UNIVERSIDADE FEDERAL DO AMAPÁ
DEPARTAMENTO DE FILOSOFIA E CIÊNCIAS HUMANAS
BACHARELADO EM RELAÇÕES INTERNACIONAIS

RODOLFO CAMPANA TRES

GEOPOLÍTICA E PODER NA ERA DA *CYBERWARFARE*: O CASO DO STUXNET

Macapá
2018

RODOLFO CAMPANA TRES

GEOPOLÍTICA E PODER NA ERA DA *CYBERWARFARE*: O CASO DO STUXNET

Artigo Científico apresentado no âmbito da Graduação em Relações Internacionais da Universidade Federal do Amapá, como requisito para obtenção do grau de Bacharel em Relações Internacionais.

Orientador: Prof. MSc. Milton José Deiró de Mello Neto

Macapá
2018

SUMÁRIO

"... Ciberespaço. Uma alucinação consensual experimentada diariamente por bilhões de operadores legítimos, em todas as nações, por crianças aprendendo conceitos matemáticos... Uma representação gráfica de dados extraídos dos bancos de cada computador no sistema humano. Complexidade impensável. As linhas de luz variaram no não espaço da mente, aglomerados e constelações de dados. Como as luzes da cidade, recuando."

(William Gibson, 1984; p.69).

INTRODUÇÃO

O presente artigo científico apresenta-se com o objetivo de informar, provocar e conscientizar a respeito das novas tecnologias que fazem parte dos domínios do conflito e da segurança internacional neste século, mais especificamente, a respeito da revolução causada nos assuntos militares pela constante virtualização encarada atualmente e o frenético desenvolvimento das tecnologias da informação. Este trabalho de pesquisa tem por objeto de estudo o caso de ataque cibernético de 2010, denominado de Stuxnet, e seus respectivos impactos e consequências em âmbitos domésticos e internacionais, da política e da segurança, tanto física quanto virtual.

Através de três capítulos, equilibradamente divididos, far-se-á uma discussão dos principais conceitos teóricos e técnicos relevantes para que seja possível compreender a dimensão e o escopo do caso estudado, além de ser possível medir a grosso modo e estimar suas consequências, tanto imediatas quanto futuras, e quais os precedentes abertos pelo mesmo.

O primeiro capítulo consiste numa extensa, porém necessária análise teórica dos principais conceitos norteadores deste trabalho, alocados na corrente teórica do Realismo, mais precisamente do Realismo Estrutural. Utilizando autores de apoio, com suas respectivas obras, e as obras de um autor específico escolhido para ilustrar os conceitos importantes, se espera obter o devido embasamento teórico.

O segundo capítulo trata-se de uma importante compilação e construção de explicações e conhecimentos técnicos, necessários a um possível leitor para entender os processos envolvidos e ameaçados tanto nas tecnologias da informação quanto na segurança doméstica, que inicialmente é um dos alvos prioritários. Este capítulo também busca explicar conceitos novos e abstratos, de forma a orientar a percepção do leitor.

Por fim, o terceiro e último capítulo trata da descrição e explicação do caso do estudado, informando ao leitor os principais pontos e o histórico que compõe o mesmo e seus acontecimentos, bem como suas consequências a curto, médio e longo prazo, terminando com algumas conexões com os argumentos anteriores, provocações e tentativas de previsão a respeito dos precedentes abertos pelo acontecimento e pelas consequências encaradas.

CAP. 1 – CONCEITOS DAS RELAÇÕES INTERNACIONAIS

A principal importância ao discutir-se qualquer tema sob o escopo das Relações Internacionais é tentar compreender em quais das principais correntes teóricas de pensamento encaixa-se o tema em questão e os seus principais desdobramentos e consequências. Porém, nem sempre é possível traçar paralelos consistentes entre tema/hipótese e corrente teórica.

Entretanto, diversas colocações e considerações de autores e teóricos clássicos, não podem ser ignoradas. As contribuições idealistas de Woodrow Wilson no começo do Séc. XX; as colocações pessimistas acerca da natureza humana (e consequentemente da política entre as nações) de Hans Morgenthau no período entre guerras, e demais posicionamentos que já foram de grande importância nos processos de tomada de decisões devem ser considerados ao produzir qualquer tipo de análise de caráter internacional, especialmente no que tange a um tema de grande importância política (*high politics*) como a Geopolítica.

O Realismo, corrente teórica escolhida para ser aplicada neste trabalho de pesquisa e interpretação, sempre se apresenta como forte candidato para compor análises no campo internacional como mostram um bom número de autores das Relações Internacionais, devido à abrangência com que ele lida temas de alta importância no cenário político internacional, e como suas preposições também frequentemente são reavaliadas e reformuladas ao longo dos anos.

Mesmo que surjam como críticas ferrenhas, não são poucos os comentários acerca do Realismo, evidentemente delineando sua fundamental importância tanto como teoria quanto como instrumento de definição de políticas em qualquer discussão séria dentro das Relações Internacionais.

1.1 – CONCEITOS REALISTAS

Por mais recorrente e frequente que seja a presença do Realismo nas discussões, conforme já citado anteriormente, completamente ignorar as colocações de diversos teóricos dessa corrente ocasionaria um problema incompatível com o nível desta pesquisa.

O realismo político – *realpolitik* – muitas vezes traçado cronologicamente ao tempo do historiador grego Tucídides e de seus escritos sobre a guerra do Peloponeso, surge no cerne das civilizações ocidentais durante o Séc. XX (Donnelly, 2004; Pg. 1) após a disciplina das Relações Internacionais formalmente ser consolidada, aproximadamente no começo do período entre guerras, meados de 1919 (Vasquez, 2004; Pg. 32).

Quase que de forma imediata após o estouro da Segunda Guerra Mundial e ascensão, a disciplina viu-se reformulada com as contribuições de Edward H. Carr e Hans Morgenthau, os autointitulados "realistas" daquela época (Donnelly, 2004; Pg. 1), para citar alguns exemplos.

Edward Carr, com sua obra "Vinte Anos de Crise" de 1939, teceu fortes críticas às concepções idealistas da época, sob as afirmações de que essas teorias haviam sido concebidas através de estudos diretos em campo, além de que essas mesmas ideias tenham sido embasadas em uma visão utópica e desconexa com a realidade, onde se foi projetado sob o que era ideal (vide o nome idealista, dado pelos realistas a esses teóricos) e não sob o que era real vide o nome "realismo" (Vasquez, 2004; Pg. 33, 35). Carr também sustentou em suas argumentações que o propósito da teoria deveria ser entender e adaptarem-se as forças que guiam os comportamentos, tal qual deveria ser feito um contraponto ao "utopianismo" que havia dominado anteriormente (Vasquez, 2004; Pg. 35).

Os escritos de Hans Morgenthau que, segundo a opinião de Vasquez, foram os que melhor sintetizaram e promulgaram a visão destes autores. Ele nos diz que a obra Política Entre as Nações (*Politics Among Nations*), foi tão compreensiva, sistemática e teórica, que serviu de base para a consolidação do paradigma (Vasquez, 2004; Pg. 36).

O Realismo não surge nesse cerne como uma teoria pronta, como uma série de afirmações e explicações explícitas, mas sim como uma orientação mais generalizada, com ênfases normativas. O Realismo surge como uma abordagem construída ao longo do tempo, com as contribuições de diversos autores e analistas, emergindo gradativamente, estabelecendo premissas mais generalizadas, porém bem distintivas (Donnelly, 2004; Pg. 6) sobre a política internacional.

A aceitação das assertivas realistas acerca da política foi bem positiva ao longo das décadas de 40 e 50, especialmente nos Estados Unidos e Reino Unido, levando a consolidação do realismo como paradigma, permitindo que esta adquirisse as características de uma disciplina estabelecida (Vasquez, 2004; Pg. 38).

Ao longo do desenvolvimento da teoria, Vasquez nos diz que as pesquisas tornaram-se cada vez mais especializadas, ao invés de novas tentativas de uma "Grande Teoria" que abraçasse todos os conceitos delineados por Morgenthau. Ao invés disso, os esforços agora se concentravam em investigar cada conceito individualmente, e, além disso, desenvolver estudos sistêmicos a cerca de novos conceitos que surgiriam ao longo dos anos. Novos tópicos e subcampos de estudo surgiram com o tempo, e talvez a forma como se construiu esse paradigma, permitiu ao realismo se manter relevante ao longo das várias discussões e dos anos.

