A TEMÁTICA DA CYBERWAR NO CONTEXTO DAS RELAÇÕES INTERNACIONAIS: CONCEITOS E CASOS MAIS RELEVANTES NO CENÁRIO INTERNACIONAL

Bruno Marcos da Silva Miranda[1]

RESUMO

O referido artigo é um debate ao tema da segurança internacional no tocante as questões que envolvem a Cibersegurança. Inicia-se por uma abordagem teórica em Relações Internacionais quanto à corrente do Realismo Político, a qual fundamenta o pensamento defensivo e ofensivo nas políticas beligerantes, para em seguida se construir os conceitos fundamentais da Ciberguerra, bem como sua dimensão na arena internacional. Por fim, são analisados os contenciosos mais famosos e relevantes já observados mundialmente.

Palavras-chave: Ciberguerra, Cibersegurança, Ciberespaço e Ciberataque.

ABSTRACT

This article is a debate on the theme of international security with regard to issues involving cybersecurity. It starts with a theoretical approach in International Relations as to the current of Political Realism, which bases the defensive and offensive thinking in belligerent policies, to then build the fundamental concepts of Cyber War, as well as its dimension in the international arena. Finally, the most famous and relevant litigations observed worldwide are analyzed.

Key words: Cyberwar, Cybersecurity, Cyberspace and Cyberattack.

[1] Mestrando. Universidade de Brasília (UnB), Brasília – DF, Brasil. E-mail: bmsmiranda@gmail.com / ORCID: https://orcid.org/0000-0001-5249-3140

INTRODUÇÃO

Uma crescente preocupação da comunidade internacional tem se equacionado diante aos desafios de proteção e prevenção necessários para se fazer frente às ameaças sofridas no Ciberespaço, ou como é comumente referenciado: ambiente virtual. Especialistas divergem sobre termos e conceitos do ambiente *Cyber*, ou seja, a comunidade acadêmica e a esfera do poder público / governamental possuem relativa dificuldade em esclarecer a relevância e as fragilidades neste ambiente sob a ótica da segurança nacional. A Ciberguerra, portanto, emerge como consequência natural desta equação, onde Estados-nação, organizações, grupos ou indivíduos solitários sem causas específicas, se encontram em constante clima belicoso em um exercício diário de defesa e ataque.

Sistemas de barreiras, fronteiras e simulação virtual tem se tornado prioridade para os Estados-nação em matéria de Cibersegurança, onde não apenas proteger a si próprio dos possíveis ataques e ameaças é a única prioridade, mas também obter (de terceiros) dados e informações, ou ainda monitorar seus parceiros e inimigos faz parte das diversas estratégias adotadas (ANDRADE et al., 2019).

Ademais, como definir uma guerra de informações? Quais as implicações de uma possível Ciberguerra no contexto das relações internacionais? Quais foram os casos mais relevantes no cenário internacional e suas consequências? Tendo como nítido o clima de evolução na tratativa das questões de segurança nacional, bem como a emergência dos conceitos aqui explicitados, este artigo tem por objetivo examinar e esclarecer fatos relevantes na temática da Cibersegurança à luz das relações internacionais (RI), onde também se buscará responder as questões aqui expostas.

A primeira seção do artigo está dedicada a uma tratativa teórica ao tocante dos conflitos e contenciosos entre as Nações sob a luz da teoria das relações internacionais, bem como aos desafios impostos a uma sociedade conectada em rede e que faz uso de serviços computacionais providos e criados pela Tecnologia da Informação (TI) para a automação de atividades na esfera dos serviços públicos.

Já na segunda seção discutem-se os conceitos relacionados ao universo *Cyber*. Ainda, discute-se o papel da Cibersegurança, do seu uso como ferramenta de espionagem / defesa e obtenção de informações, e também sua contextualização aos temas das relações internacionais, trazendo ainda uma abordagem analítica sob o prisma da *Cyberwar* (guerra cibernética).

Para a terceira seção do referido artigo, dedicou-se um esforço de reflexão sobre os contenciosos mais relevantes - sob a ótica de danos e constrangimentos ocasionados -, já ocorridos na agenda da Cibersegurança em um contexto global.

Por fim, a seção dedicada à conclusão irá expor os aspectos finais do trabalho e realizar as análises pertinentes ao tema.

RELAÇÕES INTERNACIONAIS EM TEMPOS DE CRISE

É natural que novas agendas das RI surjam para dar respostas mais equilibradas e apropriadas às mudanças que a sociedade e os novos tempos exigem. O que se vê, é uma contestação e quebra das duas grandes estruturas mundiais do passado: a primeira, uma ordem mundial liberal sob a liderança e hegemonia europeia; a segunda, a ordem mundial da Guerra

Fria, onde agora, ambas suplantadas pelos eventos históricos e mudanças irreversíveis no cenário mundial (SARAIVA, 2012).

> Assim, embora no pós-Guerra Fria tenham os conflitos interestatais declinado significativamente, aumentaram a violência difusa e os conflitos não convencionais, colocando à prova os mecanismos de segurança coletiva concebidos após a Segunda Guerra para a promoção da paz e da estabilidade no plano internacional, mas que agora foram convocados a responder a conflitos de natureza distinta. Ao mesmo tempo, intensificaram-se os desafios correntes de fenômenos de natureza e alcance transnacional, da mudança climática à (in) segurança cibernética e cuja crescente importância alimenta, por sua vez, a necessidade e a demanda por novos mecanismos de governança nos planos regional e global (VAZ, 2012, p.14).

Conforme observado por Saraiva (2012) e complementado por Vaz (2012), uma nova ordem mundial, baseada nas novas necessidades, sobretudo em questões nascentes de segurança precisa ser construída, lapidada e fortalecida para enfim se chegar a um modelo de governança global digno dos desafios do século XXI. É possível, portanto, perceber uma nova ordem em construção, a qual precisa ser adaptativa, participativa, inclusiva e não estática.

Desse modo, é no Realismo que se encontra maior alinhamento teórico para a exploração do tema da defesa em RI, sobretudo do seu componente ofensivo no constructo de um sistema de segurança para os Estados.

Para fins de síntese e sem a pretensão de explorar o aspecto teórico dessa corrente com a profundidade que esta merece, pois, a referida análise está fora do escopo deste artigo, abordam-se no quadro 1, os aspectos do Realismo Político em suas quatro categorias, cada qual sintetizada em suas características definidoras (JACKSON; SORENSEN, 2013).

Quadro 1. Aspectos definidores do Realismo Político.

Categoria	**Descrição**
Clássico	Vertente baseada no poder, ou seja, a política de poder será o cerne das questões de decisão. Como cada Estado-nação é assimétrico em suas diversas categorias (militar, dimensão territorial, potenciais econômicos), trabalha-se com o conceito de balança de poder.
Estrutural (Neorrealismo)	É pautado no conceito de Sistema Internacional como estrutura anárquica, ausência de autoridade superior aos Estados. Neste sentido, um Estado não terá como reivindicar a uma autoridade de segurança, uma determinada situação de agressão. Acredita-se que a defesa virá por suas próprias capacidades dissuasórias.
Defensivo	A busca *a priori* é a de defesa das ameaças. Trabalha sempre pautado na possibilidade de autodefesa, sendo necessária sempre a construção de uma quantidade de poder para defesa. É neste sentido que pode ser conjugado a possibilidade de trabalhar em cooperação, onde um Estado se alia com seus parceiros em prol do bem comum e da auto sobrevivência. Exemplo clássico aplicado na Primeira Grande Guerra Mundial, onde a França, Inglaterra e Rússia, se uniram formando a Tríplice Entente, cooperação de caráter defensivo.
Ofensivo	Apontado como o mais "realista" dos realismos, acredita em um potencial não apenas dissuasório das capacidades de segurança. Opera sob cinco pressupostos teóricos, sendo estes: a) Anarquia do Sistema Internacional (SI); b) Existência de Potências; c) Incerteza das reais intenções das outras grandes potências; d) Interesse primordial é a sobrevivência das Grandes Potências; e) Racionalidade.

Fonte: Elaborado pelo autor com base em Jackson e Sorensen (2013), Nogueira e Messari (2005).

Por meio da análise do referencial teórico exposto, é possível perceber e traçar um paralelo deste com as decisões de um Estado em sua busca e promoção da própria hegemonia global ou regional, utilizando desta doutrina como um ferramental deveras importante na conquista do incremento de seu poder relativo frente às outras Nações. Quase em uma estrutura de luta, ou, como bem coloca Mearsheimer (ROCHA, 2002), uma balança de poder. Nesta

perspectiva, o poder relativo poderá ser maximizado de duas formas: a) Busca por ganhos de poder relativo; b) Contenção de ganhos de poder relativo das demais potências.

