UnB – Universidade de Brasília
Instituto das Relações Internacionais

SEGURANÇA CIBERNÉTICA NO ÂMBITO DAS RELAÇÕES INTERNACIONAIS

Albert Galoyan
15/0001517

Brasília
2019

Albert Galoyan

Monografia apresentada como um requisito para conclusão de curso de Relações Internacionais da Universidade de Brasília

Orientador: Professor Thiago Gehre

Brasília, DF
2019

RESUMO

Nosso mundo cada vez mais depende da tecnologia, que sempre está em desenvolvimento e em constante mudança. Com avanço tecnológico vem também muitos perigos e problemas. A segurança cibernética é a proteção de sistemas conectados à Internet, incluindo hardware, software e dados, de ataques cibernéticos. No âmbito de Relações Internacionais este assunto é muito importante, pois muitas Organizações Internacionais e países se baseiam na tecnologia para funcionar. O objetivo do trabalho é mostrar a conexão entre a área de Segurança Cibernética com as Relações Internacionais, bem como também explorar as estratégias de Segurança Cibernética do Brasil, dos Estados Unidos, da Rússia e de Israel.

Palavras-chave: Segurança Cibernética. Internet. Hardware. Software. Vírus. Relações Internacionais. Risco. Conflito. Guerra Cibernética. Ciber Terrorismo. Malware. Hacker. Hacktivistas. Ciberespaço. Ransomware.

SUMÁRIO

INTRODUÇÃO

A monografia foi construída como um artigo científico, para aprofundar mais o debate de Segurança Cibernética e para acossa-la com a área de estudo de Relações Internacionais. O objetivo do trabalho é mostrar a conexão entre a área de Segurança Cibernética com Relações Internacionais, como também explorar as estratégias do Brasil, dos Estados Unidos, da Rússia e do Israel, sem a intenção de estudo comparativo. Como metodologia de abordagem, adotou-se a pesquisa descritiva, pois buscou-se entender e conhecer os conceitos e relações entre a Segurança Cibernética e as Relações Internacionais, além de descrever as estratégias de quatro países em relação à temática.

O Ciberespaço é um fenômeno sempre crescente que não tem limites territoriais e não tem a ideia de soberania. Ele existe no mundo material, por exemplo, os cabos, computadores e outros componentes tecnológicos, como também no mundo virtual. A Internet que conhecemos e usamos agora é somente uma parte pequeno do Ciberespaço. É complexo medir seu tamanho, por sua natureza sempre crescente. Além disso, existem também múltiplos tipos de ameaças, principalmente as criadas pelos indivíduos para prejudicar outros sistemas, surgindo assim a ideia de Guerra Cibernética.

Guerra Cibernética é um termo amplo, no qual um dos significados é o uso da força tecnológica no ciberespaço. Esse tipo de conflito não implica escala, protração ou violência, que são tipicamente associadas ao termo da guerra. Quando um país ataca outro país para prejudicar os sistemas vitais dos computadores militares ou outras tecnologias, e o país atacado retaliar, pode considerar-se uma Guerra Cibernética. Ainda, existe um debate sobre a aplicabilidade das regras de uma guerra convencional ao contexto de uma guerra cibernética.

Embora o campo da segurança cibernética não seja novo, a maturidade intelectual da perspectiva está se desenvolvendo. Grande parte do trabalho a ser feito no futuro requer uma maior consideração de métodos, evidências, bem como abordagens epistemológicas críticas que desafiariam a natureza dos arranjos institucionais relativos as questões cibernéticas. Há muito que o campo pode aprender das perspectivas da teoria e da ética das Relações Internacionais. Devido a importância do domínio cibernético para a pesquisa, educação, negócios e interações sociais, as ações no domínio trazem grandes riscos, mas também grandes possibilidades. O futuro pode não estar cheio de conflitos e violência, mas a linha entre estabilidade e caos corre sempre o risco de ser explorada no ciberespaço. A cooperação é o melhor caminho para um futuro estável.

1 O QUE É CIBERESPAÇO?

Para conseguir entender melhor a importância de segurança cibernética, é necessário primeiramente entender o que é o ciberespaço. Determinar o que é ciberespaço é complexo, pela dimensão global dele, como também do fato de estar sempre em desenvolvimento. Tudo começou com o Departamento de Defesa dos EUA, que criou a Rede de Agências de Projetos de Pesquisa Avançada (ARPANET), a primeira rede criada no mundo. Usando mesmos protocolos, foi criada a Internet que conhecemos agora. À medida que o projeto progrediu, os protocolos de *internetworking* foram desenvolvidos para que várias redes separadas pudessem ser unidas em uma rede de redes. O Acesso à ARPANET foi ampliado em 1981, começando a ser usada amplamente pelas outras organizações governamentais dos Estados Unidos. A ARPANET foi desativada em 1989.

A segurança cibernética surgiu em décadas recentes, pois nos anos 1970 – 1980 não havia tecnologia avançada para ser hackeada. Existiam violações de rede e *malware* que foram usados para roubar dados dos países inimigos e para espionagem. A exemplo, menciona-se o *hacker* alemão Marcus Hess, que em 1986 conseguiu hackear múltiplos computadores militares e roubar vários dados para vender os segredos de outros países para o KGB. Neste período, o vírus tornou-se uma ameaça muito perigosa para a confidencialidade dos segredos dos países. Por causa disso, começaram a ser criados novos programas que poderiam conter os vírus.[1]

Um exemplo importante de vírus é ‘a minhoca do Morris’, criado nos anos 1980 – 1990. Robert Morris teve a ideia de ver qual era o tamanho da internet, e por isso criou um programa que deveria ir de uma rede para outra, se replicando, o que resultou na total quebra da internet. Isso chamou a atenção dos governos para a segurança das redes, criando-se assim a primeira Equipe de Resposta a Emergências de Computadores, onde o alvo de qual, além de responder as emergências, era detectar e conter diferentes tipos de vírus que poderiam danificar a internet e servidores. A Minhoca do Morris foi um ponto de partida para os vírus mais fortes e ainda mais perigosos, com a capacidade de afetar múltiplos sistemas de uma vez.[2]

---

[1] **THE History Of Cyber Security** — Everything You Ever Wanted To Know. In: Sentileone, 10 mar. 2018.
[2] Idem.