1.1.1 – REALISMO DEFENSIVO

Categorizado de forma mais abrangente pelo termo "Realismo Estrutural", esse conjunto de assertivas acerca da política internacional e do comportamento de Estados é o que se compreende como Neorrealismo: Uma abordagem atualizada e reformulada dos conceitos que fizeram do Realismo o que este é hoje, embasada em novos estudos, autores, temas e desafios impostos pela nova ordem mundial.

O Realismo Estrutural recebe este nome devido a constante presença em suas formulações de análises focadas nas características estruturais (sistêmicas) dos componentes da política internacional, a exemplo da "anarquia internacional", na contramão do Realismo Clássico, que sustenta suas análises sobre premissas acerca da natureza humana e comportamentos (Donnelly, 2004; Pg. 11). Essa abordagem é perceptível quando se analisa as obras dos autores em questão, particularmente as de John J. Mearsheimer e Kenneth N. Waltz.

Em especial, a variação escolhida para tratarmos aqui, o Realismo Defensivo, tem como principal proponente, Kenneth Waltz, autor e teórico de grande importância para os estudos das relações internacionais. Waltz trabalha em algumas de suas obras consultadas para esta pesquisa, conceitos bastante importantes para as análises propostas aqui. Elenca-se o conceito de "capacidades" e sua interpretação de "poder" e assertivas sobre a "anarquia internacional" como os focos deste.

A denominação “defensivo”, a esta variação do Realismo advém de uma classificação autointitulada de Mearsheimer aos seus escritos e argumentos, que consistem numa base de assertivas semelhantes aos conceitos base do Realismo Estrutural, porém focados na maximização do poder e das capacidades, o que ele chama de “Realismo Ofensivo”, num direito contraponto ao foco utilizado por Waltz, baseado em um objetivo mais moderado, de sobreviver adequadamente no ambiente anárquico internacional (Vasquez, 2004; Pg. 288, 289).

Mearsheimer frequentemente faz menções à obtenção de hegemonia dentro do sistema internacional, e também emite opiniões e previsões acerca de eventos relacionados, porém, tal abordagem, embora fundamental para o debate teórico em Relações Internacionais, não se aplica ao presente trabalho, cujo foco é mais analítico e menos teórico.

1.1.2. – CONCEITOS APLICÁVEIS

O conceito que verdadeiramente mais interessa a esta análise aplicada à tecnologia da informação é o de “(distribuição de) capacidades” de Waltz. Inicialmente, cabe um aviso importante para situar o conceito no seio desta pesquisa.

Waltz, em sua obra, *Teoria da Política Internacional*, de 1979, trata da distribuição das capacidades em ambos os níveis da análise política: Doméstica e Externa. Porém, apesar da sensibilidade em considerar o ambiente doméstico importante para discutirem-se as relações internacionais, opta-se preferencialmente pelo uso deste conceito em relação à política externa, reforçando a ideia de que o tema e a hipótese em questão são de maior interesse aos atores internacionais (Estados).

Definindo de forma solta, Waltz nos diz que o que diferem Estados dentro de um ambiente anárquico (internacional) não são os objetivos ou as tarefas que estes buscam cumprir, estes são funcionalmente semelhantes, mas sim as capacidades, superiores ou inferiores, de conseguir cumprir com tais objetivos de cada uma dessas unidades[1] (Waltz, 1979; Pg. 97). Ele também nos diz que a estrutura do sistema em si muda quando se muda a distribuição dessas capacidades entre as unidades do mesmo sistema.

[1] Waltz utiliza a nomenclatura “unidades” para se referir aos atores internacionais em questão, principalmente acerca dos Estados.

Pode-se entender então, que “capacidades” são os atributos individuais que caracterizam o que aquela determinada unidade consegue alcançar, e mais precisamente a distribuição destas, trata-se de uma espécie de medida abstrata da competência dos atores internacionais para cumprir tarefas e/ou objetivos relativamente semelhantes dentro de um sistema internacional anárquico. Waltz também argumenta que, por mais abstratas e intangíveis que pareçam essas estruturas que permitem tecer análises no campo da política internacional, um mínimo de conteúdo existe e é perceptível (Waltz, 1979; Pg. 97).

Estados, então, são basicamente diferenciados pelo poder que estes possuem. Pelas suas capacidades em obter o que lhes é interessante. E o poder, diz Waltz, é estimado através da comparação entre as capacidades de cada unidade presente no sistema, a um nível geral, e não individualmente (Waltz, 1979; Pg. 98).

Se interpretarmos, de forma plausível, que, o domínio e a ampla utilização de tecnologias da informação como recursos a serem explorados por essas unidades do sistema internacional, podemos concluir então que tais tecnologias e o respectivo *know-how* são atualmente parte do que se entende por “capacidades” de um ator internacional? Partindo dessa suposição, a análise do caso em questão e suas consequências encontram-se devidamente encaixados na base teórica proposta.

Paralelamente, de forma a complementar a discussão proposta e os questionamentos levantados nesta pesquisa, discutir-se-á de forma breve também, os posicionamentos de Waltz acerca de “poder” e “anarquia”.

Trabalhando os dois conceitos e seus desdobramentos de forma bem próxima, ele analisa os principais comportamentos que as unidades costumam ter mediante as adversidades e obstáculos impostos pelo convívio possivelmente conflituoso no sistema internacional.

As interações entre os Estados, diferentemente das interações domésticas, estão condicionadas ao sistema de autoajuda que impera internacionalmente. Ele discute que, a ausência de uma organização que subordine os Estados de forma direta, faz com que cada unidade desse sistema se incentive a buscar sua própria sobrevivência, já que não pode contar com o auxílio de qualquer outra para isso, e onde também, os Estados não se colocarão em situações de maior dependência, onde os ganhos estão subordinados a segurança própria (Waltz, 1979; Pg. 107).

Os Estados competem entre si, mas não de uma forma que a somatória de seus esforços juntam-se para o benefício mútuo das unidades, mas sim de uma forma que melhor os coloquem dentro desse sistema. Assim se entendem as considerações do mesmo sobre a “anarquia” que rege o sistema internacional. Ela apresenta-se como uma característica sistêmica, que recompensa os esforços racionais e bem distribuídos.

Ainda que, discutível sejam algumas de suas assertivas, como ele mesmo demonstra em seu livro, para efeitos de compreensão, estas conceituações servem ao propósito aqui tido. Compreendendo isto, podemos passar então a como essas unidades escolhem alinhar-se e disputar a sobrevivência dentro desse sistema.

Balança de poder talvez seja o termo que melhor explique a forma como se comportam as unidades do sistema. As teorias entendem a política internacional como um domínio de competitividade, onde nele, a sobrevivência e a manutenção dos Estados dependem da forma como cada um reage às ações dos outros. A tendência, segundo ele, é a de que mediante demonstrações de força e desenvolvimento de tecnologias, estratégias e armamentos, observe-se uma homogeneização destes espólios entre os competidores, levando a um relativo balanço de forças no sistema (Waltz, 1979; Pg. 127).

Em casos onde o balanço das forças encontra-se prejudicado, devido a disparidades destes ativos entre as unidades do sistema, ou devido a coalizões que muito favoreçam um dos lados dos possíveis conflitos em questão, Waltz argumenta que a tendência dos Estados estará em buscar o balanceamento adequado, seja se juntando a coalizão enfraquecida, que melhor valorizará os ativos destes Estados e permitirá uma melhor capacidade de dissuasão, ou buscando outras formas de evitar o conflito direto (Waltz, 1979; Pg. 126).

Com isso, ele afirma que a tendência também é a de que os Estados prefiram o balanceamento do poder, ao invés de sua maximização. Pois se preferissem o posterior, buscariam se juntar as coalizões mais fortes, e isso levaria a possibilidade de que eles se tornassem os próximos em conflito com possíveis grandes potências dentro dessas coalizões (Waltz, 1979; Pg. 126), e isso vai de encontro com a busca por segurança e sobrevivência, objetivo máximo dentro desse sistema.