Porém, conforme salienta Saraiva (2012), há fraqueza no léxico herdado por partes dos realistas, sobretudo, no contexto da segurança, haja vista por exemplo, a não previsibilidade do fim da Guerra Fria ou mesmo do grande ataque terrorista de 11 de setembro de 2001 contra os Estados Unidos (EUA). Fatos estes que fortalecem a diversidade de questionamentos constantemente impostos a essa corrente de pensamento.

Desse modo, a teoria do poder relativo arraigado no conceito de balança de poder, na visão de "todos contra eles" – sendo um modelo de viés armamentista -, se demonstra obsoleta frente aos desafios impostos na arena internacional contemporânea, desafios estes próprios do século XXI. Ademais, a visão de que os países desenvolvidos eram fornecedores de valores superiores ocidentais às Nações menos desenvolvidas, demonstrou-se conceito equivocado, onde tal concepção retrógrada deixou até hoje um legado negativo de dependência para as Nações em desenvolvimento (SARAIVA, 2012). Ou seja, há grande descolamento da realidade atual para com este pensamento anterior, deixando assim uma lacuna no processo de crescimento destes países (em desenvolvimento) antes recebedores de recursos e "suporte".

A depender de sua capacidade individual dissuasória, cada Estado poderá ainda lançar mão de parcerias no âmbito da defesa nacional, fator evidenciado pela perspectiva do Realismo Defensivo (JACKSON; SORENSEN, 2013). Não obstante, tais parcerias em geral vêm no bojo de um forte relacionamento noutros campos de cooperação, uma vez que são temas sensíveis à cada Nação, conforme o caso observado das relações Brasil-EUA:

> The United States and Brazil enjoy robust political and economic relations. The United States was the first country to recognize Brazil's independence in 1822. As the two largest democracies and economies in the Western Hemisphere, the United States and Brazil have a partnership that is rooted in a shared commitment to expand economic growth and prosperity; promote international peace, security, and respect for human rights; and strengthen defense and security cooperation (EUA, 2019, p.1).

A saber, Brasil e EUA por meio do acordo de cooperação *"U.S.-Brazilian Social Security Agreement"*, firmado por ambos os países em 2015 (SOCIAL SECURITY, 2015), possuem sólida parceria no campo estratégico da defesa nacional, para ficar apenas no exemplo da parceria Brasil-EUA.

De toda forma, quando da não parceria institucionalizada na temática da segurança, os países podem ainda lançarem mão de acordos de não espionagem e/ou não intrusão (minimamente) para com os seus parceiros comerciais, como os casos envolvendo os EUA e a Alemanha, e novamente, dos EUA com o Brasil, por exemplo. Porém, em ambos os casos ocorreram contenciosos delicados de violação do acordo por uma das partes justamente na arena cibernética (TAPPER, 2015), a saber, os Estados Unidos, segundo Roberts (2015).

Traçando um paralelo entre a perspectiva do realismo nas RI e o tema da Cibersegurança proposto para o referido trabalho, não é de se admirar que as grandes potências sejam auto defensivas e maximizadoras de seu poder relativo. Utilizam-se, portanto, de todo o ferramental possível para não apenas defender-se das ameaças, mas também de sua capacidade ofensiva para frear o desenvolvimento da capacidade dissuasória do vizinho, ou seja, conforme prega o realismo ofensivo por John Mearsheimer (ROCHA, 2002).

Mas afinal, qual a necessidade de se construir sociedades conectadas? É mesmo possível em era tecnológica - da atualidade - possuir acesso a todos os recursos tecnológicos com relevante segurança e privacidade? Por que as mudanças tecnológicas hoje são mais

perceptíveis que antes? O que há de novo nesse contexto? Talvez Kissinger (2015) tenha conseguido resumir em poucas palavras as inquietações aqui colocadas, "O que há de novo na era atual é o ritmo da mudança proporcionado pelo poder dos computadores e a expansão da tecnologia da informação para todas as esferas da existência".

> A revolução na computação é a primeira a reunir um número tão grande de indivíduos e processos sob a ação do mesmo meio de comunicação e a traduzir e rastrear suas ações numa única linguagem tecnológica. O ciberespaço — uma palavra cunhada, àquela altura, como um conceito essencialmente hipotético, ainda na década de 1980 — colonizou o espaço físico e, pelo menos nos grandes centros urbanos, começou a se fundir com ele. A comunicação através dele, e entre seus nódulos que têm se proliferado em escala exponencial, é quase que instantânea. (KISSINGER, 2015, p.297)

Usando um pouco mais de ênfase e com mais de quinze anos de antecedência, porém, na mesma linha de Kissinger (2015), ressalta Castells (1999) em sua obra clássica, sua visão do que viria a se tornar a grande revolução provocada pelos meios tecnológicos na sociedade.

> Meu ponto de partida, e não estou sozinho nessa conjetura, é que no final do século XX vivemos um desses raros intervalos da história. Um intervalo cuja característica é a transformação de nossa "cultura material" pelos mecanismos de um novo paradigma tecnológico que se organiza em torna da tecnologia da informação. (CASTELLS, 1999, p.67)

Para os céticos, é bom reforçar que a palavra por Castells utilizada foi mesmo "revolução", ao dar a dimensão dos fatos que a TI proporcionou entre mudanças e quebras de paradigmas, "o exagero profético [...] que caracteriza a maior parte dos discursos sobre a revolução da tecnologia da informação não deveria levar-nos a cometer o erro de subestimar sua importância verdadeiramente fundamental" (CASTELLS, 1999, p.68). Nesses termos, o dado gerado por cada transação e em cada serviço utilizado em rede, toma a conotação de um bem precioso, o qual por vezes pode também se tornar alvo dos ataques cibernéticos gerados.

Há muito se define que o dado, grosso modo, é a matéria-prima da informação, onde para os dias atuais - à luz do século XXI -, ele representa o novo petróleo[2] no cenário da competição internacional, dizem estudiosos do tema (THE ECONOMIST, 2017). Porém, apesar de tal conceito ter se demonstrado verdadeiro e resistente às desconfianças naturalmente impostas, os desafios de sua manutenção têm se demonstrado enormes.

A saber, os milhões de dados gerados diariamente por usuários de mídias e redes sociais, se analisados e compilados para determinados fins, tem sido capaz de elevar certos graus de discussão em temas abertos na sociedade, tais como, estimar / vislumbrar possíveis eventos adversos, realizar mobilizações sociais contra regimes e partidos ou até mesmo abalar um sistema partidário e eleitoral de uma Nação (CASTELLS, 2017). Como fora visto na história recente, dois antigos inimigos políticos, EUA e Rússia, acabaram se envolvendo em um contencioso cibernético durante a eleição presidencial de 2016 naquele país, onde o resultado de uma possível interferência cibernética teria dado vantagens ao candidato vencedor do referido pleito, Donald Trump (HARDING, 2016).

O poder da informação e sua velocidade de propagação mudaram radicalmente a política mundial, o mercado financeiro internacional, a forma de se fazer jornalismo, a construção de

[2] A propósito, é importante salientar que tal comparação tomou por base o contexto de uma supervalorização dessa commodities na matriz energética mundial predominante a partir do século XX, e de certo modo vigente até os dias atuais.

conhecimento técnico-científico, a democracia, as representatividades nas questões sociais e o modo de vida de maneira geral (CASTELLS, 2017). Portanto, não é de se surpreender que no contexto das relações internacionais o impacto também fora singular e marcante.

OS CONCEITOS DO UNIVERSO CYBER E SUA DIMENSÃO NA ARENA INTERNACIONAL

Difícil é a tarefa de sistematizar conceitos ainda em construção e/ou transformação. Assim é para o conceito da dimensão ciber para a análise das questões que envolvem aspectos tais como: a) Delimitação de fronteiras físicas e lógicas; b) Segurança internacional; c) Privacidade / segurança de dados; d) Manutenção e fortalecimento da democracia; e) Proteção e difusão de conhecimento e informações; para citar apenas alguns.

Ciberespaço (do inglês *Cyberspace*) é uma terminologia que surge para definir o conjunto das interações entre os indivíduos, tecnologias, processos, telecomunicações, máquinas e protocolos, sendo intermediados por sistemas informáticos e interconectados na rede mundial de computadores, a internet.

