raramente possuem muito *hard power*[49], mas a Revolução da

[48] HALPIN; TREVORROW; WEBB; WRIGHT, op. cit.
[49] NYE JR., op. cit., apud NYE JR., Joseph S. **Soft Power: The Means To Success In World Politics**. Public Affaris, 2004.

> Informação evidenciou seu *soft power*. Eles podem levantar campanhas pautadas em "nomear e envergonhar" marcas corporativas ou governos de forma relativamente fácil. (NYE, 2011, p. 88) (Tradução nossa).

Conhecidos os principais atores que, pela posse de poder cibernético, desempenham exercício direto dos ataques dentro do ciberespaço, no próximo tópico descreveremos a natureza das ações que caracterizam os ataques cibernéticos.

2.2.3 – Alvo: informação

Conforme podemos constatar ao longo do presente trabalho, os fenômenos ligados à cibernética, ainda que velozes, acontecem de maneira processual – ou seja, cada transformação tecnológica abre espaço para que outra transformação ocorra, para que outro fenômeno surja. No que se refere aos ataques cibernéticos, esse paradigma também é válido.

Sucedendo o surgimento da cibernética e o desenvolvimento da Internet, a Revolução da Informação mudou exponencialmente a maneira como os homens comunicam-se em todas as instâncias de suas vidas, até mesmo no que concerne a conflitos entre si ou entre nações.

No entanto, mesmo com seu aparente ineditismo, os ataques cibernéticos internacionais são comumente enquadrados no que é chamado por diversos autores de *Guerra da Informação*. Libicki insere os ataques cibernéticos como parte da Guerra da Informação quando afirma que "a conquista hostil do ciberespaço é um aspecto da Guerra da Informação que, por sua vez, pode ser definida como o uso de informação para atacar informação"[50]. Voltando ao conceito básico de que a Internet consiste em uma rede de computadores interligados, conforme mencionado no capítulo anterior deste trabalho, inferimos que tal interligação refere-se à troca de informações que ocorre hoje em todo o mundo e a todo momento. Dessa forma, infere-se que todo e qualquer ataque que ocorre dentro do domínio cibernético ou através dele, está ligado a informação.

Baseando-se em tal assertiva, Libicki[51] desenvolve umas das principais contribuições quando se trata de Guerra da Informação. Como forma de sistematizar os

[50]LIBICKI, op. cit., p. 49.
[51]Ibidem, p. 24

tipos de informações existentes no ciberespaço e como elas podem ser atacadas, o autor divide o ciberespaço em três camadas distintas:

a) A camada física, que consiste nos vários meios que permitem a circulação de bits. Isto é, esta camada equivaleria ao que conhecemos como *hardware*, a aparelhagem dos computadores e outras máquinas com conexão à internet.
b) A camada sintática, correspondendo às várias instruções e comandos que usamos para dizer aos sistemas de informação o que fazer com a informação. É geralmente nesta camada que ocorrem os ataques dos *hackers*.
c) A camada semântica, que corresponde ao conteúdo das informações de um sistema. Essas informações podem ser armazenadas (por exemplo, em bancos de dados) ou circuladas (como em mensagens). [52]

Partindo da premissa de que o propósito da informação é guiar as decisões tomadas pelos autores – com exceção dos que a usam para fins de entretenimento, os ataques cibernéticos têm como objetivo principal confundir a tomada de decisões de seus alvos, ou de máquinas a eles pertencentes, para o benefício de interesses próprios. Tal confusão entre informações pode dar-se por meio de diversas formas, destacando-se decisões erradas, decisões atrasadas ou decisões que, por mais que possam ser benéficas para o inimigo, também tendem a ser benéficas para quem o ataca. [53]

Quanto à informação em si, esta pode ser destruída ou degradada de muitas maneiras, como sendo roubada, apagada, deslocada ou até tornar-se difícil de ser encontrada. Ademais, informações desnecessárias podem ser adicionadas a informações relevantes, de modo a confundir os tomadores de decisões – sendo chamados de *codemakers* os hackers especialistas desse tipo de ação.[54]

Finalmente, além de todos esses fatores, mesmo que a informação não seja alterada, a maneira que ela afeta a tomada de decisões por ser influenciada devido à mudança da credibilidade com que ela é recebida; por exemplo, pessoas podem ser induzidas a dar a certas ações mais credibilidade do que merecem.[55]

No que concerne ao processo dos ataques cibernéticos, observa-se um padrão: geralmente inicia-se através de um mapeamento detalhado da rede do alvo; coleta de

[52] LIBICKI,op. cit., pp. 22-23
[53] Ibidem, p. 20
[54] Ibidem, p. 12; 28
[55] Ibidem, p. 21

dados em dispositivos da rede para executar uma análise de vulnerabilidade. Em seguida, a arma apropriada é lançada, o que não necessariamente implica em sua ativação – que pode ocorrer mais tarde, em momento determinado pela programação do hacker através de condições lógicas ou outro comando específico. Em certos casos, um teste de reação pode ser feito previamente, para averiguar as capacidades de defesa do sistema atacado[56].

A quantidade de ataques cibernéticos a atores internacionais depende, primordialmente, do quão vulneráveis eles são. Nesse quesito, há uma certa ironia no ciberespaço: quanto mais avançado é um país em termos de Tecnologia da Informação, mais dependente ele é das infraestruturas de comunicação e, consequentemente, mais vulnerável a ataques cibernéticos. É o caso dos Estados Unidos, por exemplo, que é, ao mesmo tempo, berço da Internet e alvo da maior quantidade de ataques online.[57]

No que concerne à duração e à intensidade dos ataques *online*, autores como Libicki fazem uma comparação entre os conflitos realizados no ciberespaço e aqueles realizados em terra, mar, ar ou espaço. Este assinala que, enquanto os conflitos de outras naturezas deixam consequências indeterminadas e a longo prazo, os resultados dos conflitos cibernéticos são por duração limitada, podendo inclusive serem restaurados em até quarenta e oito horas; contudo, não há nada que prove que seus efeitos também sejam limitados em grau.[58]

2.2.4 –Relevância e reconhecimento

Dada a importância dos conflitos cibernéticos no que tange ao número crescente de casos e incessante surpresa mundial ao constatar quão vulneráveis os Estados estão em termos de segurança cibernética, algumas medidas tomadas por superpotências mundiais nos mostram que já há atenção das autoridades para a gravidade desses conflitos – mesmo que ainda não haja nenhuma medida coercitiva efetiva para impedi-los.

Os Estados Unidos, um dos principais países atacados, já observam a ameaça dos conflitos cibernéticos desde a década de 1990. Em janeiro de 1995, o secretário de defesa dos Estados Unidos criou o Corpo Executivo da Guerra da Informação ‘para

[56]HALPIN; TREVORROW; WEBB; WRIGHT, op. cit., p. 42.
[57]NYE JR., op. cit., p. 204.
[58]LIBICKI, op. cit., p. 42

desenvolver e alcançar metas nacionais relacionadas à Guerra da Informação'. No ano seguinte, em julho de 1996, foi criada a Comissão Presidencial Para Proteção da Infraestrutura Crítica (PCCIP), tendo como objetivo a avaliação de 'ameaças físicas e cibernéticas para infraestrutura vital nacional' e o desenvolvimento de 'estratégias para protegê-la'. No mesmo ano, foi criado o Centro de Proteção da Infraestrutura Nacional com a intenção de 'aumentar a coordenação da proteção da infraestrutura'. Já no final da década, em 1998, foram criadas duas agências: o Centro de Proteção da Infraestrutura Nacional (NIPC), que responde ao FBI, e o Escritório para Garantia da Infraestrutura Crítica, pertencente ao Departamento de Comércio[59].