A explicação mais recente do Ciberespaço foi feita em 2008 pelo Pentágono, onde determinaram este fenômeno como um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computadores, e processadores e controladores incorporados.[3] Por esta definição ser ampla, Peter Singer propôs uma mais simples, determinando o Ciberespaço como um domínio das redes de computadores nas quais as informações são armazenadas, compartilhadas e comunicadas *on-line*. Assim, percebe-se que este fenômeno não é algo físico, sendo difícil determinar sua dimensão e dar uma explicação pontual. Mas isso não significa que o ciberespaço é somente virtual, ele também compreende os computadores que armazenam os dados, bem como os múltiplos sistemas que o permitam fluir, ou seja, a internet, as tecnologias celulares, computadores, e todos os tipos de comunicações baseadas no espaço, como por exemplo, os satélites.

A Guerra de Informação é algo muito comum no nosso século, sendo a base desse rumo o roubo de informações privadas de vários usuários, criando assim um risco de vazamento de dados pessoais. O alvo desses tipos de ataques, além do econômico, também é direcionado às elites políticas, assim vazando dados classificados e até segredos de Estado. As empresas da nova era estão lidando com muito mais dados do que no passado. Como os dados vêm em novos tipos e formatos, são menos estruturados, ao contrário dos dados convencionais, e isso lhes põe em grande risco, pela falta de processos internos adequados e organizados. Outro grande risco para essas empresas é o fato de que eles usam o armazenamento em nuvem, pela limitação dos servidores, o que os coloca em uma situação vulnerável.

Os sistemas e tecnologias do ciberespaço foram criados pelo homem, isso significa que ele é definido tanto pelo domínio cognitivo quanto pelo físico ou digital. O mundo está dividido em nações e nacionalidades e o ciberespaço é diferente, ele não tem as noções de soberania, nacionalidade e propriedade, não tem uma divisão visível, mas certamente existe a divisão entre o virtual e físico. O Ciberespaço não pode ser governado por somente uma nação, o que o torna um fenómeno único, com métodos, regras, técnicas e políticas de uso diferenciados.[4]

---

[3] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014. p. 13

[4] Idem, p. 14.

O ciberespaço é uma fusão de todas as redes de comunicação, bancos de dados e fontes de informação, em um vasto e diverso emaranhado intercâmbio eletrônico. Assim, um ecossistema de rede é criado, um lugar que não faz parte do mundo físico normal. É virtual e imaterial, um ambiente bioeletrônico que é literalmente universal e que existe em toda parte onde há fios telefônicos, cabos coaxiais, linhas de fibra ótica ou ondas eletromagnéticas. O ciberespaço não é apenas virtual, mas também é baseado na realidade física composta de servidores, cabos, computadores, satélites e outros meios tecnológicos. Tendemos a usar os termos ciberespaço e Internet de forma quase intercambiável, mesmo que a Internet seja apenas uma parte do ciberespaço, embora certamente a mais importante nos dias de hoje.[5]

A segurança cibernética é tanto sobre a insegurança criada por e através deste novo espaço, quanto sobre as práticas ou processos para torná-lo mais seguro. Refere-se a um conjunto de atividades e medidas, tanto técnicas como não técnicas, destinadas a proteger o ambiente bioelétrico e os dados que contém e transporta de todas as ameaças possíveis. A terminologia em segurança da informação é muitas vezes aparentemente congruente com a terminologia nos discursos sobre segurança nacional, ou seja, trata-se de ameaças, agentes e vulnerabilidades.[6]

Uma maneira para categorizar ameaças é diferenciar as falhas, os acidentes e os ataques. Falhas são eventos potencialmente danosos causados por deficiências no sistema ou em um elemento externo do qual o sistema depende. As falhas podem ser causadas por erros de design de software, degradação de hardware, erros humanos ou dados corrompidos. Acidentes incluem toda a gama de eventos que ocorrem aleatoriamente, como desastres naturais. Ataques são eventos potencialmente prejudiciais orquestrados por um adversário humano. Essas categorias são o foco principal do discurso de segurança cibernética.[7]

No debate sobre segurança cibernética, o *hacking* é considerado um *modus operandi* que pode ser usado não apenas por indivíduos com habilidades tecnológicas para pequenas contravenções, mas também por grupos de atores organizados com intenção realmente ruim, como terroristas ou estados estrangeiros. Alguns hackers podem ter habilidades para atacar as partes da infraestrutura de informações consideradas críticas para o funcionamento da sociedade. Existem várias ferramentas e modos de ataque. O termo usado para a totalidade dessas ferramentas é o

[5] CAVELTY, Myriam Dunn. **Cybersecurity Contemporary Security Studies**. Oxonia, UK: Oxford University Press, 2012. p. 2
[6] Idem.
[7] Idem.

malware, que são *softwares* maliciosos. Exemplos bem conhecidos são vírus e minhocas, programas de computador que replicam cópias funcionais de si mesmos com efeitos variados que vão desde simples aborrecimento e inconveniência até o comprometimento da confidencialidade.[8]

Antigamente o fenômeno Ciberespaço foi usado somente para comunicação e comércio eletrônico, mas passou a ser usado para a infraestrutura crítica da sociedade moderna, ou seja, agricultura, distribuição de comida, saúde, transporte, água e energia. Todas essas áreas são interdependentes e conectadas ao Ciberespaço, com tecnologia de informação, também chamados de sistemas de controle de supervisão e aquisição de dados (SCADA). Estes são os sistemas de computador que monitoram, ajustam a comutação e controlam outros processos de infraestrutura crítica. O Presidente dos EUA à época, George W. Bush, mencionou que o Ciberespaço é um sistema nervoso, ou seja, um sistema de controle de nossa economia, mas agora é muito mais que isso, o Mundo inteiro está dependente do Ciberespaço. Mas tudo no nosso mundo vem com riscos e perigos, e o Ciberespaço não é uma exceção.[9]

A Internet é global, isso significa que o mundo inteiro tem acesso ao mesmo espaço. Cada computador em existência é uma parte da mesma rede, e o Sistema de Nomes de Domínio lhes disponibiliza uma lista de todos os domínios, ou seja, sites criados. Os prestadores de serviços de internet, que são principalmente companhias privadas, disponibilizam o acesso dos computadores à internet. Tudo isso cria Sistemas Autônomos na rede global, que definem a arquitetura das conexões de internet, e são interligados de modos diferentes.[10] Entendendo todas essas explicações básicas da internet, podemos perceber duas compreensões da segurança cibernética: a primeiro é que para a função da internet não é necessária uma coordenação perfeita. A segunda, nos mostra que os coordenadores e usuários precisam se comportar de maneira adequada, para evitar quaisquer pontos de estrangulamento, que criam vulnerabilidades para ataques dos *hackers*.