> Although the concept of cyberspace is plastic and contentious, our purposes can be served if cyberspace is defined as analogous to the Internet. Cyberspace, as such, can be characterized as an agglomeration of individual computing devices that are networked to one another (e.g., an office local-area network or a corporate wide-area network) and to the outside world. This is not meant to be a comprehensive definition; the distinction between a cell phone network and the Internet is becoming harder to make with every day. (LIBICKI, 2009, p.31)

Fato é que a sociedade acompanha novos hábitos e anseia por necessidades crescentes de bem-estar por parte dos indivíduos. O que não necessariamente quer dizer que tais mudanças tragam sempre benefícios.

> Um computador é uma máquina fantástica. Com sua ajuda, foi possível ao homem pousar na lua, iniciar expedições exploratórias interplanetárias, mapear o genoma humano e criar a Internet – o ícone da modernidade que, de forma muito veloz, está derrubando todos os muros existentes entre os países (sic). Com os computadores podemos, ainda, criar sistemas que podem integrar e automatizar tudo o que ocorre no interior de uma empresa; enfim, disponibilizar um grande volume de informações que podem literalmente afogar o ser humano (MORAES, 2001, p.5).

Interessante a abordagem que Moraes (2001) usa em sua definição, ao que se possa dizer, da modernidade e da conectividade que a atrai. Por um lado, a beleza do advento da tecnologia, do outro a sensação de transbordamento, de afogar-se em algo que veio para ajudar, amparar e inovar, mas que agora adverte com uma sensação de insegurança e por vezes impotência em criar meios de frear as externalidades negativas[3] ocasionadas durante o processo evolutivo.

Para Hundley e Anderson (1995), é na característica do anonimato que grupos mal-intencionados e bem preparados tecnicamente, se armam para cometer ilícitos por meio do

[3] Externalidades são eventos (ações) que podem ocorrer como fruto de uma atividade de produção ou de consumo e que não são capturados pelo preço de mercado. Onde estas recebem ainda a classificação de positiva, caso seus efeitos sejam benéficos para os agentes, ou negativa, para o caso contrário ocorra.

ambiente virtual. Entende-se por ilícitos as ações de: a) Obter dados e informações sigilosas de maneira ilegal; b) Promover insegurança dos dados de usuários de serviços *online*; c) Constituir ataques em massa para fins de negação dos serviços tecnológicos de terceiros; d) Espionagem.

Ainda segundo os autores referenciados, por vezes a distinção entre tais tipos de crimes é difícil de ser feita, fato que confunde e dificulta o papel das autoridades responsáveis por executar uma investigação e detenção dos culpados. Por vezes, os ataques são realizados por meio de máquinas infectadas por *softwares* maliciosos que dão uma espécie de cobertura às ações dos criminosos ou até mesmo potencializam os ataques feitos, como a já conhecida técnica "cavalo de Tróia" – técnica essa que permite que dispositivos infectados hajam de maneira orquestrada com o objetivo de sobrecarregar a infraestrutura alvo -, mesmo sem terem a mínima noção de que seus equipamentos estão silenciosamente cometendo delitos no ambiente cibernético (LEMONNIER, 2015).

Por sua vez, Oram e Viega (2009) acrescentam que, antes tais ataques possuíam uma característica individualizada, ou seja, eram realizados por indivíduos buscando algum tipo de benefício próprio. Hoje em dia, percebe-se um comportamento em comunidades e para alvos pré-determinados. O alvo dos referidos ataques podem ser governos, empresas ou companhias, indivíduos, e a própria sociedade como um todo. O alcance do dano e as consequências deixadas pelo rastro são fatores definidores para categorizar o mal causado. Em prol de um melhor entendimento, Hundley e Anderson (1995) sugerem a seguinte categorização dos males oriundos das atividades maliciosas no ambiente virtual, as quais são apresentadas no quadro 2.

Quadro 2. Aspectos definidores do dano causado em espaço virtual.

Categoria do dano	**Descrição**
Pequeno aborrecimento ou inconveniência	Ciberativismo, clone de páginas, propagação de informações falsas, roubo de informações pouco relevantes.
Dano limitado	Obtenção de usuários e senhas em serviços online.
Perda importante e ou generalizada	Indisponibilidade de determinado serviço em rede devido aos ataques sofridos. A maioria das vezes se exige grande esforço de recuperação da informação e da infraestrutura.
Grande desastre	Perda completa do domínio das informações e indisponibilidade da infraestrutura empregada. Na maioria dos casos sequer a recuperação é possível. Quase sempre acompanhada de grande perda material e tecnológica.

Fonte: Elaborado pelo autor com base em Hundley e Anderson (1995).

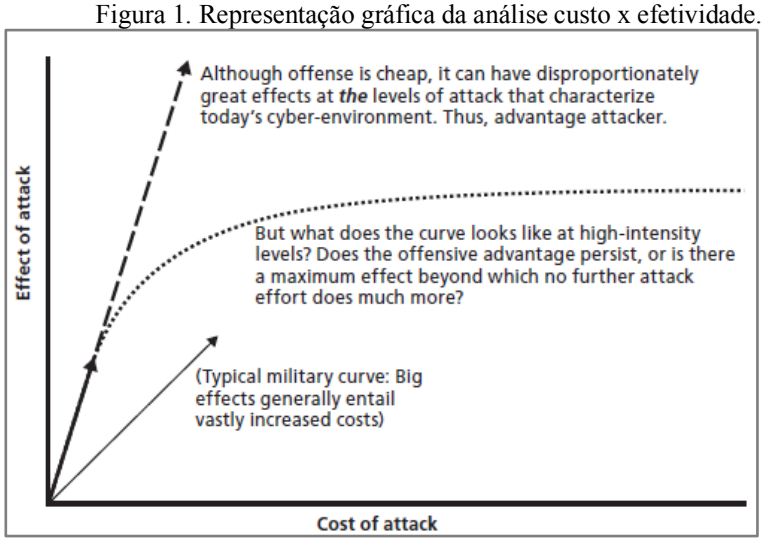
Mas com tantos meios dissuasórios e ou ofensivos já disponíveis para os líderes militares, por que afinal se investir tantos recursos financeiros em pesquisas de novas tecnologias de defesa e ataque no universo cibernético? Talvez uma análise gráfica possa refletir um pouco melhor essa quase "inescrupulosa" análise custo x efetividade que certamente vem sendo aplicada na arena belicosa internacional atualmente.

> The attraction of cyberdeterrence is that, if it works, it can reduce the cost of defending systems. Instead of having to put money into making systems more secure, the defender inhibits the attacker's efforts by threatening retaliation against successful attacks […]. If the attacker can be persuaded to reduce its efforts in the face of punishment, the defender can save some of what it would have spent on defense and still achieve the same level of security (LIBICKI, 2009, p.34).

Como pode se observar na figura 1, a relação entre gastos empregados *versus* o impacto negativo causado no inimigo, é bastante relevante para as novas tecnologias empregadas na

arena de conflitos cibernéticos, frente aos meios físicos empregados por métodos tradicionais de combate.

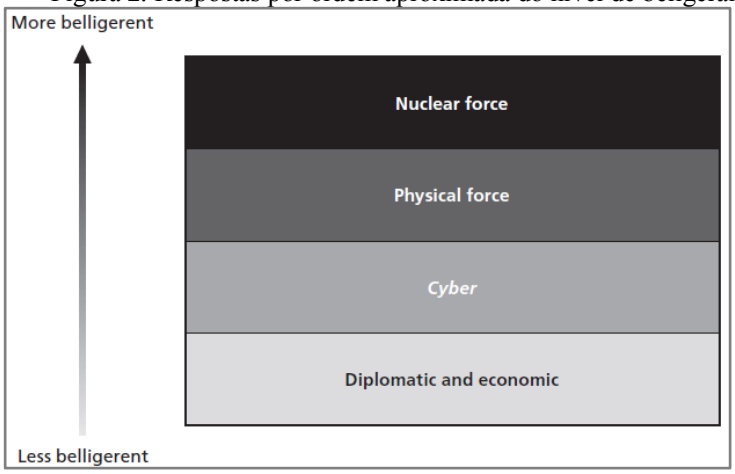
Figura 1. Representação gráfica da análise custo x efetividade.



Fonte: Adaptado de Libicki (2009).

Ainda na linha de comparação entre meios ofensivos empregados no teatro de guerra da atualidade, pode-se observar o impacto relativo das tecnologias hoje disponíveis para a grande maioria das potências mundiais trazidos novamente de maneira pictórica na figura 2.

Figura 2. Respostas por ordem aproximada do nível de beligerância.



Fonte: Adaptado de Libicki (2009).