Na mesma época, James Adam afirmou em edição da publicação *Foreign Affairs* que: "A Guerra da Informação representa um risco estratégico de derrota militar e perdas econômicas catastróficas e é uma das maiores ameaças que esta nação encara no final deste século".[60]

Em meados da década seguinte, o empenho dos Estados Unidos em compreender e defender-se de ataques cibernéticos continuou. Em 2005, a CIA conduziu uma simulação de guerra com o intuito praticar a defesa contra uma possível tentativa de agressão eletrônica na mesma escala dos ataques de 11 de setembro e para testar a habilidade do governo e da indústria em responder aos crescentes ataques no domínio cibernético.[61]

Também a Europa demonstrou reconhecer a relevância dos ataques cibernéticos já na década de 1990. Em 1997 e 1998 quatro seminários foram realizados em colaboração com industriais, acadêmicos e autoridades públicas que culminaram com o estabelecimento da Iniciativa de Segurança Europeia dentro do Programa de Tecnologias de Sociedades da Informação (IST), órgão regido pelo Diretório Geral da Sociedade da Informação da Comissão Europeia. O objetivo proposto foi o levantamento de questões de confiabilidade em sistemas e serviços, tratando da segurança e de novas vulnerabilidades.[62]

No escopo transnacional, as Nações Unidas também reconheceram a importância da discussão sobre a segurança cibernética no cenário internacional. Em dezembro de 1998, a Assembleia Geral lançou sua Resolução 53/70, que trata da segurança dos sistemas de telecomunicações e informações globais e promove a

[59]HALPIN; TREVORROW; WEBB; WRIGHT, op. cit., p. 33.
[60] LIBICKI, op. cit., p. 38
[61] LIBICKI, op. cit., p. 45.
[62] HALPIN; TREVORROW; WEBB; WRIGHT, op. cit., p. 34.

consideração das potenciais ameaças existentes no campo da segurança da informação. Em 1999, duas agências da ONU – o Departamento para Assuntos de Desarmamento (DDA) e o Instituto para Pesquisa de Desarmamento (UNIDIR) – organizaram, pela primeira vez no contexto das Nações Unidas, uma reunião para discutir 'desenvolvimentos no campo da informação e telecomunicações no contexto na segurança internacional'. No mesmo ano, uma segunda resolução (54/49), baseada no número de visualizações e acessos de certa quantidade de países, convidou estados-membros a definirem noções básicas relacionadas à segurança da informação e a desenvolver princípios internacionais a fim de aumentar a segurança da informação global e dos sistemas de telecomunicações. Desde então, outras resoluções foram adotadas pela Assembleia Geral (55/28, 56/19, 57/53, 58/199), o que indica interesse crescente em relação a este assunto dentro da Organização das Nações Unidas.[63]

2.3 – Respostas a curto, médio e longo prazo

Partindo do pressuposto de que a Internet, enquanto novo instrumento de poder, é uma arma extremamente difusa na contemporaneidade, podendo ser utilizada por atores individuais, corporações ou Estados, a premissa a que se chega quando se trata de segurança cibernética é o de que não há possibilidade de impedimento de ataques – seja em razão de sua grande quantidade ou pelo fato de que a identificação das identidades e das motivações de seus autores é bastante improvável[64]. Mais além neste tópico, mesmo em casos em que, de forma bem-sucedida, os ataques são identificados, não há leis claras para coerção de seus autores, especialmente quando se tratam indivíduos[65].

Dessa forma, as melhores soluções para o futuro da segurança dos sistemas de informação é pauta de divergência entre vários acadêmicos. Parte deles propõem soluções focadas nos sistemas de defesa, isto é, propõem ações tomadas por usuários e voltadas para a diminuição de sua vulnerabilidade. Outro grupo, porém, aponta soluções visando a coibir os ataques cibernéticos, o que, de uma forma ou de outra, está alinhado com a criação de órgãos e instrumentos internacionais de coerção. Veremos então, as propostas apresentadas por autores de obras importantes no que concerne à segurança cibernética internacional.

---

[63] HALPIN; TREVORROW; WEBB; WRIGHT, op. cit., p. 35
[64] SHELDON, op. cit., p. 313.
[65] NYE JR., op. cit., p. 107.

Para Libicki[66], por exemplo, as soluções devem voltar-se para a defesa dos sistemas de informação, mais do que para armas informacionais propriamente ditas. De acordo com ele, o início da defesa cibernética estaria baseada em: controle de acesso - a maioria dos sistemas usa senhas, mas a criptografia seria muito mais resistente a ataques; habilidade de separar mensagens benignas de malignas entre os componentes de um sistema; e habilidade de exploração da propriedade física para assegurar sistemas virtuais: assinaturas digitais, em particular, podem assumir bem um papel crescente em proteção de sistemas.[67]

Nye, por sua vez, remete a ideias de especialistas de que a solução a longo-prazo seria uma espécie de reengenharia da Internet que tornasse os ataques virtuais mais difíceis de operacionalizar do que são sob a estrutura atual, que, segundo o autor, enfatiza a facilidade do uso em detrimento da segurança. Uma das formas para que isso acontecesse, por exemplo, seria através da redução da conectividade com a Internet para determinados setores da sociedade; ou até mesmo que certas instituições privadas com infraestruturas críticas (por exemplo, finanças e eletricidade) pudessem utilizar sistemas seguros em vez de confiar na Internet aberta[68].

Entretanto, considerando a grande difusão da Internet e da proveniência de seus ataques, até mesmo o mais seguro dos sistemas eletrônicos não seria capaz de impedir ataques cibernéticos. Por isso, diversos outros observadores da segurança cibernética, defendem o foco não em sistemas eletrônicos de defesa, mas na coerção dos ataques. Entre eles, há um ponto em comum constantemente apresentado: a discussão sobre uma legislação que pudesse ser aplicada em âmbito global. Sobre essa questão, o próprio Nye observa o estado embrionário da atual governança cibernética internacional ao comparar o domínio cibernético, o ciberespaço, com o domínio marítimo: enquanto o alto mar consistiria em um espaço dividido entre vários países e com fronteiras bem definidas, o ciberespaço atualmente seria como um condomínio de propriedade geral, sem regras bem desenvolvidas[69].

No entanto, Nye ainda observa que a governança pode, futuramente, assim como acontece com o oceano, vir a ser baseada em fronteiras geográficas. O autor assinala que a infraestrutura física da Internet permanece ligada à geografia e os governos são soberanos sobre espaços geográficos – como pode-se observar pelo controle de acesso a

[66] LIBICKI, op. cit., p. 40.
[67] LIBICKI, op. cit., p. 33
[68] NYE JR., op. cit., p. 107
[69] NYE JR., p. 105

websites imposto por alguns governos e corporações, com base nos IPs[70] de usuários de determinada localidade[71].

Em busca de soluções, a obra *Cyberwar, Netwar and the Revolution in Military Affairs*, já mencionada anteriormente no presente trabalho, seus editores apontam estratégias a curto, médio e longo prazo para o desenvolvimento da segurança cibernética.

A curto prazo, então, a primeira estratégia seria distinguir, independentemente da repercussão da mídia, os eventos acidentais de ataques reais ligados à Internet e, em seguida, rastrear a origem de tais ataques. A médio prazo, aplicar-se-ia o desenvolvimento de ferramentas sofisticadas e sistemas mais robustos podem reduzir a vulnerabilidade encontrada na contemporaneidade[72].

A longo prazo, dada a natureza transnacional do problema, seria inevitável o estabelecimento, em acordo mútuo, de normas internacionais claras no que diz respeito às ações realizadas no domínio cibernético. Já as fases de julgamento e punição poderiam ficar a cargo de entidades transnacionais já existentes e respeitadas, como a Organização das Nações Unidas, a Corte Internacional de Justiça, o G8 ou o G20[73].

Além de tais medidas voltadas ao direito internacional, os autores sugerem que a cooperação internacional seja fomentada em vários níveis[74]. Nesse sentido, governos e instituições privadas deveriam reunir-se para chegar ao entendimento de quais seriam as responsabilidade claras de cada setor – se seriam públicas, privadas ou compartilhadas, para, em seguida, compreender de que setor é esperada determinada ação. Nesse contexto, os próximos passos seriam referentes à coordenação, partindo dos governos, de parcerias público-privadas visando à segurança cibernética global[75].

Independentemente das divergências de ideias que objetivam solução no que tange aos ataques cibernéticos, e apesar de alguns países já contarem com leis nacionais para regulamentação da Internet, não há registros de ações sólidas na sociedade internacional que tenha como intuito a regulamentação no domínio cibernético. Contudo, como podemos constatar através de referências apresentadas neste capítulo, já há sinais do despertar de autoridades e outros tomadores de decisões do cenário

[70]O Internet Protocol (IP), ou Protocolo de Internet, é o método ou protocolo através do qual dados são enviados de um computador para outro na Internet.
[71] NYE JR., op. cit., p. 99.
[72] HALPIN; TREVORROW; WEBB; WRIGHT, op. cit., pp. 45-46
[73] G8 é o grupo das oito nações mais industrializadas do mundo, mais a Rússia. G20 é o grupo formado pelo G8 mais outras nações emergentes.
[74] HALPIN; TREVORROW; WEBB; WRIGHT, op. cit., pp. 46-47
[75]Ibidem, p. 43

internacional a respeito da relevância dos ataques cibernéticos para o Globo e de tímidas iniciativas tomadas em direção à coerção de crimes cibernéticos.