“Only if survival is assured can states safely seek such other goals as tranquility, profit, and power. Because power is a means and not an end.” (Waltz, 1979; Pg. 126).

O argumento mais forte aqui é o de que o poder não deve ser o objetivo, mas apenas um meio para garantir a tão visada sobrevivência, exaltando a característica anteriormente mencionada de “defensiva”.

Por fim, compreendendo os principais pontos argumentados pelo teórico proposto para embasar esta pesquisa, pode-se então buscar compreender os termos técnicos que norteiam esta pesquisa, para então estudar e analisar o caso, os problemas envolvidos e a hipótese proposta para este trabalho de pesquisa.

CAP. 2 – CONCEITOS TÉCNICOS

Antes de adentrar profundamente no histórico do caso, e suas respectivas consequências, far-se-á um conjunto de breves explicações e conceituações a respeito de termos técnicos e específicos aos estudos de segurança, física e virtual, e termos das tecnologias das informações. Conceitos como os de “*worms*”, “*malwares*”, ”Infraestrutura Crítica”, “Vulnerabilidades *Zero-Day”,* “ciberespaço” e claro “Cyberwarfare” serão explorados aqui. Compreendendo os termos utilizados para descrever o caso, pode-se então, compor análises e conclusões mais precisas e coerentes, necessárias a esta pesquisa.

2.1. – TERMOS E CONCEITOS

Com a constante tendência a virtualização que se testemunha atualmente, cada vez mais e mais todos os aspectos da vida contemporânea estão entrelaçados as tecnologias da informação. A dependência atual das civilizações modernas de computadores, *smartphones*, inteligências artificiais e da internet no geral, apenas serve para reforçar a ideia de como segurança virtual se tornou parte fundamental das agendas e objetivos de tanto indivíduos quanto atores internacionais. Estar presente online e mundialmente nunca se tornou tão importante quanto antes. Sistemas informacionais, comunicações, e demais recursos que permitem acesso a estes passam a fazer parte de estruturas vitais aos atores internacionais.

E na mesma medida que essa tendência forneceu soluções, também trouxeram novos e requintados problemas para se pensar e lidar com. Vírus de computador, fraudes virtuais[2], Hackers, Hacktivistas[3], *Malwares*, Ataques Virtuais, etc. A quantidade de novas ameaças a segurança individual e coletiva caberia num artigo inteiro por si só. Porém, como o foco aqui se delimita a um caso específico e suas consequências ao longo de seu descobrimento, apenas uma breve exposição do que é relevante será feita.

2.1.1. – TERMOS DAS TECNOLOGIAS DA INFORMAÇÃO

A palavra *Malware*, é uma contração para o termo *malicious software*, ou "programa malicioso" numa tradução livre. O termo refere-se a qualquer programa ou código desenvolvido para obter acesso a recursos e/ou informações sensíveis, seja para roubá-los, destruí-los ou impedir o seu acesso pelo usuário original, causando ou não, prejuízos físicos ou monetários e no geral levando a perda de privacidade além de outros comportamentos ilegais ou abusivos (NASH, 2005; Pg. 11). Geralmente, este termo é utilizado para descrever qualquer tipo de programa ou processo indesejável que esteja operando num determinado sistema.

Outro termo importante para se esclarecer aqui, é o termo *worm*. Inicialmente, *worm* faz referência a um programa malicioso com a capacidade de se autorreplicar e espalhar-se por uma rede de computadores ou pela internet através de vulnerabilidades nos respectivos sistemas, sem a necessidade da intervenção de um usuário ou controlador para isso, infectando o maior número de sistemas possíveis dentro das conexões de rede ou a internet que a sua programação permitir, como exemplificado por Troy Nash, em seu estudo de caso de 2005, citado anteriormente.

Esses mesmos programas, além de possuírem essa alta capacidade de infecção, geralmente são utilizados para permitir outros tipos de atividades indesejadas nas máquinas e sistemas afetados[4].

[2] Ataques de *phishing* são os melhores exemplos de tentativa de roubo e fraude de informações, ver TROY, Nash. 2005; Pg. 11.
[3] Ver PAGET, François. 2012.
[4] Ver também SCHOCH, John & HUPP, Jon, 1982

Desde novas infecções com outros tipos de *malwares*, até permitir o controle remoto externo do equipamento afetado em questão, os *worms* servem vários propósitos quando se deseja obter acesso a um determinado sistema e/ou rede.

Uma característica frequentemente observável quando se trata desse tipo de ameaça virtual, conforme Nash nos explica, é que o programa malicioso frequentemente causa grandes aumentos no uso de tráfego numa determinada rede, devido a sua autorreplicação, causando incômoda lentidão, e em muitos casos levando a sua descoberta. Vale ressaltar também, que um *worm* age de forma diferenciada de um vírus, no qual este último necessita das ações diretas de um usuário, consciente da natureza do programa ou não (ZETTER, 2014; Pg. 15).

Uma vulnerabilidade *zero-day* (ou *zero-day exploit*) se trata de uma vulnerabilidade valiosa e previamente desconhecida em algum determinado programa ou função de um sistema operacional de qualquer computador ou equipamento similar utilizado por hackers ou *malwares* para conseguir o tão desejado acesso e/ou controle dos objetivos citados anteriormente. O principal ponto é que, diferentemente de uma vulnerabilidade comum, esses *zero-day exploits* são falhas na segurança que os fabricantes e os desenvolvedores de programas de antivírus não sabem que existem ainda, e portanto podem ter um impacto significante (ZETTER, 2014; Pg. 8).

Ainda assim, tais vulnerabilidades são raras, e requerem uma quantidade de esforço muito grande por parte tanto de hackers quanto de desenvolvedores de programas para serem encontradas, e isso as torna um instrumento de grande valor, tanto quanto nos mercados negros de softwares e *exploits* já existentes e consolidados quanto numa nova modalidade de mercado, que lembra os mais tradicionais mercados de armamentos e seus empreiteiros, onde compradores privados e governamentais se fazem presente, os chamados mercados “cinzas” (ZETTER, 2014; Pg. 9, 62, 68). Nota-se aqui, como a autora faz comparações dos conceitos e programas com os mercados de contratantes de armamentos e defesa, muito conhecidos e controversos nos Estados Unidos.

Talvez, o mais abstrato destes conceitos aqui expostos seja o de *Cyberspace* (ciberespaço). O termo em si, foi publicamente exposto pela primeira vez pelo autor da citação que abre este trabalho de pesquisa, William Gibson, em seu curto romance de 1982, *Burning Chrome*.

Mas é somente no romance de 1984, *Neuromancer*, que William Gibson, e consequentemente o termo aqui discutido, realmente ganharam notoriedade pelas suas abordagens e pelas temáticas futuristas que abordam. Ao falar de Ciberespaço, Gibson acabou por cunhar um termo que passou de um chavão artístico e de pouco sentido, a ser utilizado oficialmente por estrategistas, teóricos, oficiais governamentais e a cultura de massa no geral[5].

O termo passou então a significar de forma solta, qualquer tipo de interação que viesse a ocorrer de forma virtual, indireta, alheia aos meios já popularmente conhecidos no mundo, e ainda mais forte a crescente cultura dos computadores, que começou nos anos 80 e se expandiu fortemente pelos anos 90, com a popularização de computadores pessoais e da Internet em si. Um desses exemplos da cultura que conhecemos hoje como "Cultura da Internet", é a Declaração de Independência do Ciberespaço, de John Perry Barlow, escrita em 1994[6].

Ainda que existam definições em dicionários e plataformas governamentais e acadêmicas atualmente, não há um exato consenso sobre do que se trata o Ciberespaço, uma definição bem abrangente é a de que "The notional environment in which communication over computer networks occurs." (Oxford Living Dictionaries, 2018).

Não significa, porém, que o termo tem sua importância diminuída ou renegada, muito pelo contrário, a quantidade de flexibilidade teórica que tal fato proporciona só faz contribuir as análises propostas.