Cibersegurança é um termo tão abrangente quanto os problemas com os quais ele visa orientar e/ou criar uma discussão em torno da problemática ocasionada pela conectividade, onde esta conectividade tornou-se própria dos meios produtivos, tecnológicos e de comunicação do século XXI, e como bem pondera Kissinger (2015), "[...] a ciência e a tecnologia são os conceitos que servem de guia para a nossa era. Ao longo da história, elas proporcionaram avanços sem precedentes para o bem-estar humano. Sua evolução transcende limitações culturais tradicionais.", mas como quase todo lado positivo possui um revés, o autor complementa, "No entanto, elas também produziram armas capazes de destruir a humanidade".

> A tecnologia criou um meio de comunicação que permite contato instantâneo entre indivíduos ou instituições em qualquer lugar do planeta, assim como o armazenamento e a recuperação de enormes quantidades de informação ao toque de

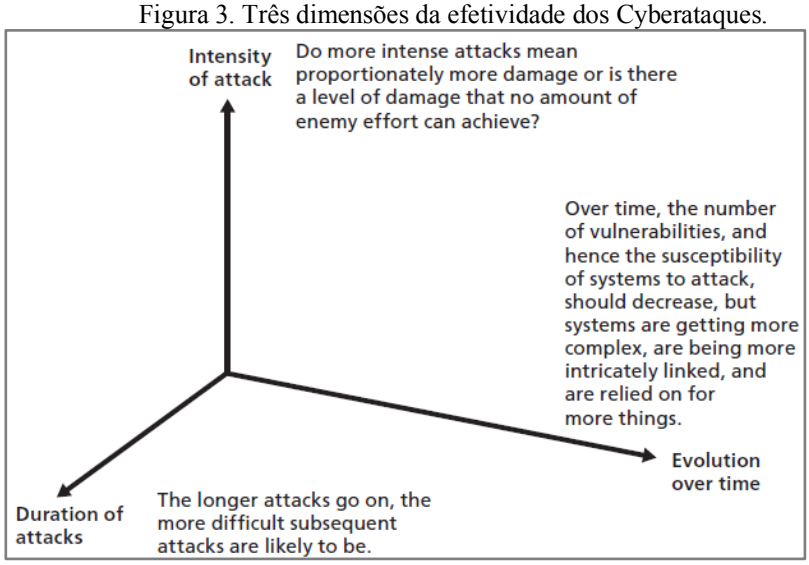
> um botão. E, no entanto, essa tecnologia está imbuída de que propósitos? O que acontecerá à ordem internacional se a tecnologia se integrou de tal maneira à vida quotidiana a ponto de definir o seu próprio universo como sendo o único relevante? A capacidade de destruição da tecnologia associada às armas modernas é tão imensa que um medo comum pode unir a humanidade para eliminar o flagelo da guerra? Ou a posse dessas armas acabará por criar um mau presságio permanente? A rapidez e o alcance da comunicação farão cair as barreiras entre sociedades e indivíduos e proporcionarão uma transparência de tal magnitude que os sonhos seculares a respeito de uma comunidade humana se tornarão realidade? (KISSINGER, 2015, p.286)

Basicamente, toda a gama de facilidades, evolução dos meios de troca, velocidade de difusão do conhecimento e da informação, se contrapõe a um ambiente virtual que pode ser hostil, vulnerável e, sobretudo, inseguro. E justamente no aspecto da segurança da população de um Estado que se firmou o conceito já abordado da balança de poder (ROCHA, 2002), a qual parece agora também ter que se adaptar aos novos tempos que a almejada modernidade traz consigo.

> A balança de poder tradicional enfatizava a capacidade militar e industrial. Uma mudança na distribuição de poder só poderia ser alcançada de forma gradual ou por conquista. A balança de poder moderna reflete o nível do desenvolvimento científico de uma sociedade e pode ser ameaçada de forma drástica por desdobramentos inteiramente no interior do território de um Estado. (KISSINGER, 2015, p.142)

O conceito de ciberdefesa se emprega a todo o conjunto de ferramental, técnicas e recursos físicos / lógicos para se fazer frente aos desafios provenientes de ciberataques. Como já fora dito anteriormente, o poder de intrusão e destruição de um ciberataque pode ser tão arrasador quanto a um ataque físico (ao se mensurar estritamente o aspecto financeiro do dano, resguardando por óbvio, a perda de vidas humanas envolvidas) e ou gerá-lo, em última instância. Um ataque cibernético possui três dimensões quanto a sua efetividade, são estas (LIBICKI, 2009, p.85): a) Intensidade; b) Evolução no tempo; c) Duração do ataque.

Figura 3. Três dimensões da efetividade dos Ciberataques.



Fonte: Adaptado de Libicki (2009).

Alinhado ao modo tradicional de enfrentamentos entre Nações (conflitos físicos), uma definição pura e simples do ato de guerra, segundo Clausewitz seria "Each tries through physical force to compel the other to do his will" (CLAUSEWITZ; HEUSER, 2007, p.27), ou

seja, tem por objetivo necessariamente criar uma condição de subjugação, onde um lado, o vencido, é obrigado a fazer a vontade do vencedor.

Libicki (2009) traz uma definição esclarecedora sobre o conceito da guerra cibernética, colocando os ataques cibernéticos para fins privados, como atividades criminosas que usam de estratégias de uma guerra cibernética, não a sendo de fato, uma vez que esta se caracteriza apenas tendo Nações umas contra as outras. Salienta ainda, que como numa guerra convencional, tal estratégia só deva surgir quando os esforços de retaliação político, diplomático e econômico falharem e/ou não puderem ser usados por se julgarem inócuos.

Fato é que, seria praticamente impossível relatar todos os episódios já ocorridos no tocante da Cibersegurança no cenário internacional, mesmo porque não se sabe ao certo se este é um termo novo para tratar um evento antigo, ou um termo antigo (e repaginado) para tratar de um assunto relativamente novo. Devido a isso, talvez seja eficaz recorrer à história para tentar se entender como o cenário atual se desenhou.

Para fins históricos, remonta-se à década de 80, ao período que precedeu o fim da Guerra Fria o termo "Guerra nas Estrelas", o qual fora influenciado por um projeto de segurança militar do governo da ex-União Soviética (URSS). O referido projeto visava o lançamento no espaço de uma nave espacial equipada com um canhão a laser que seria capaz de destruir "teoricamente" qualquer míssil vindo dos EUA para o seu território (NATIONAL INTEREST, 2016).

O projeto batizado por *Polyus* foi uma inovadora iniciativa tecnológica na área de defesa. Este experimento visava à destruição de satélites americanos em órbita, bem como a formação de uma plataforma de defesa orbital do governo da antiga União Soviética. A curiosa ideia saiu do papel e chegou a ser confeccionada em termos de protótipo, porém, não se sabe ao certo de sua eficácia, haja vista que o então presidente Mikhail Gorbachev[4] não autorizou o seu lançamento para fins de testes em órbita e em seguida o projeto foi descontinuado (NATIONAL INTEREST, 2016).

Ao analisar a incrível história do Projeto *Polyus*, é mesmo difícil prever se o temido canhão teria sido mesmo capaz de cumprir a façanha prometida, mas o certo é que o aparato figurou na imaginação e ideário de toda uma geração.

Apesar de tema não consensual, há especialistas cada vez mais convencidos desta possibilidade de conflito na arena do ciberespaço. O governo norte americano, por exemplo, é um forte investidor nesse ramo de atuação da defesa nacional. Sua divisão de combate a crimes cibernéticos, a *U.S. Army Cyber Command*, conta com um contingente de 19.000 homens atuantes (entre militares e civis) em escala permanente de trabalho – vinte e quatro horas por dia, setes dias por semana -, atuando em atividades de pesquisa, exercícios de simulação e monitoramento das questões de Cibersegurança (U.S. ARMY CYBER COMMAND, 2017). Cabe a ressalva, que Rússia e China também possuem um centro com características e objetivos semelhantes (CLARKE; KNAKE, 2010).

> A nation that has invented the new technology, and the tactics to use it, may not be the victor, if its own military is mired in the ways of the past, overcome by inertia, overconfident in the weapons they have grown to love and consider supreme. The originator of the new offensive weaponry may be the loser unless it has also figured out how to defend against the weapon it has shown to the rest of the world. (CLARKE; KNAKE, 2010, p.6).

[4] É um político russo. Foi o último líder da União Soviética e governou durante os anos de 1985 a 1991.