Em nosso ponto de vista, as solução apresentadas pelos autores da obra *Cyberwar, Netwar and the Revolution in Military Affairs* seriam as mais adequadas, uma vez que os autores abrange tanto a defesa, como solução a curto prazo e paliativa para os ataques, como também sistemas de coerção, como solução a longo prazo. Nesse sentido, estes autores encerram as controvérsias existentes entre acadêmicos em torno da melhor forma de solução aos ataques ao incorporar as duas vias (defesa e coerção) em sua proposta.

Para fins de análise e exemplificação dos fatores aqui descritos como causas, características, consequências, reconhecimento e soluções para os conflitos cibernéticos, o próximo capítulo do presente trabalho trata-se de um estudo de caso a respeito do ataque cibernético através do *malware* Stuxnet.

CAPÍTULO 3 - O caso do Stuxnet

3.1 – Potência do Oriente

Há milênios o Oriente Médio é uma região bastante visada pela humanidade – além de sua importância geográfica, por estar no centro de três continentes (Europa, Ásia e África), a região é berço das maiores religiões do mundo, o Cristianismo e o Islamismo[76].

Nesse contexto de diversidade religiosa e étnica e de disputas por recursos naturais, naturalmente a região tornou-se foco de uma grande gama de conflitos. Em meio aos dezessete países[77] que compõem a região, o Irã destaca-se não apenas por sua grande extensão territorial[78], a segunda maior da região (atrás apenas da Arábia Saudita), e pelas grandes reservas de petróleo, mas sobretudo devido à sua política de projeção de poder frente aos demais países da região e postura desafiadora frente ao Ocidente[79].

3.2 – Política Externa Iraniana

Em 2005, com a eleição do presidente Mahmoud Ahmadinejad e após um período de foco na política interna, o Irã retomou a política de inserção internacional, notadamente no que tange ao enfrentamento da superpotência hegemônica atual, os Estados Unidos da América, e de Israel, clássico e poderoso inimigo de grande parte das nações do Oriente Médio. Em um tom desafiador, Ahmadinejad retomou a política nuclear daquele país e renovou o discurso nacionalista para a população. Além disso, Ahmadinejad aumentou a aproximação com os grupo político Hezbollah[80] – que contavam com seu apoio de forma às vezes oculta, às vezes mais aberta.[81]

---

[76] Field Listing: Religions. **The World Factbook.** Disponível em: <https://www.cia.gov/library/publications/the-world-factbook/fields/2122.html>. Acesso em: 04 jun. 2015.
[77] Arábia Saudita, Bahrein, Catar, Chipre, Egito, Emirados Árabes Unidos, Iêmen, Israel, Irã, Iraque, Jordânia, Kuwait, Líbano, Omã, Palestina, Síria e Turquia.
[78] 1 648 195 km²
[79] PENNA FILHO, Pio. O Irã e sua Inserção Internacional. **Boletim Meridiano 47**, v. 10, n. 106, p. 20-22, 2009.
[80] Movimento político islâmico que tem por objetivo a inexistência do Estado de Israel.
[81] PENNA FILHO, op. cit.

Contra os Estados Unidos, o Irã possui a não-aceitação dos pressupostos neoliberais capitalistas, que contam com a liderança daquele país. Contra Israel, por sua vez, as discordâncias são mais profundas, vão desde divergências econômicas e militares históricas até adentrar num tema no mínimo frágil na região do Oriente Médio: a religião. Apesar de o Estado de Israel já ter sido ratificado pela ONU há décadas e reconhecido pela grande maioria dos Estados do Globo[82], o Irã ainda é contra a sua existência.

Nesse sentido, notadamente nas décadas seguintes após a Revolução Iraniana[83] (1979), ainda que variando entre tom pacífico e ameaçador, a inserção internacional iraniana tem sido baseada na defesa de interesses próprios, autonomia no cenário internacional, protagonismo no Oriente Médio e exportação de seus valores baseados no islamismo fundamentalista. Mais recentemente, afinal, entende-se que este país tem assumido uma postura predominantemente ativa, e por vezes até agressiva, no sistema internacional.[84]

Não obstante, é importante salientar que a inserção internacional agressiva iraniana não advém apenas de iniciativa própria ou interesse espontâneo, mas pode ser vista como uma reação a ataques estrangeiros numa região que há séculos é assolada por uma vasta gama de conflitos. Além da clássica inimizade com Israel e do recente estranhamento com os Estados Unidos, o Irã tem como países vizinhos Estados considerados hostis, como Azerbaijão, Turcomenistão, Paquistão, Afeganistão e Iraque.[85]

3.3 – O Programa Nuclear Iraniano

Dada a tamanha atenção dada pelas autoridades e pela mídia ao programa nuclear iraniano nos últimos anos, pode haver a impressão, por parte da opinião pública, de que o início do programa é também recente. Contudo, o programa nuclear do Irã foi iniciado há mais de meio século, quando, em 1957, em meio à Guerra Fria e alinhamento ao ocidente, o país assinou acordo com os Estados Unidos, através do qual

[82] Em 1947, a ONU aprovou o plano de Partilha da Palestina. Com isso, o território palestino foi dividido em dois Estados, um judeu e outro árabe. Em maio de 1948, a criação do Estado de Israel foi oficialmente instituída.
[83] Também conhecida como Revolução dos Aiatolás, transformou o Irã de monarquia autocrática pró-Ocidente a república islâmica teocrática.
[84] PENNA FILHO, op. cit.
[85] CAETANO, Karizia Ribeiro Pereira. **O programa nuclear iraniano: ameaça internacional ou busca pela segurança do país**. 2014 apud VIZENTINI, 2002

este último proveria assistência técnica, arrendamento de vários quilos de urânio enriquecido e cooperação em pesquisa sobre o uso da energia nuclear de forma pacífica[86]. O provável interesse para a assinatura de tal acordo estria pautado no aumento das exportações de petróleo e gás iranianos, a serem substituídos internamente pela energia nuclear.

Entretanto, nas décadas seguintes, o Irã, alvo de interesse e disputa internacional desde o início do século XX por causa das reservas de petróleo[87], passou por conturbações, como a Revolução Branca e a Revolução Islâmica, que levou à alteração extrema da liderança política daquele país, assumindo a partir de então uma agenda nacionalista, fundamentalista e oposta aos valores ocidentais.[88] Na década de 1970 os Estados Unidos puderam sentir consideravelmente os efeitos do não-alinhamento iraniano quando tornaram-se um dos países mais prejudicados pela Segunda Crise do Petróleo, causada pela interrupção do fornecimento de petróleo por parte do Irã.[89] No final da década, em 1979, os Estados Unidos cessaram o apoio ao programa nuclear iraniano, enquanto o Irã já havia gasto cerca de 2,5 bilhões de dólares, o que adiou o programa nuclear desse país.[90]

Nos anos 1980, então, o Irã rompeu as relações com os Estados Unidos, quando, acusando o país de imperialismo e de apoio ao governo do Xá Reza Pahlevi, estudantes iranianos invadiram a embaixada dos Estados Unidos em Teerã e fizeram 63 funcionários como reféns, dos quais 52 só foram libertados três meses depois. [91]

Apesar das relações estremecidas com o Ocidente, a década de 1990 representou relativa paz para o Irã, tanto em âmbito interno, em que pode focar nessa década[92], quanto externo. Sob os governos dos presidentes Ali Akbar Hashemi Rafsanjani e Mohammad Khatami, o governo apresentava discurso moderado, de modo a evitar conflitos com outras nações – este último, inclusive, promovendo discursos de paz em relação a Israel, um inimigo histórico.[93] A postura pacifica de Khatami contribuiu para disfarçar as suspeitas de construção de usinas nucleares com fins bélicos, cuja

[86] CAETANO, op. cit., apud CORDESMAN; AL-RODHAN, 2006, p. 58.
[87] Idem apud PECEQUILO, 2009
[88] Idem apud OLIVEIRA e BRUNETTO, 2009, p. 69
[89] Idem apud FUSER, 2005, p. 173
[90] Idem apud CORDESMAN e AL-RODHAN, 2006, p. 63
[91] BARBOSA, Igor Andrade Vital. O Programa Nuclear do Irã: Novos Acontecimentos. **Conjuntura Internacional**. Belo Horizonte, ano 3, n. 17, jun. 2006.
[92] PENNA FILHO, op. cit.
[93] DE OLIVEIRA RAMOS, Lohana Gabriela Simões. Programa nuclear iraniano na era Ahmadinejad: implicações geopolíticas no Oriente Médio. **Anais ABED-PB 2012**, v. 1, n. 1, 2013.

investigação foi iniciada em 2002 atreladas a diversas fotos de satélites e relatórios da Agência Internacional de Energia Atômica (AIEA)[94]. À época, o governo alegou que a construção das usinas tinha como objetivo principal a geração de energia elétrica, uma vez que a população do país havia quase dobrado desde a Revolução Islâmica e que, por serem o petróleo e o gás seu principais itens de exportação e alvo de investimentos externos, a energia nuclear parecia uma boa opção para fonte energética de uso interno.[95]

No entanto, além das fotos de satélite, outro fator despertava desconfiança internacional: as usinas nucleares iranianas aumentaram a percentagem de enriquecimento de urânio de uma escala que variava de 3 a 5 % para 20%, o limite aceito como sendo de uso civil. [96] Apesar desse percentual ser insuficiente para fabricação de armas nucleares (para tal o percentual deveria chegar a 90%), o rápido aumento da capacidade de enriquecimento de urânio foi o principal fator das desconfianças externas.[97]

Em 2005, Khatami foi sucedido na presidência por Mahmoud Ahmadinejad, de perfil oposto. Enquanto Khatami apresentava postura reformista e discurso de paz, Ahmadinejad apresentava tom ultraconservador, fundamentalismo religioso e radicalização política contra o Ocidente.[98] Tal perfil do novo presidente resultou em grande preocupação internacional, também no que se refere à comercialização de petróleo e gás, mas principalmente em relação ao programa nuclear daquele país – apesar deste ser signatário do Tratado de Não-Proliferação Nuclear.