Autores da literatura específica que serão utilizados mais adiante, assim como Michael Dillon, fazem menção a como o ciberespaço evoluiu para então conceituar um domínio onde ocorrem alguns dos conflitos atualmente. Dillon (2008, Pg. 522, 523) argumenta também que as comunicações e as informações passaram por um processo de *weaponization* (armamento), onde, da mesma forma que estes se tornaram vitais para o desempenho dos sistemas e armamentos utilizados atualmente, a informação (interpretado aqui como o ciberespaço) passou a ser um domínio da guerra.

[5] Ver: https://en.wikipedia.org/wiki/Cyberspace
[6] Disponível em: https://www.eff.org/pt-br/cyberspace-independence

Com isso, é perceptível o quanto a abrangência desses termos deve ser esclarecida para que um possível leitor se situe ao comparar a problemática apresentada com as soluções que serão propostas. Tratando-se das Tecnologias da Informação, os conceitos podem ser tão fechados e complexos, quanto abertos e abstratos.

2.1.2. – INFRAESTRUTURA CRÍTICA

Infraestrutura Crítica, ou Infraestrutura Nacional Crítica[7] pode ser conceituada, através de uma combinação de definições advindas de órgãos governamentais de países desenvolvidos, como o conjunto de instalações, sistemas, processos, serviços, redes, tecnologias e ativos essenciais ao pleno funcionamento da sociedade contemporânea atual[8][9].

São indispensáveis todos estes *assets* para a manutenção da ordem e da sobrevivência das civilizações atualmente. Quando um ou mais destes são afetados e/ou desativados, existe perigo real de prejuízo a serviços essenciais, prejuízos materiais e financeiros e até mesmo consequências sociais, econômicas ou perdas humanas (CPNI-UK, 2018). Alguns setores, como o setor espacial ou o industrial de defesa, não são recorrentes em todas as três classificações aqui exemplificadas, mostrando como as particularidades de cada Estado influenciam em suas decisões estratégicas.

Ainda que com algumas diferenças na abrangência do que um determinado Estado considera uma Infraestrutura Crítica, percebe-se um padrão delineado no conteúdo de cada estratégia visualizada. Obviamente, serviços básicos como água, energia, comida e transportes, além de órgãos governamentais que prestam serviços de segurança, saúde e regulação são considerados parte desse conjunto. Mas e quanto aos outros? O que lhes configura como parte desse conjunto de essencialidades atuais?

---

[7] Este é o termo oficial usado pelo Governo Britânico para definir esse conjunto de setores. Disponível em: https://www.cpni.gov.uk/critical-national-infrastructure-0

[8] Segundo o Departamento "Homeland Security" dos EUA: https://www.dhs.gov/what-critical-infrastructure

[9] Segundo o Departamento de Segurança Pública do Canadá: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

Argumenta-se que, como anteriormente demonstrado, o comprometimento destes serviços/processos/tecnologias, possa causar impactos duradouros no cerne de uma determinada sociedade. A inclusão de serviços de comunicação e tecnologia da informação nestas estratégias muito demonstra o que foi argumentado no início deste capítulo. Estes serviços e tecnologias encontram-se tão enraizados nas necessidades atuais, que, perder acesso a eles ocasionaria os possíveis impactos já discutidos.

A importância dada a uma rede de comunicação e a serviços como a Internet ter de certa forma, se igualado a de um reator nuclear, a exemplo, pode provar isso.

2.1.3. – CYBERWARFARE

Os termos *cyberwarfare* ou *cyberwar*, usados de forma intercalada, servem como complementação ao que já foi explanado sobre ciberespaço e infraestruturas críticas. Os termos definem de forma geral, segundo o Centro Cooperativo de Excelência em Ciber-Defesa[10] da OTAN, como operações ou ataques cibernéticos autorizados ou patrocinados por atores estatais contra as redes de comunicação e os sistemas informacionais de um determinado Estado, buscando prejudicar e/ou danificar o funcionamento do mesmo, seja impedindo a execução de suas atividades ou causando danos físicos a sua infraestrutura crítica.

Em 2009, a pedido da Força Aérea Americana, a RAND Corporation produziu um extenso relatório sob a autoria de Martin Libicki, denominando, conceituando e provocando discussões a respeito das primeiras especificidades deste novo domínio do conflito internacional, onde ele nos afirma:

> "Cyberspace is its own medium with its own rules. Cyberattacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Permanent effects are hard to produce. The medium is fraught with ambiguities about who attacked and why, about what they achieved and whether they can do so again. Something that works today may not work tomorrow (indeed, precisely because it did work today)." (LIBICKI, 2008. Pg. 5).

[10] Ver: https://ccdcoe.org/cyber-definitions.html

A assertiva reforça pontos já expostos anteriormente, e traz a tona alguns pontos que serão discutidos posteriormente nesta pesquisa. Porém, o que realmente interessa ao discutido de imediato, é o fato de que o ciberespaço já se é considerado um domínio próprio onde o conflito e todos os seus desdobramentos e conceitos teóricos se aplicam diretamente ou necessitam de urgente adaptação ou completa atualização.

Diversos Estados e atores internacionais já possuem comandos especializados em suas forças de segurança domésticas e suas forças armadas para lidar com ameaças vindouras do domínio do ciberespaço.

Além de que como observamos nas fontes oficiais, maioria destes mesmos Estados possuem estratégias e doutrinas delineadas ao redor deste novo domínio[11].

Os Estados Unidos, por exemplo, possuem divisões contra crimes virtuais[12] e divisões de cibersegurança[13] bem estabelecidas em seus respectivos órgãos responsáveis, assim como o próprio Exército Americano possui sua divisão especializada em *cyberwarfare*[14].

Atualmente, o Exército Brasileiro também conta com um comando especializado neste novo e desafiador domínio da geopolítica internacional. O CDCiber, vinculado ao Ministério da Defesa (MD) tem como algumas de suas responsabilidades organizar, documentar, capacitar recursos humanos e executar a Estratégia de Defesa Cibernética vigente no país[15], mais uma vez mostrando que o domínio em questão já faz parte das agendas políticas mais importantes para os atores internacionais preocupados em manter-se relevantes.

Porém, como Libicki faz menção no capítulo dois de seu relatório e posteriormente no capítulo seis, ações de *cyberwarfare* podem ser executadas também por atores não estatais, tornando o ato de identificar e retaliar uma ação deste cunho difícil e impreciso, arriscando a possíveis escalações de um conflito.

---

[11] Ver: “International Strategy for Cyberspace, 2011” do Gabinete do Presidente dos Estados Unidos.
[12] Ver: https://www.fbi.gov/investigate/cyber
[13] Ver: https://www.dhs.gov/topic/cybersecurity
[14] Ver: https://www.army.mil/armycyber#org-about
[15] Ver: http://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/cibercidviiicedn.pdf

O fato de tais atores não possuírem precisamente um território identificável, agrava a situação, nos diz Libicki (2008, Pg. 143).

Outros autores, Paulo Shakarian, em conjunto com Jana Shakarian e Andrew Ruef, igualmente importantes e decisivos ao argumentar-se sobre os assuntos em questão, também advertem quanto ao perigo de limitar a ação virtual unicamente aos atores internacionais mais comuns, como os Estados ou organizações terroristas já reconhecidas publicamente, na obra “Introduction to Cyber-Warfare” de 2013, pois como estes afirmam, operações de grande magnitude no campo do *cyberwarfare* podem ser conduzidas unicamente por indivíduos.

Shakarian P. & Shakarian J. & Ruef (2013) também oferecem uma definição para o conceito aqui enumerado, baseado numa definição de Clausewitz para a guerra. A continuação da política através de outros meios. *Cyberwar* seria então, a continuação da política através de ações em meios virtuais. Oferecem também, uma ressalva para não se considerar toda ação com motivação política como *Cyberwar*.

A abordagem oferecida pelos autores mencionados acima, além de relativamente complexa e multidisciplinar, como adianta o subtítulo do livro, oferece uma vasta gama de exemplos de casos documentados e previamente analisados para reforçar a credibilidade da ameaça que se constitui a guerra no domínio do ciberespaço. Como esperado, o caso aqui escolhido para ilustrar os pontos argumentados, consta na listagem de ações que possuem real impacto no sistema internacional.