O conceito da segurança no âmbito do Ciberespaço é diferenciado, pois para um problema virar uma questão de ameaça da segurança do usuário é necessário ter um segundo lado que querendo atingir algum alvo específico. Assim, dispositivos podem ser quebrados e erros podem ser cometidos na manutenção da internet, mas um problema cibernético só se torna uma questão de segurança cibernética se um adversário busca ganhar algo da atividade, seja para obter

---

[8] CAVELTY, Myriam Dunn. **Cybersecurity Contemporary Security Studies**. Oxonia, UK: Oxford University Press, 2012. p. 5
[9] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014. p. 15
[10] Idem, p. 24.

informações privadas, prejudicar o sistema ou impedir seu uso legítimo. Neste caso, isso é chamado de ataque cibernético e muitas vezes os alvos são grandes companhias que têm dados vitais dos usuários da internet. Assim, se tiver algum tipo de falha no sistema, isso não é uma ameaça da segurança, mas se esta falha foi causada pelo algum hacker, isso já se torna um problema de segurança.[11]

A definição básica de segurança é associada ao alívio de ameaças estimadas, especialmente aqueles que, se não forem controlados, ameaçam a sobrevivência de um determinado objeto de referência em um futuro próximo. Assim, uma ameaça direcionada a um sistema, é considerada uma questão de segurança, se o alvo é danificar qualquer tipo de informação ou dado. A segurança envolve a capacidade de perseguir ambições políticas e sociais, que é o contrario da definição de sobrevivência. Muitas vezes estes dois conceitos estão sendo associados, e neste caso, a segurança é entendida como um meio de assegurar, em alguma medida, contribuir para a sobrevivência. Além disso, mais poder significa maior capacidade de segurança.[12] Isso pode ser visto em casos de *Ciber* Segurança também, por exemplo, quanto melhor o meio de proteção, mais poderoso é sistema de detecção de ameaças, podendo ser melhor ser contidas.

Outra terminologia de segurança nos mostra que ela pode ser baseada na emancipação, ou seja, existe uma preocupação com a justiça e a provisão de direitos humanos. Nesse caso, a segurança é entendida como uma relação entre diferentes atores e não como um meio de conseguir sobreviver. Assim, a relação entre os atores decide se uma ameaça ou ação vira uma questão de segurança. Nesse caso, a segurança vem da necessidade de cooperar para obtê-la, sem priva-la de outros. Sem um objeto de referência, não pode haver ameaças nem discussões sobre segurança, porque o conceito não tem sentido sem algo para proteger. Na área das Relações Internacionais, a segurança é associada com o Estado, mais especificamente com o interesse nacional, mas no âmbito cibernético ela pode ser associada com o interesse de preservar a integridade do Ciberespaço. Esses objetos podem ser servidores de grandes firmas, bancos, como também de Ciberespaço em si.

Cada indivíduo tem suas prioridades de segurança, ou seja, eles estão preocupados com o que pode acontecer no futuro e como as ações deles podem impactar nesse futuro. Do mesmo modo, cada empresa e banco estão preocupados com a segurança, seja cibernética ou não. Assim, formam agendas de ameaças e como elas podem ser contidas. As enormes desigualdades de poder e

[11] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar.** Oxonia, UK: Oxford University Press 2014. p 34
[12] WILLIAMS, D. Paul. **Security Studies - An Introduction**. New York: Routledge, 2008. p. 6

influência que existem entre indivíduos e grupos no mundo contemporâneo, dificultam ainda mais a prevenção de ameaças e a criação de agendas de ameaça.[13] Assim, as prioridades de agentes de segurança cibernética devem ser direcionadas à proteção de seus sistemas com tecnologia mais avançada do que dos seus potenciais ameaçadores, e por isso, o monitoramento constante de sistemas é necessário para atingir a proteção suficiente.

Uma ameaça de ataque cibernética cria os objetivos canônicos de segurança em um ambiente de informações. Confidencialidade, Integridade e Disponibilidade são os três alvos mais importantes para segurança do Ciberespaço, determinados pela CIA. O primeiro alvo refere-se a manter os dados privados. A informação tem seu valor e isso significa que a proteção é muito importante. Todos os dados pessoais e dados de transições entre companhias e indivíduos devem ser mantidos classificados e com proteção forte. A confidencialidade é garantida por meios de criptografia, controle de acesso, como também pelas proteções legais dos dados. A Integridade é a parte mais importante do triunvirato clássico de segurança da informação. A premissa básica desse termo é a garantia de que o sistema e os dados nele não foram alterados indevidamente sem autorização. Assim, deve haver confiança de que o sistema fica disponível e comportar-se como esperado. A integridade é um alvo principal para todos os hackers que tem experiência e a capacidade avançada de infiltrar um sistema protegido. Determinar se um sistema está funcionando como deve é complexo, porque só o próprio sistema pode detectar os erros.[14]

A Disponibilidade significa poder usar o sistema como previsto. Quando um sistema cai por qualquer tipo de erro, causa uma temporária falta de disponibilidade, mas isso ainda não vira um problema de segurança crucial, mas torna-se um problema sério somente quando e se alguém tentar explorar a falta de disponibilidade de alguma forma. O hacker pode alcançar este objetivo privando os usuários de um sistema de que eles dependem ou simplesmente ameaçando a perda de um sistema, conhecido como ataque de *ransomware*. Um exemplo de ataque assim é considerado ataque sobre as contas bancárias individuais, ou até direcionados às informações bancárias das grandes companhias.[15]

Um dos alvos de segurança propostas pela CIA é Resiliência. Isso permite que um sistema enfrente ameaças de segurança diretamente, em vez de falhar criticamente. Uma chave para a

[13] WILLIAMS, D. Paul. **Security Studies - An Introduction.** New York: Routledge, 2008. p. 8
[14] SINGER, Peter Warren, FRIEDMAN, Allan. Cybersecurity and Cyberwar. Oxonia, UK: Oxford University Press 2014. p 35.
[15] Idem, p. 36

resiliência é aceitar a inevitabilidade de ameaças e até falhas limitadas em suas defesas. Com isso, o sistema permanece funcionando até sabendo que um ataque ou uma falha pode acontecer em qualquer momento. Assim, se um ataque acontecer, o sistema vai proteger os dados vitais e tentar voltar ao funcionamento normal o mais rápido possível. Todos esses aspectos não são somente problemas técnicos, mas organizacionais, legais, econômicos e também sociais. Segurança custa dinheiro, mas também custa tempo, conveniência, capacidade, liberdade e, exatamente por essa razão, cada problema no sistema tem sua resposta adequada de resolução.[16]