Gallagher (2017) salienta a preocupação de lideranças mundiais em torno da possibilidade de ocorrer uma Segunda Guerra da Web, fazendo referência aos incidentes ocorridos em 2007 na Estônia, o qual ficou conhecido como a Primeira Guerra da Web. Como evidência dessa preocupação crescente, o autor relata ainda os constantes exercícios de simulação de ataques e defesas em atividades cibernéticas realizadas pelo *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE).

O referido centro de defesa (CCDCOE) é situado na Estônia (não por acaso) e conta com uma estrutura de técnicos, analistas e pesquisadores de diversas nacionalidades e áreas de conhecimento em seu quadro permanente. Propositadamente, criou-se uma estrutura que une esforços em pesquisa, conhecimento militar e industrial. Com isso, garantiu-se a construção de uma visão holística sobre a Cibersegurança, sobretudo, no segmento da segurança nacional (CCDCOE, 2017).

Portanto, a OTAN[5] parece mesmo levar o tema da *Cyberwar* a sério (GALLAGHER, 2017), uma vez que com a iniciativa do CCDCOE organiza anualmente o maior e mais complexo exercício técnico de defesa cibernética mundial, cujo tem por objetivo o aprendizado de como evitar estes ataques em redes comerciais e militares. Ademais, também por meio do CCDCOE, a OTAN patrocina e organiza a conferência anual de conflitos cibernéticos (*CyCon – Cyber Security Conference*) que no ano de 2018 chegou à sua décima edição.

Em contraponto a ideia de uma "preparação" para algo que irá ocorrer no futuro (incerto, próximo), há o especialista e mundialmente conhecido no âmbito das questões de segurança cibernética, o russo Eugene Kaspersky. Ele não apenas acredita na urgência e relevância do tema, como também defende que a era das guerras cibernéticas já começou (KASPERSKY, 2012). Este especialista que já teve sua equipe contratada em 2012 pela União Internacional de Telecomunicações (UIT)[6], para analisar um vírus o qual se credita a construção ao governo israelense, é categórico em afirmar que os governos e lideranças mundiais já estão há muito tempo travando batalhas no ciberespaço.

Ainda segundo Kaspersky (2012), os governos não atuam apenas na prevenção, mas também no ataque preventivo e coordenado contra alvos específicos previamente determinados e estudados. Onde nesse caso, agiriam em prol da soberania nacional (ataque como estratégia de defesa) e não por vandalismo ou pretensões de obter vantagens financeiras, obviamente.

CASOS EMBLEMÁTICOS DA AGENDA DA CYBERWAR E SUAS IMPLICAÇÕES

Conforme citado na seção introdutória, os casos escolhidos para estudo obedeceram aos critérios de relevância no cenário mundial, intensidade das ações e danos gerados pelos atos, relacionados ao tema da *Cyberwar*, sendo estes: Estônia (2007), Geórgia (2008) e Irã (2010).

Cada caso possuiu objetivos próprios (quase integralmente desconhecidos) por parte de seus executores, e deixaram consequências por vezes imensuráveis em termos dos danos financeiros, de imagem e sustentabilidade dos serviços básicos de tecnologia nos países alvos dos ataques. Acredita-se ainda, que a maior parte dos ataques tenham sido orquestrados e/ou patrocinados por lideranças políticas a fim de:

[5] A OTAN (Organização do Tratado Atlântico Norte) é uma aliança militar intergovernamental fundada em 1949, oriunda do Tratado do Atlântico Norte.

[6] União Internacional de Telecomunicações (UIT) é a Agência do Sistema das Nações Unidas (ONU) dedicada a temas relacionados às Tecnologias da Informação e Comunicação (TICs).

i. Bloquear atividades de desenvolvimento e pesquisa dos países alvo dos ataques;
ii. Desmoralizar seus líderes políticos, bem como influenciar decisões e os rumos de política e pleitos eleitorais;
iii. Apontar fragilidades e ou desviar atenção de fatos ocorridos no cenário político.

A seguir, as próximas subseções trarão respectivamente cada caso em detalhes.

OS ATAQUES CIBERNÉTICOS DE 2007 PARALISARAM A ESTÔNIA

Mais de uma década já se passou desde o ocorrido e este caso ainda reverbera nas análises fundamentais de crimes cibernéticos dentro dos círculos de especialistas e estudiosos do tema, sobretudo, no campo da estratégia de defesa militar. Devido à dimensão e a gravidade, o referido episódio ficou conhecido como a Primeira Guerra da Web.

O emblemático caso do ciberataque à Estônia se deu em meados de abril de 2007, uma iniciativa que foi ímpar no cenário de crimes cibernéticos e jamais vista até então. Na ocasião histórica, o país teve quase a sua totalidade de serviços tecnológicos postos em indisponibilidade, foram estes: serviços bancários online, serviços de telecomunicações, radiodifusão e mesmo portais do governo (O'NEILL, 2016).

A técnica principal utilizada pelos ataques foi a DDoS (sigla em inglês para "distribuição de negação de serviço"), a qual consiste em fazer requisições dos servidores provedores de serviço, bem acima de suas respectivas capacidades de resposta, onde tais requisições são realizadas a partir de máquinas infectadas ao redor do mundo, ou seja, usuários conectados à internet e em situação de vulnerabilidade se tornam hospedeiros de algum tipo de *software* malicioso (REGAN, 2018). Este *software* uma vez instalado em algum dispositivo possui um fim determinado, o de atuar como peça do xadrez no jogo de ataques na esfera cibernética mundial.

> As for why people perform DoS attacks, that's a bit tricker. The most common, but far from the only, reason is cyber-activism, a way to protest a website or organization that the attackers disagree with in some profound way and want to either shut up or intimidate. But they can also be pranks, a ransom threat, an attempt at extortion, or a distraction for a more serious, damaging hack going on in the background. And sometimes, they're merely used to test how capable a server is. (REGAN, 2018)

Mas qual teria sido afinal a causa que deu origem aos transtornos? Acredita-se que o início dos ataques se deu devido à decisão do ex-presidente do país, Thomas Hendrik IIves[7], em transferir uma antiga estátua em homenagem a um soldado da Era Soviética do centro da cidade de Tallinn[8] para um cemitério nos arredores da cidade, fato que desagradou muitos cidadãos do país, onde um terço da população possui ascendência russa (SCHULTZ, 2017).

A sequência de eventos quase imprevisíveis poderia figurar qualquer editorial de ficção cientifica no mundo, afinal, quem poderia acreditar em um ataque virtual em massa contra um país, motivado por questões ideológicas e com um forte viés político por trás dos fatos ocorridos? Ou ainda, como em 2007 com os recursos computacionais da época, poderia se pensar em tais níveis de vulnerabilidades dos serviços tecnológicos mais básicos hoje em dia?

[7] Toomas Hendrik Ilves é um político da Estônia. Foi presidente do seu país entre os anos de 2006 a 2016. Era o presidente do país no período dos ataques cibernéticos que bloquearam os serviços tecnológicos do país.
[8] Tallinn é a capital da Estônia, localizada no golfo da Finlândia, na costa norte do país junto ao mar Báltico.

Apesar de não confirmado, credita-se ao governo russo a época pelos ataques realizados contra o país e que duraram mais de duas semanas. Ademais, se atribuem causas politicas para os beligerantes ataques. Em recente pronunciamento (SCHULTZ, 2017), IIves critica a postura da OTAN em tratar o caso e acusa a Comissão Europeia de inércia de ações para dirimir futuras e iminentes questões de segurança, sobretudo, naquelas que envolvem a segurança cibernética. O ex-líder cita ainda que: a) Líderes políticos não conhecem de tecnologia e desconhecem os perigos envolvidos; b) O conselho de segurança da UE não lida bem com a questão de ameaças cibernéticas; c) Os crimes possuem viés politico e são usados para manipular eleições e resultados importantes em pleitos ao redor do mundo.

Conforme salienta O'Neill (2016), os ataques cibernéticos sofridos pela Estônia podem não terem sido marcantes e mundialmente conhecidos como o fatídico 11 de Setembro sofrido pelos Estados Unidos ou tão chocante tal qual a invasão ao Iraque em 2003, ou ainda, terem sido midiatizados com tais. Porém, resguardando as proporções - pois nos dois primeiros existe o custo intangível da vida humana -, os ataques cibernéticos mudaram a história mundial tais quais os eventos anteriormente citados. Para tanto, resgatou-se a antiga ferida de uma URSS combalida e findada, colocando em fronte de combate dois velhos (e "irmãos") países, Estônia e Rússia. Importante também salientar que a Estônia como ex-integrante do bloco da União Soviética, obteve sua independência em 1991 com o colapso do bloco soviético, onde desde então sua relação com o agora vizinho nunca foi tranquila.