Retornando a Libicki (2008), ele discute ao longo de sua obra, como alguns temas e conceitos já aplicados a guerra convencional podem ser adaptados ou necessitam sofrer reformulações para ampliar o nível de conhecimento sobre este novo domínio, abordagem esta, que caberia integralmente num artigo próprio, portanto contentar-se-á com este resumo informativo. Ele também contribui a discussão oferecendo dois conceitos adicionais para compararmos o domínio virtual com o domínio real que conhecemos da guerra: *Cyberwar* estratégico e *Cyberwar* operacional.

Libicki (2008, Pg. 117,118) diz, que uma campanha de ataques cibernéticos lançados por uma nação em direção a outra e sua respectiva sociedade com o objetivo primário, porém não exclusivo, de afetar o comportamento da nação alvo é o que se chama de *Cyberwar* estratégico.

A comparação que podemos fazer aqui é com a dos ataques aéreos estratégicos da Segunda Guerra Mundial, onde um determinado ator acredita que pode se beneficiar com a disrupção e a confusão causada pela perda de acesso a um determinado recurso estratégico (fábricas e radares no caso da Segunda Guerra Mundial, sistemas informacionais e comunicações no caso atual). Podemos associar também esse comportamento, a tentativa de dissuasão entre nações conflituosas.

Já, segundo ele, *Cyberwar* operacional consiste no uso de ataques cibernéticos contra alvos militares ou alvos civis com relação militar. Argumenta também, que ainda que tal operação não constitua uso direto de força bruta, certamente é um fator multiplicador caso aplicado de forma precisa (LIBICKI, 2008. Pg. 139). Comparação semelhante que pode se estabelecer aqui, é com a característica de suporte que possui uma força aérea num conflito convencional; ainda que muito importante e eficiente caso aplicado de forma correta, é muito difícil de ganhar um conflito ou coagir uma população a se render com a utilização exclusiva deste recurso (LIBICKI, 2008. Pg. 141). Supremacia aérea durante um conflito é um fator poderoso, mas longe de decisivo caso aplicado de forma isolada.

Para encerrar essa longa, porém necessária exposição de conceitos, que permitirá traçar claros e importantes paralelos com o caso a ser estudado a seguir, retorna-se a o que Dillon (2008, Pg. 523, 524) cita em seu artigo sobre ameaças e perigos, fazendo menção direta a modalidade de conflito aqui discutida. Os processos pelos quais a informação e as comunicações, o ciberespaço em si, passaram, causaram uma revolução nos assuntos militares (*revolution on military affairs*), e essa revolução levou aos exércitos e estrategistas mudarem a forma como estes veem ameaças no mundo.

CAP.3 – O CASO DO STUXNET: RELATO E ANÁLISES

Em 2010, um novo caso de ataque cibernético começava a ganhar espaço na mídia internacional. Um programa malicioso parte de um combinado de códigos e programas denominados de Stuxnet, que aparentemente tinha como alvo, equipamentos de controle industrial, havia sido descoberto e analisado por diversas firmas privadas de segurança virtual no segundo semestre daquele ano.

E, com a identificação da origem da maior parte das infecções pelo programa advindas do Irã, e posteriormente, uma declaração pública do então presidente, Mahmoud Ahmadinejad, de que programas maliciosos haviam causado danos ao ainda larval programa nuclear iraniano, uma série de especulações e argumentações tomou conta do cenário internacional de segurança virtual, onde especialistas e teóricos emitiram declarações e opiniões acerca do que poderia ser o maior caso de *cyberwarfare* até então visto (SHAKARIAN, 2011; Pg. 1).

Stuxnet atingiu o mundo (real e virtual) de forma direta e impactante, abrindo precedentes e estabelecendo dúvidas sobre o que poderia acontecer com o mundo e suas infraestruturas críticas em eventuais casos de ciber ataques mais difusos e eficientes. Ralph Langner (2013), frequentemente em suas exposições públicas, seja via textos, entrevistas ou palestras, insiste na prerrogativa de que o *malware* é um exemplo didático de como se fazer se *cyberwarfare*, afirmando que, mesmo depois de anos, o programa continua a impressionar estrategistas, teóricos e a população em geral. Ele afirma com convicção que, o programa marca um ponto crucial de virada nos estudos e análises de segurança virtual e da história militar, onde a sofisticação empregada pelo uso do mesmo é o ponto central desse caso.

3.1. – RELATOS DO CASO

Em meio a um cenário conflituoso internacional e regional, onde o Irã, país membro de um grupo de nações com fortes opiniões contrárias a Israel e os Estados Unidos, começava a desenvolver um programa de energia nuclear, pode-se encaixar o valor estratégico que o ataque cibernético teve nesse contexto.

A autora elencada para contar os relatos e os detalhes do caso, Kim Zetter, fez em sua obra de 2014, “Countdown to Zero Day - Stuxnet and the Launch of the World’s First Digital Weapon”, uma longa e complexa exposição de todos os fatores, detalhes e elementos que compõem o histórico e as características do ataque em si. Decide-se então, que usando seus escritos, acompanhados das opiniões de alguns autores relevantes e dos relatórios oficiais produzidos sobre o mesmo, um breve resumo expositivo será aqui realizado, para então ser possível finalmente analisar a luz de todas as informações anteriormente expostas, as consequências e previsões a respeito do Stuxnet e de seus respectivos desdobramentos.

Retornando aos anos anteriores a 2010, Zetter (2014) nos conta que mediante o desenvolvimento do programa nuclear iraniano, muitas controvérsias e opiniões conflituosas foram refletidas nas discussões que occoriam internacionalmente, onde Israel, alvo direto de conflitos regionais e constante atrito com os países de maioria muçulmana na região, era veementemente contrário a aquisição por parte do Irã, de tecnologia nuclear, pois sabe-se que o que separa a tecnologia pacífica de energia nuclear da capacidade bélica, é uma linha relativamente tênua e sinuosa.

Então, ela nos diz, que as instalações nucleares iranianas eram constante alvo de fiscalização e visitação por parte de oficiais e agentes da IAEA[16] (Agência Internacional de Energia Atômica), especialmente a Planta de Enriquecimento de Combustíveis de Natanz, no centro do Irã, que havia sido recentemente instalada.

As tensões ao longo dos anos, se agravaram e se reduziram, levando a períodos de ausência de fiscalizações, até que com a assinatura de alguns acordos, chegou-se a um consenso de que, a IAEA iria fiscalizar as instalações, de forma a evitar que o país tentasse desenvolver tecnologias bélicas nucleares e de que os resíduos e materiais produzidos e enriquecidos fossem corretamente encaminhados, e não fossem desviados para usos aquém dos alegados ofcialmente pelo país.

Porém, em Janeiro de 2011, conta Zetter (2014), os oficiais da IAEA detectaram que o Irã estava removendo e substituindo centrifugas de urânio danificadas ou com mal funcionamento numa frequência alarmante, muito maior do que o esperado, ainda que a tecnologia utilizada fosse relativamente falível, os números indicavam algum tipo de problema. Inicialmente, os oficiais pensaram que a falta de conhecimento técnico e operacional por parte dos operadores iranianos era a principal causa, mas tal hipótese logo foi derrubada em favor de suspeitas maiores.

Posteriormente, diz Zetter (2014), os oficiais suspeitaram de alguma tentativa de fraudar o processo de segurança estabelecido nas diretrizes da agência, mas verificando imagens gravadas na instalação e aumentando a rotina de fiscalização, as suspeitas voltaram-se a outra possibilidade: Sabotagem. Este coincidentemente, não seria o primeiro caso de sabotagem que o programa nuclear iraniano sofreria, remetendo a um caso de componentes sabotados enviados da Turquia para o mesmo.

[16] Ver: https://www.iaea.org/newscenter/focus/iran/iaea-and-iran-iaea-reports

Porém, o que estava acontecendo ali estava tão próximo e ao mesmo tempo tão distante da atenção e do alcance dos técnicos locais e dos oficiais da agência internacional, que quase se percebe certa ironia no acontecimento. O Stuxnet, que havia infectado a rede e os sistemas da instalação, e estava continuamente sabotando o processo de enriquecimento de urânio realizado por essas centrífugas, de forma sutil porém eficiente, ao longo de vários períodos de tempo, conforme é possível entender no que demonstra Zetter (2014).