Ataques cibernéticos podem ser realizados de formas diferentes e para alvos variados. Mas para um ataque acontecer é necessário ter um lado que deseja ganhar algo do outro lado. Existem três tipos de ações que os *hackers* podem fazer com um computador: roubar os dados, usar credenciais de forma inadequada e roubar recursos importantes. Com a grande dependência de tecnologia na humanidade, um ataque qualquer pode causar muitos danos. Dados roubados podem revelar os planos estratégicos de um país ou minar a competitividade de toda uma indústria. As credenciais roubadas podem dar a capacidade de alterar ou destruir códigos e dados, alterar folhas de pagamento e muito mais. Os *Hijacks*, ou roubos de recursos, podem impedir que uma empresa alcance clientes ou negue a capacidade de comunicação de um exército. Cada tipo de ameaça deve ser respondido com recursos adequados, e é importante saber os alvos dos Hackers, os dados roubados e como eles vão ser utilizados.[17]

Um dos tipos de ataques mais comuns é o *Malware*, que é qualquer programa ou arquivo que seja prejudicial a um usuário de computador. O *malware* inclui vírus de computador, minhocas, cavalos de Tróia e *spyware*. Isso tem sido usado não apenas para controlar um sistema de computador, mas para manter o controle dele, a fim de explorar seus recursos computacionais e de rede. Assim, o *Malware* pode ser usado para coletar dados pessoais de qualquer usuário, criptografa-los e até manipular as ações do usuário. Vírus, é o tipo mais comum de *malware*, definido como um programa malicioso que pode se executar e se propagar, infectando outros programas ou arquivos. Outro tipo de ataque comum é considerado o ataque DDoS, que visam os subsistemas que lidam com conexões com a Internet, como servidores da Web. Suas vulnerabilidades baseiam-se no princípio de que, responder a uma consulta recebida consome recursos computacionais e de largura de banda. Assim, um site e até o servidor ficam corrompidos

[16] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014. p. 36
[17] Idem, p. 39

e param de funcionar. Pode-se perceber que as vulnerabilidades existem em todo tipo de sistema de informação no ciberespaço.[18]

Recentemente um novo tipo de ameaça ao Ciberespaço apareceu, chamada de APTs, que são as ameaças persistentes avançadas, ganhando cada vez mais notoriedade nos últimos anos, mas ainda é pouco compreendida. Ela ilustra o desafio no mundo da política, para chamar atenção aos desafios emergentes muito reais no ciberespaço, mas também evitar reações exageradas, excitação e histeria. Esse tipo de ameaça tem muito mais planejamento atrás da realização do que qualquer outro tipo de ameaça existente. Eles têm o seu alvo específico e sabem o que querem ganhar do ataque. Os alvos do APT são variados, podem ser projetos de jatos militares ou até segredos comerciais de empresas petrolíferas. Os *Hackers* atrás do ataque são parte de uma equipe coordenada de especialistas, onde cada um deles assume papéis diferentes. Eles geralmente usam sites como Google para colecionar o máximo de informações sobre uma companhia ou sobre uma pessoa antes de realizar o ataque, assim eles conseguem achar as vulnerabilidades do seu alvo. Estes tipos de ataque começam por diferentes meios, mas o mais comum é quando os *Hackers* mandam e-mails com um documento infetado de *Malware* muito sofisticado, que até o antivírus do computador não pode detectar, e assim, a vitima está completamente sob a controle do Grupo de *Hackers*. Além de roubar todos os dados, os APTs também deixam um programa sofisticado para conseguir detectar e roubar qualquer novo dado, assim este tipo de ataque é o mais perigoso para qualquer companhia. [19]

O crime cibernético e os vírus se tornaram uma realidade indiscutível e cotidiana, enquanto os grandes ataques cibernéticos com grande impacto, que substanciariam tal raciocínio, permaneceram meras fantasias, ou seja, a porcentagem desses ataques de grande escala é comparativamente menor. Do ponto de vista construtivista, a segurança nacional sempre foi sobre a constelação social de questões específicas, como uma ameaça, e sobre a definição de respostas desejáveis para essas questões. No caso de novas ameaças, os profissionais de segurança têm uma necessidade ainda maior de estabelecer uma conexão confiável para a segurança nacional, porque a dimensão da segurança nacional é menos explícita quando se trata do meio ambiente, da sociedade ou da economia. Os riscos existem em um estado permanente de virtualidade e só são realizados através de antecipação delas, pois não podem ser vistos. A antecipação desses futuros

[18] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014, p. 44
[19] Idem, p. 56

desastres, em vez de experiências passadas ou uma sólida justificativa para o atual nível de ameaça, é a principal razão para agir no presente.[20]

Antigamente, as ameaças cibernéticas não recebiam muita atenção do público em geral, nem foram vistas como um problema para a sociedade, pois a ameaça pertencia principalmente às redes do governo e às informações classificadas que residem nelas. Não obstante, o crime cibernético continua sendo um fator determinante no discurso em geral, pois é a representação da ameaça com o elo mais próximo da realidade. Por causa da subestrutura tecnológica, os ataques prejudiciais poderiam ser realizados de inúmeras maneiras, potencialmente por qualquer pessoa com um computador conectado à internet e para propósitos que vão desde o delito juvenil ao crime organizado, ao ativismo político e à guerra estratégica.

A literatura atual sobre a regulação do ciberespaço não está mais focada em saber se o ciberespaço pode ser regulado, mas sim concentra-se em como o ciberespaço é regulado e quem são os reguladores. É geralmente aceito que o Estado não pode controlar adequadamente o ciberespaço através de leis e regulamentos, mesmo quando elas são mantidas atualizadas com os desenvolvimentos tecnológicos, pois a eficácia é limitada, as dimensões transnacionais de grande parte da ilegalidade cibernética e as arquiteturas da tecnologia digital praticamente garantem isso. Além do código e da arquitetura, os próprios mercados podem servir como instituições reguladoras. Em comparação com as leis promulgadas pelo governo, a auto-regulamentação oferece maior velocidade, flexibilidade e sensibilidade às circunstâncias do mercado, como também, eficiência e menos intervenção do governo. A configuração institucional apropriada para a segurança cibernética variará com o tempo e o local, dependendo da configuração de segurança em questão e das capacidades predominantes dos participantes individuais. Os esforços do setor privado podem, em algumas situações, compensar as deficiências por parte do governo.[21]

Sob o princípio da soberania territorial, um Estado exerce autoridade plena e exclusiva sobre o seu território. Deve ser lembrado que a soberania territorial tem um caráter relativo, na medida em que não oferece apenas proteção aos Estados, mas também impõe obrigações aos mesmos. Existe uma visão amplamente aceita sobre o Ciberespaço, de que, ele não é um lugar físico, desafia a medição em qualquer dimensão física ou espaço de tempo contínuo. É um ambiente

[20] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010.
[21] CHANG, Y. C. Lennon; GRABOSKY, Peter. The governance of cyberspace. In: Regulatory Theory: Foundations and applications. Canberra, Australia: ANU Press, The Australian National University, 2017. p. 535

criado pela confluência de redes cooperativas de computadores, sistemas de informação e infraestruturas de telecomunicações comumente referidas como a *World Wide Web*. Assim, o ciberespaço em sua totalidade não está sujeito à soberania de um único Estado ou grupo de Estados e é imune à apropriação.[22]

Imunidade Soberana significa que qualquer interferência em um objeto que goze de tal imunidade constitui uma violação da soberania desse Estado. Deve-se ter em mente, entretanto, que em tempos de conflito armado internacional, o princípio da imunidade soberana não desempenha nenhum papel nas relações entre os Estados beligerantes. A imunidade pode ser destruída se eles se qualificarem como alvos legítimos ou estiverem sujeitos à captura como espólio de guerra pelas forças armadas do inimigo. Além disso, a imunidade soberana não é ilimitada.