Como saldo positivo após o aniversário de dez anos dos fatos ocorridos neste marcante episódio, entende-se que a sociedade ganhou:

i. Criação e fortalecimento do Centro de Excelência de Defesa Cibernética Cooperativa (sigla em inglês CCDOE);
ii. Criação da conferência mundial sobre o tema da Cibersegurança (da sigla em inglês *CyCon*);
iii. Aumento da conscientização e difusão do tema no cenário internacional;
iv. Criação do Manual Tallinn de Direito Internacional Aplicado para Operações Cibernéticas (ANSLEY, 2017).

O rico manual está subdivido em quatro partes, sendo estas (SCHMITT, 2017):

a. *General international law and cyberspace*;
b. *Specialized regimes of international law and cyberspace*;
c. *International peace and security and cyber activities*;
d. *The law of cyber armed conflict*.

Ou seja, o Manual Tallinn de Direito Internacional Aplicado para Operações Cibernéticas para ser o conjunto das regras do jogo que faltava no já longínquo ano de 2007.

A GUERRA RUSSO-GEORGIANA EM 2008 NO ÂMBITO CIBERNÉTICO

Ossétia do Sul, uma região da República da Geórgia que hoje é um território separatista apoiado e ocupado militarmente pela Rússia. O país de pequena extensão territorial que possui longa fronteira ao norte com a Rússia, foi palco de um dos mais duros episódios no cenário da ciberguerra da atualidade. Motivo? A autonomia / independência da região citada inicialmente.

Cabe a ressalva, que a história dos conflitos na região é antiga e não será objetivo de explanação desse artigo, o qual irá deter-se apenas no estrito fato dos ciberataques realizados.

Devido a causas políticas, as ofensivas no campo dos ataques cibernéticos foram resultados de ofensivas tradicionais (terrestre, física) realizados por líderes separatistas e com apoio político-militar da Rússia com a intenção de tornar a região da Ossétia do Sul independente do governo da Geórgia, a qual tentou se defender e teve como seu aliado, ninguém menos que os EUA (PERES, 2010). Segundo a atual presidente da Geórgia, os conflitos na região remontam da opção feita por maioria da população em tornar-se membro da Europa, "É algo profundamente enraizado na mentalidade georgiana: os georgianos sentem que são europeus - não é algo que ambicionem. Eles são europeus" (ZURABISHVILI, 2019), onde na visão da presidente, a Rússia os acusa de buscarem uma "ocidentalização" da cultura, algo inaceitável para um ex-membro da antiga União Soviética, por assim dizer.

Porém, a presidente diz que a trajetória é um caminho sem volta e que tais conflitos podem ainda ter desdobramentos mais prolongados, "[...] vamos continuar esse caminho para alcançarmos progressos muito claros em direção à Europa e para fazermos parte da Europa" (ZURABISHVILI, 2019), ou seja, o capítulo da guerra Russo-Georgiana ainda não concluiu.

Tal descrição da mandatária somente reforça a tese de que os ataques / conflitos cibernéticos atualmente, são cada vez menos obra de grupos isolados sem motivos evidentes para tal, tornando-se cada vez mais um desdobramento de atos políticos que os embasam (ORAM; VIEGA, 2009).

Do ponto de vista técnico, mais uma vez, a técnica utilizada foi o DDoS, como visto anteriormente, porém, no caso da Geórgia não foi possível prever os ofensores de forma precisa, pois os ataques foram feitos de forma "pulverizada". Segundo Tikk et al. (2008) do centro de defesa CCDCOE, "the case with Estonia, there is no conclusive proof of who is behind the DDoS attacks, even though finger pointing at Russia is prevalent by the media. There seems to be a widespread consensus that the attacks appeared coordinated and instructed".

De forma estratégica, os grupos por trás dos ataques organizaram sites contendo manuais e *softwares* maliciosos de fácil utilização e ainda uma lista de sites preferenciais dos ataques. Tais *softwares* não exigiam qualquer conhecimento por parte do usuário, ou seja, qualquer um por mais leigo que fosse e que concordasse com a causa separatista poderia se tornar um "*hacker*" momentaneamente e participar do grande movimento que estava se desenhando. Esse fato só evidencia ainda mais que as inciativas foram de certa forma coordenadas, conforme salienta ainda Tikk et al. (2008) "the conclusions leave little doubt that the Georgian cyber attacks were largely coordinated, not simply an ad hoc reaction of individual cyber-activists sympathetic to the Russian cause[…]", trazendo, portanto, certo nível de sofisticação ao que se percebeu no episódio sofrido pela Estônia.

Ainda mais agravante no caso desses ataques, foi que uma vez os principais portais governamentais indisponíveis, o país ficou completamente "fora do ar" nacional e internacionalmente, gerando grave crise de desinformação na população georgiana e também na comunidade internacional. Diferentemente do caso da Estônia, relatado anteriormente, agora os alvos não foram apenas empresas privadas, e sim tendo o foco principal o governo da Geórgia, gerando grande sensação de passividade e a não formação de opinião por parte da população, "[...] in Georgia, the heart of the damage lied in limiting the nation's options to distribute their point of view about the ongoing military conflict– in "making its voice heard" to the world.", Tikk et al. (2008).

> The unavailability of crucial websites of the Georgian government caused by the DoS and DDoS attacks severed communication from the Georgian government in the early days of the Georgian-Russian conflict – a period that was doubtless the most critical

> in the events and where the Georgian government had a vital interest in keeping the information flowing to both the international public and to its own residents. The unavailability of the core state institutions' websites can additionally be seen as serving a discouraging effect on Georgian nationals. (TIKK et al., 2008, p.16)

Os ataques tiveram duração curta, sendo o mais longo durando aproximadamente seis horas, de acordo com o relatório *Cyber Attacks Against Georgia: Legal Lessons Identified* produzido pelo CCDCOE (TIKK et al., 2008, p.10) , mas com ampla intensidade e com efeitos duradouros dos resultados das ações, ficando a lição de como a força e o potencial desta "nova arma" pode ser um grande aliado às forças militares tradicionais, bem como da necessidade de investimento massivos em pesquisa, desenvolvimento e construção de todo um sistema de defesa por partes dos Estados.

OS ATAQUES CIBERNÉTICOS AO IRÃ EM 2010 E O PROJETO STUXNET

O Projeto *Stuxnet* – como ficou conhecido -, o qual não se tem a precisão da data de início, mas acredita-se que tenha começado em meados do segundo semestre de 2009 e início 2010 (o ponto forte das ações), é apontado como tendo sido capitaneado pelo governo americano em parceria com Israel para dissuadir a capacidade iraniana no processo de enriquecimento de urânio, em sua corrida pelo desenvolvimento e amadurecimento da sua tecnologia nuclear (NAKASHIMA, 2012). O alvo foi a usina nuclear situada em Natanz, no Irã, onde a usina controlava as centrífugas de enriquecimento de urânio.

É importante salientar que o esquema de sabotagem aos planos iranianos iniciara antes do levante tecnológico promovido pelo *Stuxnet*, desta vez já por meio da utilização de sanções e embargos ao comércio iraniano, onde componentes eletrônicos essenciais ao desenvolvimento de seu projeto nuclear, foram incluídos na pauta do bloqueio, impedindo que o Irã os adquirisse de maneira legal. Tal medida foi liderada e divulgada na ocasião pela então Secretária de Estado Americano (2009 - 2013) durante o governo de Barack Obama (2009 - 2017), Hillary Clinton (BROAD et al., 2011). Vale ressaltar que o místico plano teve início (uma fase de estudos e investigações) ainda durante a administração de George W. Bush e fora em seguida repassado ao então presidente eleito no pleito americano de 2008, Sr. Obama.

Hoje já se sabe que o alvo do vírus foi um equipamento específico utilizado na infraestrutura da usina iraniana. Afasta-se, portanto, a ideia de uma eventualidade e traz à tona a necessidade massiva de investimentos em tecnologia da informação com foco em segurança. Acredita-se que a ação conseguiu destruir 1.000 das 9.000 centrífugas para enriquecimento de urânio do projeto iraniano, causando grande dano e atraso em seus objetivos (KREMER; MÜLLER, 2014). Ainda segundo os autores, "Stuxnet introduced a comprehensive cyber offensive package in the cyber warfare with an ability of attacking the target with high precision".