A sabotagem, que ocorria de forma silenciosa e precavida, só veio a ser descoberta depois de uma larga janela de tempo, devido a própria natureza do programa.

Conforme Zetter (2014) e Shakarian (2011) demonstram, o programa malicioso só foi descoberto em Junho daquele mesmo ano, quando uma firma privada de segurança virtual da Bielorrússia, nomeada Virus-BlokAda, que prestava serviços a uma firma do Irã recebeu uma cópia do *malware* devido a uma máquina infectada que apresentou problemas sérios. O pesquisador e atualmente especialista em segurança virtual, Sergey Ulasen, foi o primeiro a ter contato técnico direto com o programa, e em colaboração com seu parceiro Oleg Kupreev, foram os primeiros a se depararem com a complexidade técnica e lógica do *worm* que lhes fora apresentado. Não demorou muito para que novas infecções fossem encontradas ao redor da infecção originalmente descoberta.

Zetter (2014) prossegue então, dizendo que os dois programadores encontraram as falhas e os métodos que o programa utilizava para se propagar e se manter escondido de programas antivírus e operadores, e que uma dessas vulnerabilidades se tratava de um *zero-day*. Além de que, outro importante detalhe, era de que o programa malicioso utilizava assinaturas digitais válidas e certificados credenciados para conseguir se instalar nas máquinas, driblando assim alguns níveis de proteção adicionais que existiam nos sistemas operacionais mais atuais da época. Após frustradas tentativas de contatar as empresas responsáveis pelos softwares e pelos certificados provavelmente falsificados, os dois programadores decidiram apelar para os fóruns da Internet.

Não demoraria em que alguém notasse algo de errado. Padrões começavam a ser identificados, e as especulações teriam início.

O Stuxnet começava a ficar conhecido internacionalmente, ainda que primariamente através da Internet. Mas não antes, alguns pesquisadores e especialistas de outra empresa do mesmo ramo, a Symantec Corporation, empresa norte-americana com presença mundial e responsável pelo programa “Norton Antivírus”, foram incumbidos da árdua tarefa de decodificar o *malware* para tentar entender qual era o propósito do mesmo, já que diversas infecções começaram a ser identificadas em um grande número de máquinas no Irã e algumas outras em países ao redor.

Após algum tempo, apenas três pesquisadores continuaram no trabalho, nos diz Zetter (2014), Nicolas Falliere, Liam O’ Murchu e Eric Chien, enquanto que outros foram chamados a atender outras demandas de outras ameaças que surgiam naquele momento, afinal, os resultados conquistados até aquele momento eram mínimos, e mais informações deveram ser coletadas antes que qualquer conclusão pudesse ser obtida. Eles decidiram separar o *malware* em duas partes, a parte do “Míssil”, responsável por atingir os alvos, e a “ogiva” parte responsável pelos danos.

Os pesquisadores passaram algum tempo desconstruindo o que eles chamavam de a porção do “míssil” da arma digital, pois quanto mais se debruçavam sobre os métodos de infecção e propagação, mais informações preocupantes e confusas encontravam. Ao todo, Zetter (2014) informa que os pesquisadores conseguiram encontrar o total de quatro vulnerabilidades *zero-day*, o que indicava que os autores daquela ameaça não eram o típico hacker ou criminoso virtual. A possibilidade de ter quatro valiosos recursos descobertos indicava que algo maior estava por trás.

Conforme os pesquisadores e desenvolvedores adentravam nos detalhes do código impressionantemente complexo[17] e se deparavam com o fato de que quatro valiosíssimas vulnerabilidades haviam sido utilizadas sob o risco de serem descobertas e corrigidas, suspeitas começavam a apontar para possíveis criadores daquele programa, ainda que de forma tímida, Zetter (2014) informa que no mínimo a presença de recursos estatais fora considerada pelos três especialistas. Porém, isso representava uma situação incomum, inesperada. Resolvido isso, as atenções voltavam-se agora para descobrir quais eram os alvos que se buscava atingir com esse programa, considerando o fato de que a extensa possibilidade de infecções e métodos de propagação.

[17] Ralph Langner em sua palestra para o TED Conferences faz menção a aproximadamente +15000 linhas de código na composição do *malware*, ocasionando em um arquivo incomunmente pesado.

Zetter (2014) faz menção à dificuldade dos programadores e desenvolvedores em entender quais eram os alvos da "bomba digital" que eles possuíam em mãos. Vale ressaltar, que a aquele ponto, o Stuxnet já havia recebido atenção internacional dentro dos fóruns de discussão e de pesquisadores independentes, e certo grau de competição passou a existir para quem conseguiria desvendar os mistérios daquela nova e complexa ameaça.

A parte da "ogiva", porém, exigiu uma série de desdobramentos mentais maiores, onde, ainda que inicialmente fora possível descobrir quais era os alvos primários daquela ameaça. Zetter (2014), Shakarian (2011) e Langner (2013) informam detalhadamente que os arquivos e os códigos contidos na sessão da "ogiva" do programa possuíam como alvo, computadores com versões dos sistemas operacionais "Windows" da Microsoft, e com a presença de *software* do Grupo Siemens, forte conglomerado industrial alemão de tecnologia.

O que se descobriu inicialmente, é que se um determinado computador ou sistema fosse infectado e não cumprisse com tais requisitos, o *worm* não executaria sua carga maliciosa, apenas tentaria se espalhar pela rede. Porém, como diz Zetter (2014) fazendo menção a Langner (2013), havia uma boa parte da "ogiva" que não se ativava nem nas máquinas determinadas como alvo pelos pesquisadores. Este era um dos mistérios mais premiados daquela ameaça, que só veio a ser desvendado, quando Ralph Langner, nos diz Zetter (2014), passou a traçar alguns paralelos com as informações advindas de pesquisadores independentes e de reflexões pessoais feitas pelo próprio e sua equipe.

Langner, conta a autora, através de contatos e emails direcionados, conseguiu traçar paralelos com uma série de controladores industriais que poderiam ser afetados pela possível carga contida no *malware*. Através de esforços competitivos entre Langner e sua equipe, os pesquisadores da Symantec Corporation e de outros times, como o da Kaspersky Lab[18], fora possível concluir que o Stuxnet, através de deliberadamente complexos e furtivos processos, infectava redes e sistemas de computadores industriais instalados com *software* pertencente à Siemens, para então, através de arquivos infectados escritos para dar comandos a controladores

[18] Empresa russa de segurança virtual, fundada pelo controverso ex-KGB, Eugene Kaspersky, a qual contratou Sergey Ulasen, um dos programadores que descobriu o Stuxnet em 2010. Há uma entrevista do mesmo para o blog pessoal de Eugene disponível em: https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/

industriais, mais especificamente Controladores Lógicos Programáveis (PLC) que se ligavam aos mais variados tipos de equipamentos industriais, incluindo as centrifugas de enriquecimento de urânio anteriormente citadas, causar prejuízos físicos aos equipamentos, (neste caso, as centrifugas), alterando a frequência de rotação e o funcionamento de válvulas dos equipamentos, e silenciosamente desabilitando alarmes de segurança e avisos de manutenção.

Além de toda essa inacreditável especificidade e complexidade citada, Zetter (2014) ainda informa que, o programa malicioso podia ser controlado e atualizado[19] de forma remota, através de conexões a Internet por seus criadores, enviando também relatórios de dados e funcionamento dos equipamentos ligados aos sistemas. Stuxnet havia sido desenvolvido com uma engenharia semelhante à de um equipamento militar, afirma Langner (2013).

Somente isso, automaticamente levanta a uma série de questões. Como tal ataque poderia ser tão assombrosamente específico? Como as informações necessárias para obter-se tamanha precisão chegaram a seus criadores? Como foi possível utilizar tantas vulnerabilidades e processos, e ainda assim causar mínimo a nenhum dano colateral?

Foi nesse momento, em conjunto com análises forenses digitais e técnicas, e uma boa quantidade de *brainstorming*, que se chegou a uma suposição? E se o ataque tivesse sido conduzido ou diretamente patrocinado por um Estado?