A representação da ameaça da guerra cibernética é fortemente influenciada pela crescente sofisticação tecnológica dos militares dos EUA e evoluiu em paralelo com a do terrorismo cibernético. Dentro da vasta família de conceitos de guerra de informação, ataques a redes de computadores, ações tomadas através do uso de redes de computadores para interromper, negar, degradar ou destruir informações residentes em computadores e redes, são equacionados à ideia de ciber-guerra. A intervenção da OTAN em 1999 contra a Iugoslávia marcou o primeiro uso sustentado do espectro completo dos componentes da guerra de informação em combate. Muito disso envolveu o uso de propaganda e desinformação através da mídia, que é o aspecto mais importante de guerra de informação, mas também houve amplos ataques distribuídos de negação de serviço em vários sites.[23]

Atualmente, toda tensão política ou conflito é acompanhada de atividade intensificada no ciberespaço, e é norma que nossas sociedades são confrontadas diariamente com crimes cibernéticos e todos os tipos de incidentes cibernéticos mais ou menos destrutivos que causam crimes menores e, ocasionalmente, grande inconveniente para usuários particulares, empresas e organizações governamentais. Esse tipo de retórica contra as ameaças invoca as imagens inimigas, mesmo que não haja um inimigo identificável, favorece as soluções nacionais, em vez de

[22] HEINEGG, Wolff Heintschel von. Territorial Sovereignty and Neutrality in Cyberspace. **International Law Studies**, v. 89, 2013, p. 125

[23] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010. p. 183.

internacionais, e centra-se nas medidas de segurança nacional, em vez de soluções econômicas e comerciais.[24]

Apesar da crescente atenção que a segurança cibernética está obtendo nas políticas de segurança, e apesar da possibilidade de um incidente catastrófico importante e sistêmico envolvendo infraestruturas críticas, as vulnerabilidades das redes de computadores são principalmente um problema de negócios e de espionagem. Dependendo de sua gravidade, no entanto, os incidentes disruptivos continuarão a alimentar o discurso militar e, com isso, os temores de uma guerra cibernética estratégica. Sem duvida, o planejamento das respostas aos piores cenários é uma tarefa legítima do aparato de segurança nacional. No entanto, eles não devem dar muita atenção aos problemas mais plausíveis e possíveis.[25]

Assim, pode-se perceber que o Ciberespaço é um fenômeno pouco explorado pelo seu tamanho quase infinito. Mas isso não significa que ameaças não existem nela. Muitos governos usam a sua capacidade tecnológica para avançar a sua segurança cibernética por causa de múltiplos ataques cibernéticos e roubo de dados cruciais. Existem múltiplos tipos de ameaças, que estão sendo enfrentados diariamente. É necessário explorar melhor o Ciberespaço para conseguir responder melhor a todos os tipos de ataques no futuro com métodos mais eficientes. É difícil prever o futuro do Ciberespaço, mas com a popularização da inteligência artificial, novas oportunidades vão se abrir no mundo cibernético e com isso surgirão novas ameaças.

[24] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010. p. 183

[25] CAVELTY, Myriam Dunn. **Cybersecurity Contemporary Security Studies**. Oxonia, UK: Oxford University Press, 2012. p. 24

2 GUERRA CIBERNÉTICA

Para compreender o que pode ser considerado uma Guerra Cibernética, é necessário entender melhor o conceito. Um ataque cibernético pode ser chamado de um protesto on-line ao roubo de segredos da Internet, sabotagem cibernética de pesquisas nucleares e até atos de guerra no campo de batalha com o uso de alta tecnologia. A exemplo disso, as Forças Militares dos EUA são alvos de múltiplos ataques cibernéticos todos os dias. Um ataque cibernético não é como qualquer ataque convencional, são usados meios digitais e ações diferentes de computadores.[26]

Um ataque no Ciberespaço não tem limites territoriais nem constrangimentos nacionais, é muito mais rápido e pode ter múltiplos alvos, sempre atingindo um computador e as informações nele contidas. Os resultados pretendidos do ataque podem ser, por exemplo, danificar algo físico, mas esse dano sempre resulta, em primeiro lugar, num incidente no reino digital. Além disso, é difícil determinar quem iniciou o ataque e de que forma. Em alguns casos os Hackers colocam seu nome no *Malware* que criaram para serem reconhecidos, pois para eles isso é um prestigio.

Existem diferentes tipos de ataques, sendo eles: *ataques de disponibilidade*, que tentam impedir o acesso a uma rede, sobrecarregando-a com visitas, que pode criar uma negação de serviço ou até mesmo desativando-a para encerrar os processos físicos ou virtuais que dependem dela; *Ataques de confidencialidade*, que são esforços para entrar nas redes de computadores, a fim de monitorar as atividades e extrair informações sobre os sistemas e os dados dos usuários. O tempo e o custo dessa ação dependem da quantidade de dados a serem extraídos;[27] *Ataques de integridade,* envolvem a penetração no sistema para mudar, em vez de extrair informações. Eles manipulam dados no mundo virtual, bem como os sistemas e pessoas que dependem desses dados. Este tipo de ataque pode ser feito como meio de vandalismo ou para causar danos significantes ao sistema.