Segundo Broad et al. (2011), especialistas em segurança internacional apontam que Israel possua infraestrutura física de testes com equipamentos no complexo tecnológico de Dimona, idênticas aos utilizados pelo projeto iraniano, a saber, as centrífugas de enriquecimento que utilizam o micro controlador P.C.S.-7 do fabricante alemão de tecnologia Siemens, que teve suas fragilidades exploradas por meio do vírus desenvolvido. O complexo Dimona de Negev em Israel é conhecido por abrigar a inteligência do núcleo de estudos e desenvolvimento tecnológico em energia nuclear deste país, onde o mesmo foi apontado por ter sido o palco dos testes do projeto *Stuxnet*.

A técnica utilizada no projeto foi a construção de um poderoso *software* (ou super vírus) que possuía a capacidade de rápida propagação e infecção nos computadores aos quais teriam acesso. O *software* tinha a capacidade de mapear os *hardwares* conectados na rede o qual havia se alastrado e passava informações a outro programa externo, o qual captava e processava essas informações, as quais serviam para o planejamento das próximas ações (NAKASHIMA et al., 2012). A ideia foi realmente inovadora e ainda inédita no cenário da cibersegurança, "the emerging details about Flame provide new clues to what is thought to be the first sustained campaign of cyber-sabotage against an adversary of the United States".

> This threat could come in the form of targeting systems which are dependent on software for their operation; […] The Stuxnet virus is another example, its focus on disabling safety systems to damage equipment being used in the Iranian nuclear program. Threats to information or the ability to manipulate information could be catastrophic as the world becomes more information reliant. (KREMER; MÜLLER, 2014, p.46)

Acredita-se que uma vez propagado o vírus na cidade de Natanz, o vírus primeiramente infectou o computador pessoal de um dos técnicos da usina (essa informação nunca pôde ser confirmada por especialistas se foi um processo aleatório ou intencional), o qual portando seu *pendrive* de uso pessoal e utilizando o mesmo equipamento nas instalações e equipamentos da usina, iniciou o processo de alastramento do *software* malicioso (NAKASHIMA et al., 2012).

O *software* (ou o vírus), basicamente possuía duas missões claras em seus componentes - além de sua notória capacidade de rápida propagação -, uma seria a responsável por fazer um movimento de rotação atípico nas centrifugas de enriquecimento de urânio, ou seja, levava que o equipamento funcionasse acima de sua capacidade de controle, fato que o levaria ao dano logo após vários ciclos em funcionamento incorreto. O outro componente era capaz de gravar o funcionamento anterior da centrífuga e em seguida transmitir dados de normalidade aos sensores dos sistemas de controle, burlando sistemas de verificação da usina (BROAD et al., 2011). Ainda segundo os autores, talvez o projeto *Stuxnet* tenha contado com o apoio do governo da Inglaterra e da Alemanha, com cooperação ainda da empresa Siemens, porém, tais suspeitas não foram confirmadas por nenhuma das partes.

De toda forma, o Irã também acusa os EUA e Israel de assassinarem ao menos quatro de seus principais cientistas responsáveis por seu programa nuclear, como forma similar de tentar dissuadi-los em seus objetivos e ou promover atrasos efetivos (THE GUARDIAN, 2012). Fatos, claro, jamais confirmados por parte dos países acusados.

É sabido que os conflitos na região ultrapassam tais questões técnicas que envolvam meramente as pretensões iranianas em seu projeto de desenvolvimento nuclear, porém, tais anseios iranianos contribuem de sobremaneira ao clima belicoso e de tensões diplomáticas envolvendo alguns países do oriente médio com seus vizinhos próximos. Tal situação não parece ter solução fácil, e conforme salienta Kissinger, "[...] pode estar prestes a acontecer uma mudança potencialmente fundamental na balança militar [...] da região. Essa mudança foi propiciada pelo rápido progresso do Irã rumo ao status de um Estado detentor de armas nucleares [...]".

> A questão da paz no Oriente Médio nos últimos anos permaneceu focada no tema altamente técnico das armas nucleares no Irã. Não existe nenhum atalho que contorne o imperativo que consiste em evitar o seu aparecimento (sic). No entanto, convém relembrar períodos em que outras crises aparentemente insolúveis no Oriente Médio adquiriram uma nova dimensão, graças à firmeza moral e a uma visão. (KISSINGER, 2015, p.150)

Nesta visão, os países estariam sob uma estrutura de anarquia internacional, buscando e tentando reafirmar o seu status de potência e soberania. É preciso salientar que cada um dos países envolvidos possui quase total incerteza das capacidades de seus pares e por fim, procuram agir de forma racional visando sua sobrevivência, manutenção da ordem no cenário internacional e fortalecimento de sua própria soberania. Neste jogo, porém, tudo seria justificado? Enfim, as capacidades dissuasórias no âmbito tecnológico seriam mais justificáveis e moralmente aceitas frente aos tradicionais meios físicos?

Por óbvio, o Irã não demonstra ter superado o episódio e nem mesmo ter se abalado quanto aos seus planos de evolução de seu programa nuclear. A paz na região está longe de ser alcançada, uma vez que cada Nação acredita e tem direito a exercer suas convicções com autonomia e em benefício de seu povo, afinal.

Kissinger (2015), em sua larga experiência diplomática aponta que "os Estados Unidos e as democracias ocidentais deveriam estar abertos ao cultivo de relações de cooperação com o Irã", mesmo sabendo que este país possui sérias restrições às parcerias ocidentais. Seguindo em sua análise e incursão à problemática na relação de cooperação, ainda pontua "o que não devem fazer (EUA) é basear essa política na projeção de sua própria experiência interna, como sendo algo inevitável ou automaticamente relevante para aquela de outras sociedades, em especial a do Irã", uma vez que este talvez este seja o país que tenha o mais coerente sentido de nacionalidade e a mais elaborada tradição de estadismo com base nos interesses nacionais.

CONSIDERAÇÕES FINAIS

É salutar a evidência teórica em qualquer tema que envolva Relações Internacionais, seja por questões definidoras e ou de entendimento, seja devido à necessidade de clareamento de novas áreas que surjam com a modernidade dos hábitos e das civilizações, como os conceitos explorados de Cibersegurança, Ciberespaço ou Ciberguerra que foram expostos nesta análise.

Mesmo que o indivíduo hoje busque a total privacidade de suas identidades digitais, sabe-se que é praticamente impossível controlar / saber o local onde os seus dados estão sendo armazenados ou criados. E tal situação, pode por vezes gerar uma sensação de insegurança pessoal. Por óbvio, que cada usuário das facilidades da conectividade está sujeito às chateações ou perdas, isso ao se analisar um universo por assim dizer, em nível micro do problema. Agora ao se pensar em nível macro, parte-se para preocupações bem maiores, pois os dados e sistemas eletrônicos de uma Nação configuram também sua riqueza, sua fonte de serviços básicos, essenciais à sua população e toda sorte de controles das diversas e milhares de transações ocorridas em um só dia produtivo da economia.

Ao se colocar o termo "Ciberguerra", talvez o leitor seja sempre levado a pensar apenas no sentido bélico, mas essa não é a verdade plena. Imagine no caso brasileiro, um ataque generalizado aos sistemas da Bolsa de Valores Monetários, ou aos sistemas do Banco Central, ou aos sistemas do Instituto Nacional do Seguro Social, ou a toda malha de Telecom do país, ou ainda, aos sistemas controladores do tráfego aéreo brasileiro. Ou seja, caos, não haveria outra palavra! Pois bem, foi nesses termos que os cidadãos da Estônia se viram no episódio relatado em seção anterior.

De certo modo, um ataque físico a uma estrutura que cause sua total inutilidade pode ser comparado a um ataque lógico em mesmas proporções? E o que pensar do caso iraniano – conforme fora abordado -, onde um ataque lógico ocasionou um dano físico de grandes dimensões ao projeto e às instalações de seu programa nuclear? Tal caso estaria posto no mesmo

contexto do direito internacional? “Ora, afinal o dano à população foi causado”, pensariam alguns analistas e pesquisadores. “Mas as fronteiras físicas não foram ultrapassadas, e desse modo a soberania não foi então ameaçada”, poderiam ser levados a crer outros. Bem, é possível perceber que muitos mecanismos de controle no âmbito internacional (leis, regulamentações) e claro, novas teorias, precisam surgir e/ou evoluir para se fazer frente aos desafios correntes e vindouros no que tangem as questões de segurança internacional, territorialidade e crimes cibernéticos, apenas para ficar no contexto do referido artigo. E talvez, tal necessidade se acentue na mesma velocidade em que os aspectos tecnológicos o façam.