Inicialmente, durante 2010, conta Zetter (2014), o governo iraniano manteve-se em silêncio acerca dos acontecimentos, ainda que cautelosamente observando a movimentação frenética que ocorria na Internet. Porém, no final daquele mesmo ano, viu-se forçado a admitir, ainda que com estimativas reduzidas, que programas maliciosos haviam causado prejuízos a seu programa nuclear.

As análises forenses conduzidas, diz a autora, principalmente pela equipe de O' Murchu, que agora contavam com a cooperação com Langner e sua equipe, revelaram alguns pedaços de informações preocupantes para os envolvidos.

[19] Segundo os autores mencionados, Langner e Zetter, diversas versões do programa foram encontradas nas redes e sistemas infectados, com correções e leves alterações entre versões;

Resquícios de informações demonstraram que parte dos códigos e métodos utilizados, assim como a utilização de certificados confiáveis apontavam para os Estados Unidos e Israel, como autores do ataque.

O desenvolvimento da geopolítica naquele momento, conforme o informado pela autora e citado no início deste capítulo parece confirmar isso. Porém, como nenhuma proclamação oficial foi feita por ambos os Estados, ainda que Zetter (2014) aponte para algumas "dicas" dadas por ex-oficiais dos supostos órgãos governamentais envolvidos que foram entrevistados, muito se discute ainda.

Respondendo a algumas das perguntas anteriores, reunindo os dados apresentados tanto por Zetter (2014), por Shakarian (2011) e por Langner (2013), além do muito que se pode extrair do relatório completo acerca do Malware publicado por O' Murchu e seus colaboradores pela Symantec[20], pode-se afirmar o seguinte:

Algum tempo antes da liberação do Stuxnet no mundo, estimado em 2009, os seus criadores utilizaram-se de métodos semelhantes para coletar as informações necessárias para possibilitar um ataque da dimensão e capacidade do mesmo. As análises forenses, conjuntamente com a coleta de "espécies" do *malware* levaram a descoberta de semelhante programa que, batizado de "Flame", foi utilizado para coletar dados acerca das instalações de infraestrutura crítica pertencentes ao programa nuclear iraniano.

Esse programa coletou detalhes e dados a respeito de equipamentos, rotinas, funcionamento, manutenção e qualquer informação que fosse relevante ao sucesso do objetivo de sabotar o programa. O mais curioso é que, este *malware* foi utilizado como um batedor, em busca de efetuar o reconhecimento do terreno em que a missão se daria, novamente traçando paralelos a guerra convencional.

Da mesma forma, este programa que antecedeu Stuxnet, utilizou-se de métodos muito eficientes para propagar-se, evitando vestígios e incompatibilidades que viessem a causar sua descoberta. O ponto aqui é a expertise com a qual foram projetados estes programas; onde transferência direta e controle remoto dos mesmos são fatores potenciais para qualquer operação que busque discrição.

[20] Disponível em: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Por fim, Stuxnet foi criado com um objetivo e alvo específico, guiado por inteligência profissionalmente coletada, com a maior eficiência (ainda que haja controvérsias nesse ponto) em mente. O *malware* foi projetado para espalhar-se rapidamente, mas em redes limitadas, possuir uma data limite de funcionamento, e atingir em cheio unicamente o seu alvo designado, de forma a evitar danos colaterais que viessem a ocorrer na sua descoberta. Shakarian (2011) afirma que o programa obteve sucesso, ainda que discutível, em sua missão, e argumenta de forma incisiva que, este se provou uma revolução na maneira de se pensar os assuntos militares, forçando Estados a evoluírem para se manterem relevantes.

3.2. – ANÁLISE DO CASO

A problemática proposta por este artigo e apresentada de forma embasada pelos autores citados e referenciados pode ser resumida em três pontos principais:

Primeiro: Stuxnet é uma revolução dos assuntos dos assuntos militares. Shakarian (2011) diz que, o programa malicioso exemplifica pela primeira vez de forma extensivamente analisada e documentada, o caso de uma arma digital ser utilizada com relativa eficiência contra um alvo de infraestrutura crítica de um determinado Estado.

Os métodos desenvolvidos e utilizados para os fins pelo *malware*, já representam um grande avanço tecnológico em si, o objetivo para os quais ele foi utilizado representam um novo e complexo desafio para os responsáveis em pensar política e estratégia, conforme também afirma Dillon (2008) ao falar da revolução dos assuntos militares que consiste o armamento das comunicações e da informação em si. A forma como Estados tratam segurança, agora deve levar em conta também, o ambiente virtual e as comunicações.

O programa malicioso, traçando paralelos necessários a teoria realista estrutural das Relações Internacionais, apresenta-se como uma capacidade em si. A utilização de um *malware* para causar prejuízos a alvos estratégicos, primariamente militares, de um determinado Estado com o objetivo de prejudicar ou alterar a atuação daquele ator específico, pode ser facilmente encaixado sob o conceito de *cyberwar* operacional explanado por Libicki (2009), que consequentemente está coberto pela conceituação de capacidades, pertencente à Waltz (1979).

É perceptível a importância que o domínio do ciberespaço passa a ganhar com a constante evolução das ameaças virtuais. Stuxnet marcou o ponto de virada acerca da forma que se define *cyberwarfare* (Langner, 2013.), mas não é o primeiro, e nem o último ataque cibernético com objetivos medidos e guiados.

Ainda que se questione, através de comparações com métodos tradicionais, como diz Langner (2013) a eficiência que este ataque teve, é preciso ter em mente que, o ataque possuía a característica de ser limitado em si. O objetivo, traçando um vago paralelo aqui, não era a maximização dos estragos, que poderia resultar em retaliações ou acusações, mas na ambiguidade proposital, que somente um ataque deste cunho seria possível de atingir. O campo está aberto para nova ameaças.

Segundo: Stuxnet invalida algumas das principais assertivas acerca de segurança virtual. Shakarian (2011) também diz que, a assertiva que diz que sistemas isolados são mais seguros que sistemas conectados acaba por se tornar inválida quando consideramos os principais métodos de infecção pelo qual o *worm* se propaga. Através de várias programações e da exploração de brechas e vulnerabilidades *zero*-day, já mencionadas como um produto valioso dentro dos mercados negros e "cinzas" de segurança virtual, este conseguiu se infiltrar dentro de sistemas industriais indiretamente conectados.

Os PLC que foram afetados, não se conectam diretamente as redes do ambiente, conforme se pode observar no relatório da Symantec por Falliere & O' Murchu & Chien (2011), onde na sessão de "Attack Scenario" eles descrevem o provável caminho que o *malware* fez de forma a conseguir infectar o controlador industrial, seguindo um processo de infecções indiretas, onde o próprio usuário indiretamente torna-se cúmplice do processo. O menor descuido seja através do uso de aparelhos e computadores infectados (falhas humanas) ou da permissividade de aparelhos não atualizados ou com brechas de segurança permite a propagação do programa.

Vale também ressaltar que, conforme demonstra Langner (2013) tal ataque foi planejado cautelosamente, tendo em consideração as fases de transição entre máquinas e sistemas, considerando as barreiras que precisavam ser transpostas para atingir os níveis desejados, até o nível de controle físico, onde o estrago pode ser causado.

Outra assertiva invalidada de imediato, demonstrada por Shakarian (2011) é a relação de confiança estabelecida que o sistema de certificados de confiança e assinaturas digitais que incorporam os mais variados tipos de programa dentro das tecnologias da informação possuem. A possibilidade de se falsificar assinaturas digitais e fornecer certificados de confiança para programas maliciosos já abre em si um grande problema de confiança para as tecnologias atuais.

A existência desse tipo de certificação nos conta o autor, serve justamente para dificultar a criação e propagação de *malwares* capazes driblar as seguranças já existentes. Subverter esse processo e torná-lo uma janela para ameaças, diretamente afeta o futuro das tecnologias envolvidas, onde revisões dos processos e dessa relação, já utilizados precisam ser consideradas de forma imediata.

Por último: A dificuldade de se prover respostas adequadas a essa nova categoria de ameaça e o futuro aberto pelo Stuxnet. Ainda que, como já citado anteriormente, o acontecimento de 2010 tenha forçado Estados, organizações internacionais e privadas a abrirem seus escopos e enxergarem no domínio do ciberespaço uma força nova e potencialmente *game-changing*, ainda percebe-se certa dificuldade de muitos destes em lidar tanto com a geração atual de ameaças quanto as possíveis futuras.