Sem dúvida, todos os tipos de ataques precisam planejamento amplo e execução quase perfeita para atingirem os seus alvos sem nenhuma interrupção. Em muitos casos, encontra-se dificuldade em distinguir os tipos de ataques, pois, por exemplo, um ataque de confidencialidade e um ataque de integridade ambos exploram vulnerabilidades para obter acesso a um sistema.[28]

---

[26] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014. p. 69.
[27] Idem, p. 70
[28] Idem, p. 70

A Informação e seu fluxo podem ser interpretados de maneiras diferentes. A Conexão da internet e a livre navegação foram determinadas como um direito humano, pelas autoridades dos Estados Unidos da América, mas o mesmo fluxo livre foi descrito pelos líderes na Rússia e na China, não como um direito humano, mas como um ataque de informação destinado a minar a estabilidade do Estado. Como resultados, em intercâmbios internacionais, oficiais dos EUA falaram sobre ataques cibernéticos em termos de ataques e intrusão de sistemas cibernéticos e infraestrutura crítica, enquanto seus pares como a Rússia, os discutiram como parte de uma guerra de informação ocidental para minar regimes em nome da reforma democrática.[29]

Existem múltiplos tipos de *Malware* que criam programas nos computadores infectados, que servem para controlar todas as funções chaves do sistema, assim influenciando o usuário. Os três fatores mais importantes, com capacidade de capturar e utilizar outros computadores, que são particularmente importantes, são os seguintes: a) não existem limites geográficos, por exemplo, alguém no Brasil pode comprometer os computadores na África do Sul para lançar ataques a sistemas na China, que podem ser controlados por computadores localizados fisicamente nos Estados Unidos, que sem dúvida é uma ação complexa de detectar; b) O usuário pode até não saber que alguém está controlando o computador dele; c) Quando alguma atividade prejudicial é perpetrada, a análise sofisticada pode, no melhor caso, identificar o computador que está sendo usado para iniciar o ataque e, com isso, alguém que esteja por trás dele.[30]

Na segurança cibernética, em geral, existem dilemas de atribuição. É preciso pesar os ganhos potenciais *versus* as perdas de apontar o dedo para um grupo ou indivíduo que considera-se que está por trás de um ataque cibernético. Determinando o atacador, pode haver conexão com ganhos pessoais de algum país ou pessoa. Por exemplo, pode-se acusar alguém a fim de fazer um contra-ataque, ou seja, um país pode acusar um país inimigo para justificar o seu ataque de volta. Objetivos e ações diferentes exigem padrões variados. A exemplo, os EUA em 2011, p estavam dispostos a acusar a China por roubo cibernético, na esperança de causar algum efeito de vergonha, mas neste caso, não havia certeza absoluta para o seguimento da ação dos EUA.[31]

O cibercrime, conhecido também como crime de computador, é mais frequentemente definido como o uso de ferramentas digitais por criminosos para roubar ou realizar atividades ilegais. Um dos crimes que mais provocam danos é a fraude de credenciais, também conhecido

[29] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014. p. 72
[30] Idem, p. 74
[31] Idem, p. 76

como uso indevido de detalhes da conta para fraudar sistemas financeiros e de pagamento. Tais sistemas incluem cartões de crédito, contas de caixa eletrônico e contas bancárias *on-line*. Para fazer isso, os *hackers* roubam os dados dos usuários com *malware*.[32]

A possibilidade de aplicar as leis da Guerra Convencional à Guerra Cibernética está sempre em debate. Uma revisão da aplicabilidade da lei de guerra existente sugere que se abordarmos a guerra cibernética como envolvendo o uso de uma nova tecnologia para obter vantagem militar, o atual corpo de leis internacionais pode ser aplicado ao conflito cibernético, mas algumas questões envolvendo soberania, combatentes e outros assuntos da guerra, precisam de mudança de regras e redefinição. O enquadramento jurídico presente pode ser aplicado aos atores estaduais como não estatais, mas isso depende do fator do uso de força. Os ataques cibernéticos são geralmente usados para cometer crimes e espionagem, que não são reconhecidos como atos de Guerra.[33]

Dois corpos separados da lei se aplicam à guerra cibernética: o "*jus ad bellum*", onde as leis que regem a decisão de recorrer ao uso da força, que guiam a decisão de uma nação, se um incidente justifica o envolvimento em conflito armado ou desencadeia as provisões da Carta das Nações Unidas sobre o direito de uma nação usar a força em autodefesa, aplicável se o atacante é um ator estatal ou não estatal. E o segundo corpo, o "*jus in bello*", que são as leis que regem a conduta das hostilidades. Se uma exploração cibernética constituísse um ataque armado, as autoridades nacionais poderiam começar o ato de autodefesa. Uma exploração que não causou diretamente morte substancial ou destruição física, não se qualificaria como um ataque armado.[30]

O uso do ataque cibernético é regido pelo "*jus in bello*" ou a Lei do Conflito Armado. A lei estabelece regras que governam o uso da força durante conflitos armados. Três princípios do Direito da Guerra estabelecem uma estrutura para julgar a legalidade do uso de diferentes formas de ataque cibernético durante um conflito armado: a) O princípio de distinção requer que os ataques sejam limitados a objetivos militares legítimos e que objetos civis não sejam alvo de ataque; b) O princípio da proporcionalidade exige que o uso da força em legítima defesa seja limitado e proporcional à ameaça que é enfrentada; c) O princípio do ataque discriminatório proíbe ataques que não possam ser razoavelmente limitados a um objetivo militar, e com alvos civis aleatórios.[34]

---

[32] SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014. p. 85
[33] LEWIS, A. James. **A Note on the Laws of War in Cyberspace**. In: CSIS, 25 abr. 2010.
[34] LEWIS, A. James. **A Note on the Laws of War in Cyberspace**. In: CSIS, 25 abr. 2010.

As leis existentes para conflitos armados podem ser aplicadas ao ataque cibernético, mas existem áreas de ambiguidade envolvendo a violação da soberania de terceiros. O uso de ataques cibernéticos por terroristas e a quantidade e natureza dos danos causados poderiam ser interpretados como um ato de guerra. Todas essas questões precisam ser profundamente discutidas e analisadas, pois o Ciberespaço é amplo e novas ameaças surgem diariamente.