Como resultado das crescentes preocupações em torno da construção de usinas nucleares com possíveis fins bélicos, em 2006, seis países (Estados Unidos, Alemanha, China, França, Reino Unido e Rússia) formaram o grupo denominado P5+1, que correspondia aos cinco membros do Conselho de Segurança das Nações Unidas (CSNU), mais a Alemanha. Através da ONU ou de reuniões à parte, esse grupo tinha como objetivo a negociação multilateral com o Irã sobre seu programa nuclear. [99]

---

[94] Órgão da ONU responsável pela supervisão de programas nucleares, pela regulamentação do uso da tecnologia nuclear e pela inibição diplomática de países que não respeitem suas exigências, atuando no âmbito do TNP (MOTA, 2010).
[95] DE OLIVEIRA RAMOS, op. cit.
[96] O urânio enriquecido até 20% é classificado como levemente enriquecido. Mais do que isso já é considerado altamente enriquecido, isto é, enriquecer além dos 20% significa ultrapassar os limites aceitos internacionalmente os quais foram determinados pelo Tratado de Não-Proliferação de Armas Nucleares, gerando preocupações quanto à segurança Internacional.
[97] CAETANO apud MACHADO DA SILVA, 2010.
[98] DE OLIVEIRA RAMOS, op. cit.
[99] BARBOSA, op. cit.

Inicialmente, o P5+1 apresentou proposta de incentivos econômicos e políticos para o país, com a condição de que as atividades nucleares fossem suspensas e que o país cooperasse com a Agência Internacional de Energia Atômica (AIEA). A AIEA havia proposto que, como prova de seus objetivos pacíficos, o urânio pouco enriquecido daquele país fosse transportado à França e à Rússia e recebido de volta na forma de combustível de reator, em quantidades insuficientes para o desenvolvimento de armamentos nucleares.[100]Caso o Irã não aceitasse, haveria uma série de punições, principalmente econômicas, impostas pelo grupo.

Através do Conselho de Segurança da ONU, então, as grandes potências adotaram uma série de resoluções, solicitando que, para que pudesse contar novamente com a confiança internacional, o Irã comprovasse que seu programa nuclear era de fim pacífico, cumprindo com as determinações da AIEA. Além disso, foi estabelecido na resolução o pedido de suspensão do enriquecimento de urânio naquele país.[101]

No entanto, o posicionamento do Irã frente a tal proposta foi categórica: o presidente Mahmoud Ahmadinejad reafirmou que o programa nuclear iraniano possuiria fins pacíficos e que, portanto, o Irã não abriria mão de seu projeto de enriquecimento de urânio.[102]

Como consequência do descumprimento da resolução e da continuação de seu programa nuclear, o Irã recebeu sucessivas sanções, que se tornavam cada vez mais intensas.[103]

Em meio a esse contexto do uso da diplomacia por parte das grandes potências através de tentativas de negociação frustradas e da ineficácia da aplicação de sanções econômicas ao Irã para impedir sua agenda nuclear, o uso da força fez-se necessário (conforme mencionado no capítulo anterior para os casos em que a diplomacia não funciona), ao menos do ponto de vista dos Estados Unidos. Dada a ineficácia de outros métodos, a potência hegemônica resolveu, literalmente, partir para o ataque contra o Irã. Mas não um ataque militar, como fez com os vizinhos Iraque e Afeganistão. Os Estados Unidos partiram para o ataque cibernético.

3.4 – O Stuxnet

[100] VISENTINI, Paulo G. Fagundes. República Islâmica do Irã: Potência Emergente ou Regime em Crise? **Núcleo Brasileiro de Estratégia e Relações Internacionais**. Porto Alegre, 2010.
[101] CAETANO, op. cit.
[102] BARBOSA, op. cit.
[103] CAETANO, op.cit.

3.4.1 – Origens

Durante a década de 2000, seguindo os atentados de 11 de setembro de 2001 e sob comando de George W. Bush, a política externa estadunidense ocupava-se com a Guerra ao Terror, que teve como destaque a criação do chamado "Eixo do Mal"[104]. A potência hegemônica, então, não apenas incluiu o Irã nesse grupo, como também invadiu seus vizinhos Iraque e Afeganistão e aliou-se a todos os seus demais vizinhos.[105]

Nesse sentido, em meio a uma política já desgastada internacionalmente e a altos custos advindos das guerras, uma adicional invasão ao Irã a fim destruir suas instalações nucleares não valeria a pena, sob o ponto de vista dos especialistas estadunidenses[106]. O poder cibernético, surgiu, então, como uma terceira via para a resolução do problema. De forma inédita e, portanto, completamente inesperada pelo Irã, os Estados Unidos estavam prontos para por em prática um ataque cibernético.[107]

Visando a sabotar, mesmo que temporariamente, o programa nuclear iraniano e a provar a Israel que havia opção menos custosa para isso do que ataques militares, o governo dos Estados Unidos lançou o programa secreto Olympic Games.[108] Apesar de não haver garantia do funcionamento eficaz desse programa, dado seu ineditismo, tanto Washington quanto Tel Aviv concordaram em aplicá-lo.[109]

Sendo assim, a Agência Nacional de Segurança de Israel desenvolveu um software malicioso (*malware*), posteriormente compartilhado com o governo estadunidense, que seria introduzido no sistema de centrífugas para enriquecimento de urânio, situadas em Natanz, no Irã.[110] Esse *malware*, que viria a ser conhecido como

---

[104] Tal expressão, cunhada por Bush, traz duas referências implícitas: "Eixo", mesmo termo que remete aos inimigos dos EUA durante a Segunda Grande Guerra (Alemanha, Itália e Japão) e "Império do mal", como os soviéticos eram chamados pelos EUA durante a Guerra Fria. Assim, a conotação negativa dos conceitos anteriores seria agregada ao "eixo do mal".
[105] VISENTINI, op. cit.
[106] LOPES, Gills Vilar; DE OLIVEIRA, Carolina Fernanda Jost. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. **Revista Brasileira de Estudos de Defesa**, v. 1, n. 1. *apud* SANGER, 2012, p. 155.
[107] Idem apud SANGER, 2012, pp. 154, 191-193.
[108] Idem apud SANGER 2012, pp. 188-225
[109] Idem apud SANGER 2012, pp. 190-193
[110] Idem apud SANGER 2012, pp. 195-196

Stuxnet, consistia em um verme de computador (worm) criado para ser utilizado como arma cibernética.[111]

Através do mapeamento das máquinas iranianas feito por informantes israelenses, os especialistas em engenharia da computação e física nuclear dos Estados Unidos e de Israel tinham como intenção final a paralização das centrífugas, de forma a aparentar um acidente qualquer, sem nenhuma desconfiança de ataque cibernético por parte dos engenheiros iranianos[112].

Visando a compreender melhor sobre esse proeminente ataque cibernético, seguem abaixo algumas definições para o Stuxnet enquanto software malicioso, sua diferença em relação a outros softwares, e o que levaria a torna-lo uma arma cibernética.