Como já se é sabido, dois dos papéis do Estado são: preservar sua soberania e a segurança da sua população. E em época atual ou Nova Era, conforme coloca Henry Kissinger, os desafios são acompanhar as evoluções cotidianas, pensar nos avanços necessários tanto tecnológicos quanto legais e prover novas formas de segurança sejam estas físicas ou digitais aos seus cidadãos. Necessidades tais que se configuram de primeira urgência para se fazer frente às novas ameaças que possam vir a surgir.

Ao estudante, pesquisador ou profissional de RI, fica a missão clara de evidenciar fatos sob a luz da teoria e o dever incessante da busca sistemática por verdades, explicações e construções de conhecimento que auxiliem o mundo a construir a paz e a boa convivência entre os povos e as Nações. Sendo assim, por acreditar nesses termos e na capacidade intelectual dos povos e de cada cidadão em cada Estado Nação em propor novas soluções pacíficas às controvérsias próprias de qualquer organização de sociedade, que esse autor se debruçou sobre esse delicado tema a fim de dar sua contribuição e propor um entendimento, visando sempre que possível, suscitar novos debates.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, I, O. et al. SISTEMA INTEGRADO DE MONITORAMENTO DE FRONTEIRAS EM PERSPECTIVA. Rio de Janeiro: Ipea, 2019. (Texto para Discussão, n. 2480).

ANSLEY, R. Tallinn Manual 2.0: Defending Cyberspace. Fevereiro de 2017. Disponível em: <http://www.atlanticcouncil.org/blogs/new-atlanticist/tallinn-manual-2-0-defending-cyberspace>. Acesso em: 10/12/2019.

BBC BRASIL. Entenda o conflito envolvendo Rússia e Geórgia na Ossétia do Sul. Agosto de 2008. Disponível em: <https://www.bbc.com/portuguese/reporterbbc/story/2008/08/080808_entenda_ossetia_cg.shtml>. Acesso em: 15/12/2019.

BROAD, W. J.; MARKOFF, J.; SANGER, D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. Janeiro de 2011. Disponível em: <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>. Acesso em: 10/12/2019.

CASTELLS, M. Redes de Indignação e Esperança: Movimentos Sociais na Era da Internet. 2. ed. Rio de Janeiro: ZAHAR, 2017.

CASTELLS, M. Sociedade em Rede – Volume I. 2. ed. São Paulo: PAZ E TERRA, 1999.

CCDCOE. NATO Cooperative Cyber Defense Centre. About Cyber Defense Centre. Dezembro de 2017. Disponível em: <https://ccdcoe.org/about-us.html>. Acesso em: 10/12/2019.

CLARKE, R. A.; KNAKE, R. Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins Publishers, 2010.

CLAUSEWITZ, C; HEUSER, B. On War. USA: Oxford University Press. 2007.

DW. Iran opens new nuclear facility at Natanz. Junho de 2018. Disponível em: <https://www.dw.com/en/iran-opens-new-nuclear-facility-at-natanz/a-44105090>. Acesso em: 26/06/2019.

EUA. U.S. Relations With Brazil. Outubro de 2019. Disponível em: <https://www.state.gov/u-s-relations-with-brazil/>. Acesso em: 10/12/2019.

GALLAGHER, M. Especialistas temem guerra cibernética no futuro. BBC, London. Abril de 2012. Disponível em: <http://www.bbc.com/portuguese/noticias/2012/04/120430_cyberguerra_futuro_fn>. Acesso em: 10/12/2109.

HARDING, L. What we know about Russia's interference in the US election. Dezembro de 2016. Disponível em: <https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election>. Acesso em: 21/10/2019.

HUNDLEY, R. O.; ANDERSON, R. H. "Emerging Challenge: Security and Safety in Cyberspace," IEEE Technology and Society Magazine, pp. 19–28 (Winter 1995).

JACKSON, R.; SORENSEN, G. Introdução às Relações Internacionais. 2. ed. Rio de Janeiro: ZAHAR, 2013.

KASPERSKY, Eugene. A ciberguerra já começou. [Entrevista concedida a] Fernando Valeika de Barros, de Moscou. Veja, Moscou, 15 set. 2012.

KISSINGER, H. A. Ordem mundial. Rio de Janeiro: Objetiva, 2015.

KREMER, J. F.; MÜLLER, B (Org.). Cyberspace and International Relations - Theory, Prospects and Challenges. Berlin: Springer, 2014.

LEMONNIER, J. O que é o malware de cavalo de Troia? Junho de 2015. Disponível em: <https://www.avg.com/pt/signal/what-is-a-trojan>. Acesso em: 23/03/2020.

LIBICKI, M. C. Cyberdeterrence and cyberwar. Santa Monica: RAND Corporation, 2009.

MORAES, C. R. Estrutura de Dados e Algoritmos. São Paulo: Ed. Berkley. 2001.

NAKASHIMA, E; MILLER, G; TATE, J. U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. Junho de 2012. Disponível em: <https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say>. Acesso em: 10/12/2019.

NATIONAL INTEREST. The Rise and Fall of the Soviet 'Death Star'. Janeiro de 2016. Disponível em: <http://nationalinterest.org/feature/the-rise-fall-the-soviet-death-star-14854>. Acesso em: 10/07/2019.

NOGUEIRA, J.P.; MESSARI, N. Teoria das Relações Internacionais – Correntes e Debates. São Paulo: Elsevier, 2005.

O'NEILL, P. H. The cyberattack that changed the world. Maio de 2016. Disponível em: <https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia>. Acesso em: 10/07/2019.

ORAM, A.; VIEGA, J. Beautiful Security – Leading Security Experts Explain How They Think. Nova York: O'Reilly Media. 2009.

PERES, R. P. S. A GUERRA NO CIBERESPAÇO: PRINCÍPIOS DA GUERRA CLÁSSICA APLICADOS NA CIBERGUERRA. Dissertação de Mestrado em Ciência Militares, Lisboa: Academia Militar, 2010, 82 p.

REGAN, J. The Ultimate Guide to Denial of Service (DoS) Attacks. Julho de 2018. Disponível em: <https://www.avg.com/en/signal/what-is-ddos-attack>. Acesso em: 08/07/2019.

ROBERTS, D. Brazilian president's visit to US will not include apology from Obama for spying. Junho de 2015. Disponível em: <https://www.theguardian.com/world/2015/jun/30/brazil-dilma-rousseff-obama-nsa-spying-apology>. Acesso em: 26/07/2019.

ROCHA, A. J. R. Relações Internacionais – Teorias e Agendas. Brasília: IBRI. 2002.

SARAIVA, J. F. S. Relações Internacionais em tempos de crise: ordem sincrética e novos paradigmas. Brasília: Funag/IBRI, 2012.

SCHMITT, M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

SCHULTZ, T. A Decade After "Web War 1," Former Estonian President Blasts EU Cyber Inertia. Abril de 2017. Disponível em: <http://www.atlanticcouncil.org/blogs/new-atlanticist/a-decade-after-web-war-1-former-estonian-president-blasts-eu-cyber-inertia>. Acesso em: 10/12/2019.

SOCIAL SECURITY. U.S. – Brazilian Social Security Agreement. Junho de 2015. Disponível em: <https://www.ssa.gov/international/Agreement_Texts/brazil.html>. Acesso em: 16/04/2020.

TAPPER, J. Obama administration spied on German media as well as its government. Julho de 2015. Disponível em: <https://edition.cnn.com/2015/07/03/politics/germany-media-spying-obama-administration/index.html>. Acesso em: 16/04/2020.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. Maio de 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 16/04/2020.

THE GUARDIAN. Iran accuses US and Britain of role in killing of nuclear scientist. Janeiro de 2012. Disponível em: <https://www.theguardian.com/world/2012/jan/14/iran-accuses-us-britain-scientist>. Acesso em: 16/04/2020.

TIKK, E.; KASKA, K.; RÜNNIMERI, K.; KERT, M.; TALIHÄRM, A.; VIHUL, L. Cyber Attacks Against Georgia: Legal Lessons Identified. Novembro de 2008. Disponível em: <http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf>. Acesso em: 10/12/2019.

U.S. ARMY CYBER COMMAND. About Army Cyber. Dezembro de 2017. Disponível em: <http://www.arcyber.army.mil/Organization/About-Army-Cyber>. Acesso em: 15/12/2019.

VAZ, A. C. Relações Internacionais em tempos de crise política. Brasília: Funag/IBRI, 2012.

ZURABISHVILI, S. Geórgia persegue o caminho da Europa. [Entrevista concedida a] Anelise Borges, da Geórgia. Euronews, Geórgia, 28 ago. 2019.