Guerra cibernética é o uso de tecnologia de computador para interromper as atividades de um estado ou organização, especialmente o ataque deliberado de sistemas de informação para fins estratégicos ou militares. A Rússia e a China estão desenvolvendo armas cibernéticas para usar em qualquer conflito cibernético no futuro, assim como os EUA, a França e Israel, que também são ativos nessa área. Todos esses países têm a capacidade de começar uma Guerra cibernética. Existem diferentes meios de ataque cibernético, um deles é o uso de DDoS botnets, que servem para ataques de negação de serviço que podem atrapalhar e até tirar os servidores estratégicos do jogo.[35]

Os ataques de engenharia social também são armados para introduzir um invasor no sistema de um adversário. O método mais fácil de entrar no sistema do inimigo é ter um espião que poderia inserir manualmente um vírus no sistema. Um dos melhores exemplos de ataque cibernético, que pode ser classificado como Guerra Cibernética, é a acusação feita sobre a Rússia de montar múltiplos ataques cibernéticos contra a Ucrânia, incluindo o ataque *BlackEnergy* que cortou o poder de 700.000 lares no país em 2015 e o *malware NotPetya*, que se disfarçou de *ransomware*, mas na verdade foi projetado apenas para destruir os sistemas que infectou.[36]

Em suma, a guerra cibernética é o uso ou a segmentação de sistemas de controle *on-line* e de redes, em um ambiente de batalha ou guerra de computadores. Envolve tanto operações ofensivas quanto defensivas relativas à ameaça de ataques cibernéticos, espionagem e sabotagem. Tem havido controvérsia se tais operações podem realmente ser chamadas de guerra, devido às leis internacionais que determinam o significado do contexto. No entanto, os países têm desenvolvido capacidades cibernéticas e se engajaram em guerras cibernéticas, ofensivamente e defensivamente. A natureza distribuída dos ataques baseados na *Internet* significa que é difícil determinar a motivação e a parte atacante, ou seja, não é claro quando um ato específico deve ser considerado um ato de guerra e quando se deve começar a defender-se e até mesmo retaliar o

[35] Idem.
[36] HOPPING, Clare, SHEPHERD, Adam, WINDE, Davey. **What is cyber warfare?** In: ITPro, 12 dez. 2018.

ataque. A ascensão do ciberespaço como um domínio de combate levou a esforços para determinar como o ciberespaço pode ser usado para promover a paz, ou seja, limitar as armas cibernéticas e espionagem, por isso a Defesa Cibernética se torna um assunto crucial.[37]

[37] HOPPING, Clare, SHEPHERD, Adam, WINDE, Davey. **What is cyber warfare?** In: ITPro, 12 dez. 2018.

3 ABORDAGEM TEÓRICA E SEGURANÇA

Teoria das relações internacionais é o estudo das relações internacionais a partir de uma perspectiva teórica. Procura fornecer uma estrutura conceitual sobre a qual as relações internacionais podem ser analisadas, bem como aplicadas a contexto, inclusive ao estudo de segurança. Nesta seção serão exploradas algumas teorias e sua conexão com o âmbito da segurança.

O realismo clássico do século XX é geralmente datado de 1939, e marcado pela publicação da obra Vinte anos de Crise, de Edward Hallett Carr. De acordo com o realismo clássico, os estados estão continuamente engajados em uma luta para aumentar suas capacidades, porque o desejo por mais poder está enraizado na natureza defeituosa da humanidade. Basicamente, o realismo clássico explica o comportamento conflitivo das falhas humanas. As guerras são explicadas, por exemplo, por agentes do Estado particularmente agressivos ou por sistemas políticos domésticos que dão a grupos limitados gananciosos a oportunidade de buscar políticas externas expansionistas de interesse próprio. Para os realistas clássicos, a política internacional pode ser caracterizada como o mal. O realismo clássico, no entanto, postula que o comportamento do estado pode ser entendido como tendo micro fundamentos racionais.[38]

O Realismo tenta a esclarecer a relação entre ordem política e segurança. Assim, se os assuntos humanos são, de fato, caracterizados por um grupo só, pelo egoísmo e por poder-centrismo, então a política provavelmente será conflituosa, a menos que exista alguma autoridade central para impor a ordem. Quando não existe autoridade que possa impor acordos, em um estado de anarquia, então qualquer ator pode recorrer à força para conseguir o que quer. Assim, o argumento realista é que a anarquia torna a segurança problemática, potencialmente conflituosa e é uma das principais causas subjacentes da guerra. O dilema dessa abordagem é que resolvendo o problema da anarquia dentro de um grupo, apenas o amplia entre os grupos, por isso, há necessidade de combater a anarquia em todos os grupos de maneira mais estratégica.[39]

Uma diferença entre o realismo clássico e o neorrealismo, é a visão contrastante sobre a fonte e o conteúdo das preferências dos estados. Contra o realismo clássico, o neorrealismo exclui a constituição interna de diferentes estados. O comportamento dos estados pode ser um produto da

[38] WILLIAMS, D. Paul. **Security Studies - An Introduction**. New York: Routledge, 2008. p. 17
[39] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010. p. 10

competição entre eles, porque eles calculam como agir em sua melhor vantagem, sendo que os estados que não exibem tal comportamento, estão fora do sistema.[40]

O realismo defensivo compartilha os pressupostos mínimos do neorrealismo sobre as motivações do Estado. Como o neorrealismo, o realismo estrutural defensivo sugere que os estados buscam segurança em um sistema internacional anárquico, ou seja, a principal ameaça ao seu bem-estar vem de outros estados. O realismo defensivo depende unicamente da escolha racional, além disso, ela acrescenta o equilíbrio defesa-defesa como uma variável. O argumento deles é que as tecnologias predominantes ou as circunstâncias geográficas muitas vezes favorecem a defesa, os recursos apreendidos não se acumulam facilmente com aqueles já possuídos pela metrópole, os dominós não caem e a potência é difícil de projetar à distância. Assim, os estados devem apoiar o *status quo* para o seu maior beneficio.

O realismo defensivo sugere que a tentativa de um estado de se tornar mais seguro aumentando seu poder é, em última análise, fútil. Os realistas defensivos sugerem que os estados devem buscar uma quantidade apropriada de poder. Se os estados buscam a hegemonia, isso se deve às preferências geradas internamente, ou seja, buscar poder superior não é uma resposta racional às pressões sistêmicas externas. Assim o melhor método de segurança para eles é a busca de maior defesa para o seu beneficio, ao invés de buscar poder absoluto.

O realismo se baseia em três premissas centrais. O Grupismo, onde a premissa básica é que as políticas ocorrem dentro e entre grupos. A solidariedade de grupo é essencial para a política interna, o conflito e a cooperação entre as políticas são a essência da política internacional. Assim, essa premissa é chave para a segurança coletiva dos grupos; O Egoísmo, que é quando indivíduos e grupos agem politicamente e são dirigidos principalmente por interesses próprios. Essa premissa pode prejudicar a segurança coletiva; A premissa final é o Poder-centrismo, onde os assuntos humanos são sempre marcados por grandes desigualdades de poder em ambos os sentidos daquele período: influência social ou controle de recursos. A chave para a política em qualquer área é a interação entre poder social e material, uma interação que se desdobra à sombra do uso potencial do poder material para coagir. [41]

Immanuel Kant era um dos maiores filósofos do Liberalismo. Ele argumentou que os estados republicanos eram produtores de paz, isto é, eles estavam mais inclinados ao