3.4.2 Características técnicas

Os *malwares*, ou softwares maliciosos, podem ser divididos em inúmeras categorias, dentre as quais estão os vírus, vermes, cavalos de troia, *spywares* e *adwares*. Todos os tipos de *malware* são vulgarmente (e de forma errônea) conhecidos como vírus – no entanto, o Stuxnet não cabe nessa categoria. Dentro da categoria dos *malwares*, o Stuxnet corresponde a um verme, que normalmente não se espalham e afetam os computadores durante o processo de inicialização. Os vírus, por sua vez, normalmente espalham-se durante a execução de algum programa ou transferência de documentos.[113] Além disso, as ações dos vermes costumam ser direcionadas, diferentemente das ações comumente indiscriminadas/aleatórias dos vírus e outros tipos de softwares maliciosos.[114]

À exceção dos vírus e dos vermes, a grande maioria dos *malwares* têm como objetivo final de suas ações o lucro fácil, o que os permite ser facilmente rastreados: basta seguir o caminho das transações financeiras. Em sentido oposto, por não envolver quaisquer transações financeiras, o Stuxnet torna-se bastante difícil de ser encontrado.[115]

3.4.3 Funcionamento

---

[111] LOPES; DE OLIVEIRA, op. cit., apud CLARKE; KNAKE, 2012, pp. 291-294; FOLTZ 2012, p. 44.
[112] Idem apud CLARKE; KNAKE, 2012, p. 291, 295; SANGER, 2012, 189.
[113]GOYAL, Ravish; SHARMA, Suren; BEVINAKOPPA, Savitri; WATTERS, Paul. Obfuscation of Stuxnet and Flame Malware. **Latest Trends in Applied Informatics and Computing**. Oct. 2012.
[114] RAMOS, Hugo Filipe. Inevitabilidade Digital: O Poder dos Laços Fracos, Convergência e Curiosidade na Disseminação do Stuxnet. **Observatorio (OBS*)**, v. 8, n. 1, 2014.
[115] RAMOS, op. cit.

O funcionamento do Stuxnet acontece da seguinte forma:

- Na primeira etapa, um computador em uma intranet[116] é infectado com um arquivo que inclui o Stuxnet, que é transferido através da Internet ou trazido por uma mídia de memória removível (CD ou USB, por exemplo).[117]
- Depois de entrar na intranet, o Stuxnet espalha-se em muitos computadores de várias maneiras – por exemplo, por meio da troca de arquivos através da rede ou de memória removível.[118]
- O Stuxnet às vezes verifica um servidor de download na Internet e baixa dados a partir dele para atualizar-se, se uma nova versão do Stuxnet for encontrada lá. Nesta etapa, o Stuxnet comporta-se o mais discretamente possível, exceto a infecção agressiva.[119]
- Enquanto o Stuxnet está se espalhando na intranet, ele tenta procurar um determinado software HMI[120] para sistemas de controle. A partir daí, o Stuxnet reúne informações sobre o sistema e as envia para o invasor através do software HMI encontrado[121].
- O próximo passo para o Stuxnet é, então, verificar a configuração detalhada do sistema de controle para decidir se este deve ou não ser alvo de ataque.[122]
- Se não for o caso, o Stuxnet mantém silêncio, sem quaisquer outras ações.
- Se for o caso, o Stuxnet altera a programação do sistema, fazendo com que o conversor de freqüência opere fora de sua faixa de frequência normal.[123] Ao alterar a frequência do conversor, a centrífuga começa a girar mais rápida ou mais lentamente, dependendo da saída da frequência.[124]

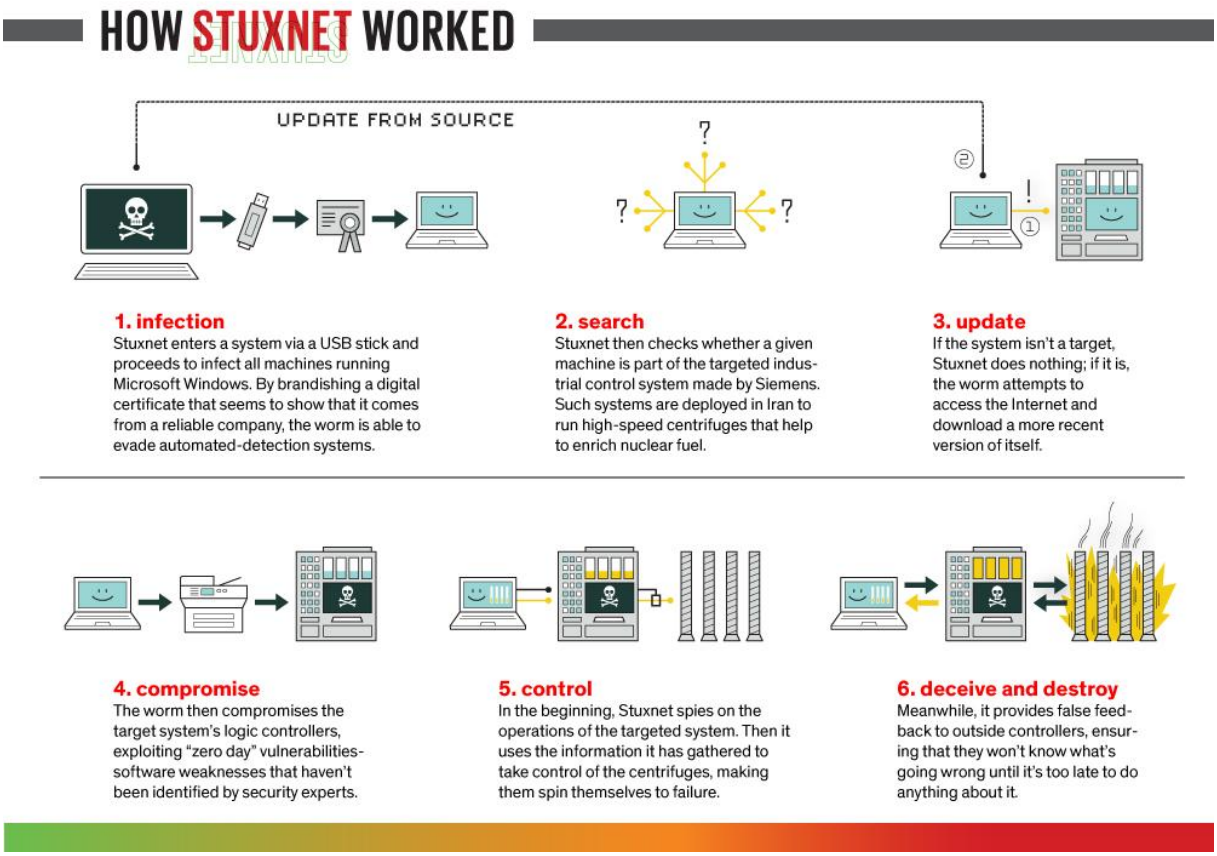
---

[116] Rede local de computadores, circunscrita aos limites internos de uma instituição, na qual são utilizados os mesmos programas e protocolos de comunicação empregados na Internet.
[117] MIYACHI, Toshio et al. Myth and reality on control system security revealed by Stuxnet. In: **2011 Proceedings of SICE Annual Conference (SICE)**. 2011. p. 1537-1540.
[118] Ibidem.
[119] Ibidem.
[120] Sigla em inglês para *Human-Machine Interface*, Interface Homem-Máquina. É o aparelho ou dispositivo que apresenta dados processados a um operador humano, e por isso, esses são capazes de monitorar e interagir com a máquina.
[121] GOYAL; SHARMA; BEVINAKOPPA; WATTERS, op. cit.
[122] MIYACHI, op. cit.
[123] LOPES; DE OLIVEIRA, op. cit., apud FALLIERE et al., 2011.
[124] Ibidem.

- Dada a alteração da velocidade da centrífuga, esta seria danificada ou destruída[125], ou, ainda, a qualidade de urânio seria prejudicada para o processo de enriquecimento[126].

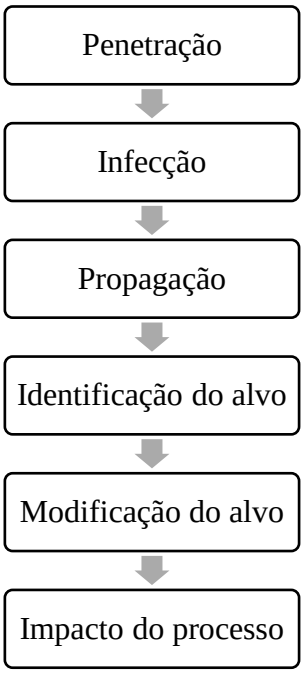
  A figura e o esquema representados abaixo reforçam e resumem a compreensão do processo acima descrito.

Figura 2: Como o Stuxnet funcionou. (Fonte: IEEE Spectrum, 2013) [127]



[125] LOPES; DE OLIVEIRA, op. cit., apud Homeland Security Newswire, 2010.
[126] Idem apud MARKS, 2010.
[127] The Real Story of Stuxnet. David Kushner. **IEEE Spectrum**. Disponível em: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Acesso em: 06 jun. 2015.