Ainda existe forte resistência tanto por parte de pensadores e teóricos quanto por parte de *policy-makers* e estrategistas em considerar o real peso da atuação virtual atualmente. Como se observa na história, e nos escritos de Waltz (1979) somente aqueles preparados para adequar-se as novas tecnologias e a distribuição das capacidades no sistema poderão atingir o objetivo máximo possível, que é a sobrevivência num meio complexo e cada vez mais fluído.

Utilizando-se de algumas comparações feitas por Shakarian (2011), é possível compreender a fluidez desse novo meio.

Em 2008, durante a guerra russo-georgiana, um bom número de ataques cibernéticos foi utilizado pela Rússia para desabilitar as infraestruturas das comunicações georgianas, e facilitar a invasão e o controle do território tomado.

Porém, diferentemente do Stuxnet, a Rússia utilizou ataques de DDoS[21] e métodos mais simples para atingir seus objetivos.

O ataque do Stuxnet representa uma evolução considerável na forma de se usar o virtual para causar disrupção no real (físico). Com os ataques se tornando cada vez mais sofisticados, as vulnerabilidades exploradas cada vez maiores e mais frequentes, e os alvos cada vez mais físicos e próximos, exemplifica Shakarian (2011), Stuxnet marcou a evolução de um método de se fazer guerra. A utilização de uma arma virtual, um amontoado de códigos e programas conseguiu causar danos físicos a uma instalação de infraestrutura.

Além disso, questões são levantadas. Quais os precedentes internacionais que tal ataque abre se tratando das formas convencionais de retaliação e resposta? Qual o verdadeiro impacto de se promover *cyberwar*? O quão centrado no Estado essa nova modalidade realmente é?

CONCLUSÃO

Entende-se que, cada vez mais o funcionamento da sociedade e de seus respectivos governos e estruturas burocráticas estão atrelados ao vasto uso das tecnologias da informação que dominam o nosso ambiente, portanto, a existência de uma ameaça tão significativa como a do Stuxnet, como classificaram alguns dos principais autores citados anteriormente, capaz de causar disrupção em sistemas físicos através do meio virtual exemplifica a crescente necessidade de se melhor e mais abrangentemente estudar e tentar combater essas ameaças, ainda que contraditoriamente, os próprios Estados muitas das vezes patrocinem e utilizem essas ferramentas e as vulnerabilidades por elas exploradas.

Ainda assim, a necessidade de prover respostas adequadas por parte das unidades e atores que possam ser alvos de ataques semelhantes existe e é de caráter urgente, já que, como afirmou Shakarian (2011), tais ataques possuem características inerentes que lhe permitem ser executados não somente por amplas estruturas estatais, mas também por indivíduos e por grupos privados com interesses em desestabilizar um governo ou alterar seu curso de ação, semelhante a manobras dissuasivas realizadas pelos próprios atores estatais.

[21] Distributed Denial of Service (Negação de Serviço Distribuída); Ver: BHATTACHARYYA, Dhruba Kumar. KALITA, Jugal Kumar. DDoS attacks: evolution, detection, prevention, reaction, and tolerance. CRC Press, Estados Unidos, 2016.

Portanto, ao lidarmos com um ataque do grau de capacidade que foi o Stuxnet, levar em conta somente as noções mais tradicionais de conflito e suas resoluções acabam por se tornar insuficiente, vide o discorrido ao longo do capítulo dois acerca da teorização a respeito do *Cyberwarfare* e suas procedências.

Então, ao somar-se o fator descentralizado da origem deste ataque, a capacidade envolvida e a dificuldade de então se prover respostas adequadas tanto para as consequências quanto para o ataque em si, alguns problemas ainda permanecem pertinentes a essa questão. Este ataque, obviamente, não se trata de um caso isolado ao buscar-se o histórico de ataques semelhante, e as possibilidades levantadas pela sua execução são várias. A utilização do Stuxnet, ainda que de forma não assumida, por um Estado para afetar outro, em si, já é uma problemática considerável.

As linhas traçadas e cruzadas pelo *malware* são frágeis e demasiadamente complexas, e o caso abre precedentes perigosos e confusos a respeito de identificar ameaças e providenciar dissuasões ou retaliações adequadas. Dessa forma, cada passo dentro deste novo e inexplorado território requer cautela e discrição, das quais só será possível obter mediante cautelosa observação, análise e (re) formulação de teorias e conceitos.

Stuxnet pode ter aberto precedentes internacionais para ataques cada vez mais devastadores e prejudiciais a vida humana, definitivamente levantando dúvidas a respeito desse novo método de se guerrear, tanto quanto a cerca de sua real eficiência, quanto a de sua suposta “moralidade”. Não existem “regras de combate” tão claras e edificadas em tratados internacionais para este novo campo de batalha.

REFERÊNCIAS BIBLIOGRÁFICAS

BHATTACHARYYA, Dhruba Kumar. KALITA, Jugal Kumar. DDoS attacks: evolution, detection, prevention, reaction, and tolerance. CRC Press, Estados Unidos, 2016.

DA COSTA, Max Mauro. JÚNIOR, Jair de Oliveira. JÚNIOR, Paulo Varela. BENÍCIO, Alberto Ayres. A POLITICA DE SEGURANÇA DA INFORMAÇÃO: UMA ANALISE DA RCA 025/2009 SICOOB CREDIP. 2009, SICOOB.

DILLON, Michael G. What Makes the World Dangerous? In: Global Politics: A New Introduction. Routledge, Londres, 2008. pg. 397-426

DONNELLY, Jack. Realism and International Relations. Cambridge University Press, 2004.

FALLIERE, Nicolas. O' MURCHU, Liam. CHIEN Eric. W32.Stuxnet Dossier. Symantec Security Response, Fevereiro de 2014.

FRANCO, João Henrique de A. Proteção da Infra-estrutura Crítica de Telecomunicações. 04 de março de 2008, ANATEL, www.cpqd.com.br.

KARNOUSKOS, Stamatis. Stuxnet Worm Impact on Industrial Cyber-Physical System Security. 2011, SAP Research, Alemanha.

LANGNER, Ralph. To Kill a Centrifuge; A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Novembro, 2013. The Langner Group.

_____. Cracking Stuxnet, a 21st-century cyber weapon. TED2011 Conference. March 2011. 10mins e 40segs. TED Conferences, LLC.

LIBICKI, Martin. Cyberdeterrence and Cyberwar. RAND Corporation, Estados Unidos, 2009.

NASH, Troy. An Undirected Attack Against Critical Infrastructure; A Case Study for Improving Your Control System Security. Vulnerability & Risk Assessment Program (VRAP), Lawrence Livermore National Laboratory. Setembro, 2005.

PAGET, François. Hacktivismo: O ciberespaço tornou-se a nova mídia para vozes políticas. McAfee Labs, 2012.

PRIOR, Tim. Measuring Critical Infrastructure Resilience: Possible Indicators, Risk and Resilience Report 9. Risk and Resilience Research Group Center for Security Studies (CSS), ETH Zürich. Abril, 2015.

SHAKARIAN, Paulo. Stuxnet: Cyberwar Revolution in Military Affairs. Small Wars Journal, Abril, 2011. smallwarsjournal.com

SHAKARIAN, Paulo. SHAKARIAN, Jane. RUEF, Andrew. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Newnes, 16 de mai de 2013.

SCHOCH, John. HUPP, Jon. The "worm" programs—early experience with a distributed computation. Communications of the ACM CACM, Volume 25, Edição 3. Nova Iorque, Março 1982.

VASQUEZ, John A. The Power of Power Politics – From Classical Realism to Neotraditionalism. Cambridge University Press, 2004.

WALTZ, Kenneth N. O homem, o Estado e a guerra: uma análise teórica. São Paulo: Martins Fontes, 2004.

_____. Man, the state and war. Nova York: Columbia University Press, 2001.

_____. Theories of International Politics. Londres: Addison-Wesley, 1979.

ZETTER, Kim. Countdown to Zero Day - Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers, Nova Iorque, 2014.