Figura 2: Esquema de ação do Stuxnet. (Fonte: International Journal of Science and Engineering Investigations, 2012).[128]

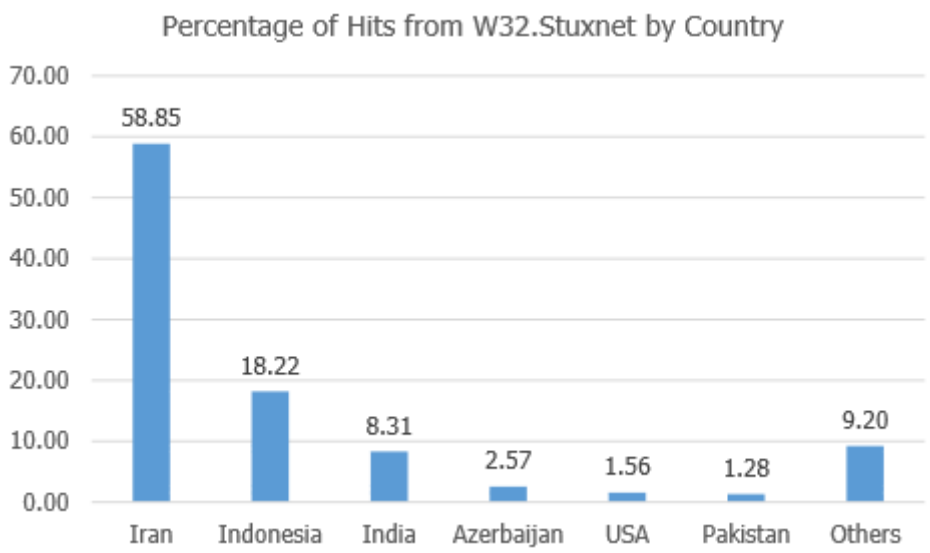


O processo de instalação e ataque do Stuxnet aparentemente poderia ser usado para quaisquer sistemas, em quaisquer países. E, de fato, como qualquer software, dada a natureza de rede da Internet, o Stuxnet acabou vazando para outros países. De acordo com a Microsoft, cerca de 22 fábricas haviam sido infetadas pelo Stuxnet até 2010, localizadas em países como Indonésia, Índia, Estados Unidos, Paquistão, entre outros.[129]

Contudo, o fato de o *malware* ter sido projetado para ataque ao Irã pode ser comprovado, ou ao menos reforçado, através da análise da figura 2, em que percebemos que a grande maior parte das infecções ocorreram naquele país.

[128] FAISAL, Mohammad; IBRAHIM, Mohammad. Stuxnet, Duqu and Beyond.**International Journal of Science and Engineering Investigations**, v. 1, n. 2, p. 75-78, 2012.
[129] COMBS, Marcia M. Impact of the Stuxnet Virus on Industrial Control Systems. **XIII International Forummodern Information Society Formation Problems, Perspectives, Innovation Approaches**, p. 5-10, 2011. *apud* (Byres, 2011) e (Clayton, 2010b)

Figura 3: Percentagem de infecções por país. (Fonte: Symantec, 2010)[130]



Além do que o gráfico evidencia, em 2010 a agência de notícias Associated Press relataram em comunicado que autoridades iranianas haviam denunciado um ataque cibernético, na forma de *malware*, que estaria prejudicando o programa nuclear do país.[131]

3.4.4 Descoberta

Não se sabe exatamente a data do ataque cibernético às usinas nucleares de Natanz. Algumas pistas indicam que este demorou meses para ser descoberto pelos engenheiros iraniano, uma vez que parte da estrutura da usina nuclear havia explodido[132] em certo momento de 2009.

No entanto, os primeiros passos para sua repercussão mundial aconteceram em meados de 2010, quando Sergey Ulasen[133], especialista da empresa bielorrussa de softwares antivírus VirusBlokAda, anunciou que um dos clientes da companhia havia sido infectado pelo Stuxnet.

Um dos colegas de trabalho de Sergey prestava assistência técnica no Irã e o informou, através de telefonema, sobre o novo *malware* descoberto, que parecia

[130] RAMOS, op. cit., apud SYMANTEC 2010
[131] RAMOS, op. cit., apud KARIMI, 2010
[132] LOPES; DE OLIVEIRA, op. Cit., apud CLARKE; KNAKE, 2012, pp. 291, 295; SANGER, 2012, p. 189.
[133] RAMOS, op. cit. apud KASPERKY, 2011

bastante complicado e suspeito. Sergey, então, estabeleceu acesso remoto ao computador afetado no Irã e, junto a seu colega, conseguiu identificar o *malware* e suas características. Chamou-lhe atenção o fato de que tal *malware* (Stuxnet) utilizava certificados digitais falso de uma empresa muio conhecida no mercado e, por isso, passava despercebido pelo anti-virus do computador – o que levou-lhe à conclusão de que os agentes por trás do Stuxnet haviam roubado os certificados digitais da empresa e introduzido no *malware*, com a finalidade que este não fosse identificado.[134]

Ciente da grandiosidade de sua descoberta, Sergey resolveu revela-la para a indústria de informática. A princípio, informaram à Realtek, de onde os certificados haviam sido roubados, e à Microsoft, empresa fabricante do Windows, sistema operacional afetado. Por não obter respostas das empresas, Sergey decidiu publicar a descoberta no site da empresa em que trabalhava.[135]

3.4.5 Repercussão

No que se refere às empresas as proporções da publicação de Sergey levaram-nas a investigar o Stuxnet mais a fundo. A Microsoft, após estudo detalhado por parte de sua equipe de engenheiros de software, concluiu que Sergey estava correto quanto à natureza do software e que estava trabalhando para resolver o problema.[136] Ademais, técnicos em softwares chegaram a declarar que o Stuxnet era "um verme sofisticado", um "virador de jogo", "o melhor *malware* já criado" e até "revolucionário".[137]

No entanto, a reação das autoridades iranianas surpreendeu Sergey, segundo o qual não existiu qualquer tipo de resposta ou comunicado oficial e, quando encontrou alguma autoridades iranianas na Bielorrússia, estes não demonstraram qualquer conhecimento acerca da existência do *malware*.[138]

Os Estados Unidos, por sua vez, reagiram com preocupação à divulgação do caso Stuxnet na mídia. Algumas reuniões foram realizadas por suas agências de inteligência acerca dos danos que a repercussão do caso poderiam causar à imagem dos Estados Unidos, visto que o Irã, um Estado soberano, havia sido secretamente atacado por eles. O presidente Barack Obama, então, evitou fazer declarações públicas sobre o

[134] RAMOS, op. cit.
[135] Ibidem
[136] RAMOS, op. cit., apud BORLAND, 2010.
[137] COMBS, op. cit., apud GROSS, 2010; KEIZER, 2010.
[138] RAMOS, op. cit., apud KASPERSKY, 2011.

assunto e continuou a focar em negociações contra o programa nuclear iraniano junto a seus aliados.[139]

No que concerne ao envolvimento de Israel, não há nenhuma evidência que comprove tal suspeita. Porém, alguns pesquisadores de segurança, como o alemão Ralph Langer, chegaram a declarar abertamente suas suspeitas de Israel estaria por trás do ataque cibernético, sob o argumento de que 60% dos sistemas afetados estariam no Irã.[140] Ainda, um artigo do jornal estadunidense The New York Times relatou que Israel havia testado secretamente o Stuxnet no completo israelense de Dimona, em centrífugas praticamente idênticas às de Natanz.[141] Além disso, em declaração bastante suspeita, um oficial de inteligência de Israel afirmou que "é bom que os iranianos pensem que temos essas capacidades"[142].

Em 2012, dois anos após a descoberta do ataque cibernético, atuais e ex-funcionários públicos dos Estados Unidos, de Israel e da Europa admitiram participação no ataque e forneceram detalhes estratégicos em entrevistas ao jornalista estadunidense David Sunger, do jornal *The New York Times*.[143] Os funcionários relataram que o projeto *Olympic Games* começou em 2006 sob administração de George W. Bush e foi acelerado após a posse de Barack Obama. Além disso, afirmaram que o *malware* Stuxnet foi desenvolvido pela agência estadunidense NSA (National Security Agency) e a Unidade 8200, o braço cibernético do Corpo de Intelogência das Forças de Defesa de Israel.

3.5 – Efeitos pós-Stuxnet

O Stuxnet caracteriza-se um marco na História por ser considerado a primeira arma cibernética a ser efetivamente utilizada, visto que, pela primeira vez, um *malware* passou do plano virtual e da pequena escala de computadores pessoas para

---

[139] LOPES; DE OLIVEIRA apud SANGER 2012, p. 205.
[140] COMBS, op. cit. apud FALLIERE et al., 2011.
[141] Idem apud BROAD, MARKOFF; SANGER, 2011.
[142] Stuxnet Worm Delayed Iran's Nuclear Bomb. Julie Stahl. **CBN News**. Disponível em: <http://www.cbn.com/cbnnews/insideisrael/2011/January/Stuxnet-Worm-Delayed-Irans-Nuclear-Bomb-/>. Acesso em: 06 jun. 2015.
[143] Obama Administration Admits Cyberattacks Against Iran Are Part Of Joint US-Israeli Offensive. Michael B. Kelley. **Business Insider**. Disponível em: <http://www.businessinsider.com/obama-cyberattacks-us-israeli-against-iran-2012-6>. Acesso em: 06 jun. 2015.

consequências no plano físico, provocando impacto internacionalmente relevante ao atrasar o programa nuclear iraniano.[144]

Não se pode dizer exatamente quais eram as expectativas da aliança Estados Unidos-Israel acerca da proporção dos efeitos após o ataque cibernético ao Irã, uma vez que a ação foi elaborada de forma completamente secreta e não houve pronunciamento oficial dos governos de nenhum dos dois países a respeito do Stuxnet.

Quanto à resposta do Irã a respeito do ataque através do Stuxnet, o ex-presidente Mahmoud Ahmadinejad admitiu que "conseguiram criar problemas para um número limitado de centrífugas com o software que instalaram em componentes elétricos"[145]. O governo do Irã não declarou abertamente quantas centrífugas foram atingidas, porém o Instituto para Ciência e Segurança Internacional, baseado em Washington (EUA), estimou que cerca de 1000 centrífugas foram danificadas pelo Stuxnet, o que corresponderia a cerca de 10% do total de centrífugas de Natanz.[146] Ainda, o especialista alemão Ralph Langer, um dos primeiros a analisar o caso do Stuxnet, estimou à época que os dados às centrífugas de enriquecimento de urânio tenham possivelmente atrasado o programa nuclear iraniano em cerca de dois anos.[147]

No entanto, sabe-se que o Irã não apenas substituiu suas centrífugas rapidamente e retomou seu programa nuclear em prazo anterior ao esperado[148], como, contemporaneamente, cinco anos após a repercussão do ataque, ainda mantém o processo de enriquecimento de urânio até os dias atuais[149].

Inferimos, nesse sentido, que, mesmo que o uso do Stuxnet tenha sido inédito e que suas consequências tenham sido pouco possíveis de serem calculadas pela aliança Estados Unidos-Israel, provavelmente os governos de ambos os países estavam cientes de que o ataque não seria suficiente para a destruição completa de todas as centrífugas de enriquecimento de urânio de Natanz, a ponto de boicotar por completo o programa

---

[144] RAMOS, op. cit.

[145] Stuxnet: Ahmadenejad admits cyberweapon hit Iran nuclear program. Mark Clayton. **The Christian Science Monitor**. Disponível em: <http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program>. Acesso em: 06 jun. 2015.

[146] Stuxnet may have destroyed 1,000 centrifuges at Natanz. Yaakov Katz. **The Jerusalem Post**. Disponível em: <http://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz>. Acesso em: 06 jun. 2015

[147] Ibidem.

[148] Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack. Joby Warrick. **Washington Post**. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html>. Acesso em: 06 jun 2015.

[149] No military solution to Iran's nuclear program: Obama. **Business Standard.** Disponível em: <http://www.business-standard.com/article/pti-stories/obama-no-military-solution-to-iran-s-nuclear-program-115060200073_1.html>. Acesso em: 06 jun 2015.

nuclear iraniano; e, ainda assim, os custos para o ataque (tanto financeiros, quanto à reputação no sistema internacional) foram considerados válidos.

É provável, portanto, que, seguindo o caso do Stuxnet esteja de acordo com o conceito apresentado no capítulo 2 do presente trabalho: os ataques cibernéticos visam, primordialmente, ao dano à informação objetivando a mudança na tomada de decisões do inimigo.

O dano à apenas 10% das centrífugas de Natanz, com a tão rápida recuperação, não valeria à pena quando se consideram os riscos de má reputação internacional para Estados Unidos e Israel. Portanto, o provável interesse desses países seria inicialmente o de *confundir* o governo iraniano – já que este desconhecia a origem do problema das centrífugas, e posteriormente observou que não seria capaz de resolvê-lo por completo, uma vez que o Stuxnet partiu de ataque externo; e, a longo prazo, que o governo iraniano *tomasse a decisão* de encerrar seu programa nuclear, ao observar que a resistência às sanções econômicas não bastavam frente às grandes potências. Os inimigos eram suficientemente fortes a ponto de atacá-los de forma surpreendente e não havia qualquer possibilidade de retaliação.

Dessa forma, ao analisarmos as consequências do Stuxnet nove anos após a sua repercussão, constatando que os Irã persiste em seu programa nuclear, poderíamos dizer que Estados Unidos e Israel não foram bem-sucedidos em seu ataque. Contudo, ao levarmos em consideração os inéditos custos extremamente baixos do uso da força – sem perdas humanas e sem utilização de armamentos pesados, além da ausência de resposta legal ao ataque, entende-se que o projeto *Olympic Games* foi extremamente bem-sucedido.

Ainda pode-se dizer que a demonstração inédita de poder cibernético confere grande respeito internacional aos seus autores, tendo servido, portanto, como um excelente instrumento para a propagação de seu *soft power*, notadamente às nações do Ocidente, onde o processo de vilanização do Irã parece surtir maior efeito.

Considerações finais

A preocupação com a segurança, o medo de ataque a partir algum se seus semelhantes, é um dos aspectos mais antigos do comportamento humano, sendo até mesmo a origem da criação dos Estados nacionais, conforme Hobbes, mencionado no primeiro capítulo deste trabalho.

Entretanto, não houve sequer um período da História da humanidade em que a paz absoluta prevaleceu, em que o medo de ataques cessou – tanto na esfera individual, quanto na interestatal. Mesmo após o surgimento dos Estados para defesa da população, mesmo após a criação de mecanismos regulatórios internacionais, o sistema internacional permanece anárquico e a segurança nacional continua fazendo parte das agendas de praticamente todas as nações do globo – e também das instituições transnacionais, conforme dita a Teoria Realista também mencionada no presente trabalho.

Dessa forma, sabendo que o conflito sempre esteve presente na História, desde os mais antigos registros, seria, sob nosso ponto de vista, ingênuo imaginar que em algum momento as controvérsias cessarão e o mundo passará a contar com segurança plena e paz absoluta. Os conflitos continurão a existir, portanto. Talvez devido à natureza má do homem, como afirmam os realistas e neorrealistas, mas disso nunca poderemos ter certeza. De certo, todavia, é que os interesses e as crenças dos homens continuarão divergentes, e sendo esse o fator principal da gênese dos conflitos, os ataques continuarão a ser ameaça constante, para indivíduos e para Estados.

O século XX poderia ser considerado como o ápice da destruição mútua entre os homens, quando se leva em consideração as duas guerras mundiais e os milhões de mortos por ela deixados, para não mencionar todos os outros conflitos ocorridos nesse século. A Segunda Grande Guerra, a mais destruidora delas, teve a participação direta ou indireta de dezenas de países e culminou com o utilização, pela primeira vez, de uma arma nuclear. O mundo assistiu, perplexo, à enorme destruição causada por humanos a seus semelhantes e a rendição imediata da parte atacada.

Nesse sentido, dentre todas as marcas que a Segunda Grande Guerra deixou, uma delas pernamence até os dias atuais e deve perpetuar-se por bastante tempo: o medo de uma possível *Terceira Guerra Mundial* e da inimaginável destruição que esta poderia causar, uma vez que diversos países já declararam possuir armas nucleares, cuja capacidade de destruição é incalculável.

Desde então, mesmo com a existência das armas nucleares (e de outros modernos artefatos de guerra), essas, felizmente, nunca foram utilizadas novamente. Os conflitos, assim como as guerras, continuam a existir, porém, de modo geral, entre grandes potências e Estados fragilizados – como na Guerra do Iraque e do Afeganistão, por exemplo – o que as torna mais sistemas de opressão do que de fato batalhas entre forças iguais.

Dessa maneira, as grandes potências, detentoras de imenso poder militar, visando a evitar o confronto militar, têm buscado outras formas para resolução de controvérsias – notadamente a diplomacia, o direito internacional, o sistema de sanções e, o tão recente e ainda pouco utilizado, ataque cibernético; como pode ser observado no caso do *malware* Stuxnet, detalhado no capítulo 3 deste trabalho.

Sendo assim, percebe-se que os ataques cibernéticos, quando comparados às guerras tradicionais, mostram-se melhor alternativa para resolução de controvérsias devido a seus custos baixíssimos, tanto humanos como financeiros. Nesse contexto, se analisarmos o funcionamento e os efeitos dos ataques cibernéticos à luz das definições contemporâneas de poder de Joseph Nye, vistas no primeiro capítulo deste trabalho, os ataques físicos (*hard power*) a sistemas de computadores mostram-se quase sempre eficazes tecnicamente, assim como sua consequente imagem de inovação e dominância tecnológica (*soft power*) possibilitaria vantagem para o agressor em relação à parte agredida ou a outros atores, visando a futuras negociações e acordos diplomáticos – possibilitando maior probabilidade à mudança de comportamento desejada pelo agressor. Portanto, os ataques cibernéticos poderiam adequar-se ao conceito de *smart power*, em que ambos *hard* e *soft power* são utilizados de modo a proporcionar maior poder aos autores dos ataques.

No entanto, evidentemente os ataques cibernéticos não podem ser defendidos como forma legítima de resolução de controvérsias, uma vez que ferem o princípio básico de soberania estatal. No sistema internacional anárquico, conforme teoria realista também vista no primeiro capítulo deste trabalho, a defesa da soberania é primordial, visto que, se não há qualquer sistema de governança transnacional, tampouco qualquer Estado possuiria legitimidade de sobrepor-se a outros Estados.

Nesse sentido, a fim de coibir os ataques cibernéticos internacionais, faz-se necessário o uso de estratégias a curto, médio e longo prazo. E tais estratégias devem ser protagonizadas pelos Estados, que, mesmo com o surgimento de diversos novos atores no cenário internacional, continuam sendo os atores mais poderosos.

A curto prazo, faz-se necessária a distinção entre ataques relevantes e pouco relevantes, e a descoberta dos autores de ataques cibernéticos. A médio prazo, seriam desenvolvidos sistemas eletrônicos mais robustos, capazes de resistir à maior parte dos ataques. E a estratégia a ser aplicada a longo prazo seria a criação em conjunto de um sistema de governança supranacional capaz de julgar e punir os autores dos ataques cibernéticos internacionais.

Referências Bibliográficas

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. **Dicionário de Política (A-Z)**. Brasília- UNB, 1998. Pp. 933-942.

CASTRO, Thales Cavalcanti. **Elementos de Política Internacional**. Curitiba: Juruá, 2005. P. 53

HALPIN, Edward; TREVORROW, Philippa; WEBB, David; WRIGHT, Steve. (Ed.). **Cyberwar, Netwar and the Revolution in Military Affairs.** Nova Iorque: Palgrave McMillan, 2006.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica**. Editora Atltas, São Paulo, 5ª edição, 2003.

LIBICKI, Martin C. **Conquest in Cyberspace**. Nova Iorque: Cambridge University, 2007.

NOGUEIRA, João Pontes; MESSARI, Nizar. **Teoria das Relações Internacionais.** Rio de Janeiro-Elsevier, 2005. P. 26.

NYE JR., Joseph Samuel. **The Future of Power**. Nova Iorque: Public Affaris, 2011. p. 85.

SHELDON, John B. The Rise of Cyberpower, p. 309. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. (Ed.). **Strategy in the Contemporary World.** Nova Iorque: Oxford University, 2013. P. 309.

Artigos

ABREU, Karen Cristina Kraemer. História e usos da Internet. **Biblioteca on-line de Ciência da Comunicação.** v. 12, p. 05-09, 2009.

AMARAL, Luis Mira. A sociedade da informação. **JD Coelho, A sociedade da informação-O percurso português**, p. 85-92, 2007.

BARBOSA, Igor Andrade Vital. O Programa Nuclear do Irã: Novos Acontecimentos. **Conjuntura Internacional**. Belo Horizonte, ano 3, n. 17, jun. 2006.

COMBS, Marcia M. Impact of the Stuxnet Virus on Industrial Control Systems. **XIII International Forummodern Information Society Formation Problems, Perspectives, Innovation Approaches**, p. 5-10, 2011. *apud* (Byres, 2011) e (Clayton, 2010b)

DE OLIVEIRA RAMOS, Lohana Gabriela Simões. Programa nuclear iraniano na era Ahmadinejad: implicações geopolíticas no Oriente Médio. **Anais ABED-PB 2012**, v. 1, n. 1, 2013.

FAISAL, Mohammad; IBRAHIM, Mohammad. Stuxnet, Duqu and Beyond.**International Journal of Science and Engineering Investigations**, v. 1, n. 2, p. 75-78, 2012.

GOYAL, Ravish; SHARMA, Suren; BEVINAKOPPA, Savitri; WATTERS, Paul. Obfuscation of Stuxnet and Flame Malware. **Latest Trends in Applied Informatics and Computing**. Oct. 2012.

KIM, Joon Ho. Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. **Horizontes antropológicos**, v. 10, n. 21, p. 199-219, 2004.

LOPES, Gills Vilar; DE OLIVEIRA, Carolina Fernanda Jost. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. **Revista Brasileira de Estudos de Defesa**, v. 1, n. 1.

MIYACHI, Toshio et al. Myth and reality on control system security revealed by Stuxnet. In: **2011 Proceedings of SICE Annual Conference (SICE)**. 2011. p. 1537-1540.

MOREIRA, Ruy. Sociabilidade e espaço: as formas de organização geográfica das sociedades na era da terceira revolução industrial-um estudo de tendências. **Agrária**, São Paulo, n. 2, p. 93-108, 2005.

PENNA FILHO, Pio. O Irã e sua Inserção Internacional. **Boletim Meridiano 47**, v. 10, n. 106, p. 20-22, 2009.

RAMOS, Hugo Filipe. Inevitabilidade Digital: O Poder dos Laços Fracos, Convergência e Curiosidade na Disseminação do Stuxnet. **Observatório**, v. 8, n. 1, 2014.

VISENTINI, Paulo G. Fagundes. República Islâmica do Irã: Potência Emergente ou Regime em Crise? **Núcleo Brasileiro de Estratégia e Relações Internacionais**. Porto Alegre, 2010.

Trabalhos Acadêmicos

CAETANO, Karizia Ribeiro Pereira. O programa nuclear iraniano: ameaça internacional ou busca pela segurança do país. 2014.

Páginas Web

Field Listing: Religions. **The World Factbook.** Disponível em: <https://www.cia.gov/library/publications/the-world-factbook/fields/2122.html>. Acesso em: 04 jun. 2015.

Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack. Joby Warrick. **Washington Post**. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html>. Acesso em: 06 jun 2015.

National Cybersecurity Strategies in the World. **Enisa**. Disponível em: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-

strategies-ncsss/national-cyber-security-strategies-in-the-world>. Acesso em: 09 jun. 2015.

No military solution to Iran's nuclear program: Obama. **Business Standard.** Disponível em: <http://www.business-standard.com/article/pti-stories/obama-no-military-solution-to-iran-s-nuclear-program-115060200073_1.html>. Acesso em: 06 jun 2015.

Obama Administration Admits Cyberattacks Against Iran Are Part Of Joint US-Israeli Offensive. Michael B. Kelley. **Business Insider**. Disponível em: <http://www.businessinsider.com/obama-cyberattacks-us-israeli-against-iran-2012-6>. Acesso em: 06 jun. 2015.

Stuxnet: Ahmadenejad admits cyberweapon hit Iran nuclear program. Mark Clayton. **The Christian Science Monitor**. Disponível em: <http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program>. Acesso em: 06 jun. 2015.

Stuxnet may have destroyed 1,000 centrifuges at Natanz. Yaakov Katz. **The Jerusalem Post**. Disponível em: <http://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz>. Acesso em: 06 jun. 2015

Stuxnet Worm Delayed Iran's Nuclear Bomb. Julie Stahl. **CBN News**. Disponível em: <http://www.cbn.com/cbnnews/insideisrael/2011/January/Stuxnet-Worm-Delayed-Irans-Nuclear-Bomb-/>. Acesso em: 06 jun. 2015.

The Real Story of Stuxnet. David Kushner. **IEEE Spectrum**. Disponível em: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Acesso em: 06 jun. 2015.

Top 13 dos ataques cibernéticos de 2014. Alcyon Junior. **Portal TIC**. Disponível em: <http://portaltic.com/84-alcyon-junior/496-top-13-dos-ataques-ciberneticos-de-2014.html>. Acesso em: 09 jun. 2015.

US Investment in Cyber-security Equal to Nuclear Strategy. Edward Smith. **International Business Times**. Disponível em: <http://www.ibtimes.co.uk/cyber-security-nuclear-budget-china-attacks-congress-467232>. Acesso em: 09 jun. 2015.