[40] WILLIAMS, D. Paul. **Security Studies - An Introduction.** New York: Routledge, 2008. p. 20
[41] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010. p. 10

comportamento pacífico do que outros tipos de estados. Assim, um cidadão comum não estaria ao lado de um político que quer começar uma Guerra. Ele atribuiu isso aos fundamentos jurídicos do Estado republicano, porque acreditava que um Estado baseado na lei era menos propenso a endossar comportamento ilegal nas relações internacionais. Ele confirmava que a ideia de equilíbrio de poder consciente era falaciosa, porque o desejo de todo estado ou de seu governante, a chegar para uma condição de paz perpétua conquistando o mundo inteiro, não é o método certo.[42]

A característica mais distintiva do liberalismo é a crença em um processo pelo qual a razão humana pode promover um mundo mais próspero, livre e pacífico. Kant descreveu a natureza humana como uma mistura de mal e bondade em proporções desconhecidas. Mas Kant permaneceu otimista sobre a capacidade do homem de evoluir para longe de seus primórdios crassos e se beneficiar da razão. Mas no nível sistêmico, examinamos como os estados interagem uns com os outros no sistema global. O efeito pacífico do comércio permanece central para a tradição da pesquisa liberal. A interação econômica funcionaria para familiarizar as nações umas com as outras e reduzir os male-entendimentos que poderão levar a conflitos. O comércio não apenas produz riqueza, mas também reduz o conflito, promovendo a compreensão e revelando a harmonia de interesses entre todas as nações. Assim, podemos perceber que a democracia, a interdependência e as instituições internacionais reduzem o conflito. Além disso, estes três pilares da paz liberal estão entrelaçados. Assim, para conseguir atingir segurança, é necessário ter um equilíbrio entre esses pilares.[43]

A abordagem clássica da Escola Inglesa envolve ver as Relações Internacionais compostas de três elementos, de sistema internacional, interligado com o realismo Hobbesiano, de sociedade internacional conectado com o racionalismo e de sociedade mundial conectado com o idealismo Kanteano. Esses elementos estão em constante interação e a natureza das relações internacionais depende do equilíbrio entre elas. Em princípio, isto abre uma ponte entre a Escola Inglesa e os Estudos Internacionais de Segurança através do elemento de realismo da teoria da Escola Inglesa. Assim, o núcleo tradicional da escola está intimamente relacionado ao realismo, cuja compreensão é centrada no Estado, poder político e conflitual das Relações Internacionais, que fornece uma estrutura geral complementar e próxima para estudos estratégicos.[44]

---

[42] WILLIAMS, D. Paul. **Security Studies - An Introduction.** New York: Routledge, 2008p. 20
[43] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies.** New York: Routledge, 2010. p. 29
[44] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010. p. 35

A vida dentro de uma sociedade política internacional de poder será extremamente diferente da vida em uma cooperativa ou convergência. Também está claro que essas sociedades internacionais representam formas de ordem social bastante distintas do senso de ordem materialista representado pela distribuição de poder no realismo. Em certo sentido, as suposições realistas estão confinadas dentro dos modelos políticos de poder e de coexistência, e prestam atenção apenas a algumas das instituições que definem esses modelos. Assim, existem múltiplas conexões entre a Escola Inglesa e os estudos de Segurança, que sem dúvida ajuda bastante a manter a segurança entre estados.[45]

A securitização examina predominantemente como os problemas de segurança emergem, evoluem e se dissolvem. A teoria da securitização argumenta que a linguagem não está apenas preocupada com o que está fora, como os realistas e os neorrealistas assumem, mas também é constitutiva dessa mesma realidade social. A securitização é uma concepção de segurança orientada pelo processo, que contrasta com as abordagens materialistas dos estudos clássicos de segurança. As abordagens clássicas de segurança enfocam as disposições materiais da ameaça, incluindo a distribuição de poder, capacidades militares e polaridade, enquanto a securitização examina como uma determinada questão é transformada por um agente em uma questão de segurança, a fim de permitir o uso de medidas extraordinárias. Além disso, o ato de securitização, para ser bem-sucedido, deve ser aceito pelo público, até se o assunto não é considerado uma ameaça verdadeira.

Todos os atos de securitização envolvem quatro componentes chaves. É necessário ter um *agente de securitização*, ou seja, uma entidade que faz o movimento ou a instrução de securitização; Uma *ameaça existenci*al, que seja um objeto ou ideal que foi identificado como potencialmente prejudicial; Um *objeto de referência*, ou seja, um objeto que está sendo ameaçado e precisa ser protegido; Uma *audiência*, que é o alvo do ato de securitização que precisa ser persuadido e aceitar o problema como uma ameaça à segurança. O fato de um determinado sujeito ser securitizado não significa necessariamente que o sujeito é de essência objetiva para a sobrevivência de um determinado estado, mas significa apenas que alguém construiu com sucesso algo, como um problema existencial. A capacidade de efetivamente securitizar um determinado assunto é, no entanto, altamente dependente tanto do *status* de um determinado ator quanto se problemas

[45] Idem, p. 36, 56.

semelhantes são geralmente percebidos como ameaças à segurança. Depois disso, pode ser declarando estado de emergência ou lei marcial, mobilizando os militares ou atacando outro país.[46]

A Teoria de Jogo também tem conexões significativas com os estudos de segurança. O conceito básico é o de um jogo em si. Um jogo pode ser considerado uma situação qualquer na qual um resultado depende das escolhas de dois ou mais tomadores de decisão. Na teoria dos jogos, os tomadores de decisão são chamados de jogadores, que podem ser indivíduos ou grupos de indivíduos que, de alguma forma, operam como uma unidade coerente. Presidentes, primeiros-ministros, reis e rainhas, ditadores, secretários estrangeiros e assim por diante, podem, por vezes, ser considerados como jogadores em um jogo. Os estados também são considerados jogadores, os quais podem tomar decisões na política externa. É até possível considerar uma coalizão de dois ou mais estados como um jogador.[47]

As decisões que os jogadores tomam, levam a um resultado específico. Na teoria dos jogos, um resultado pode ser praticamente qualquer consequência da decisão. Assim, o conteúdo empírico associado a um resultado irá variar com o jogo que está sendo analisado, mas geralmente acontecem compromissos ou conflitos. Pode acontecer, também, um jogo de soma diferente de zero, que é uma situação interativa na qual os jogadores têm motivos mistos, isto é, além de interesses conflitantes, eles também podem ter alguns interesses em comum. Dois estados presos em um conflito econômico, por exemplo, vão ter interesse em garantir os melhores termos de troca possíveis.[48]

Entre as áreas temáticas de estudos de segurança que foram fortemente influenciadas pelo raciocínio de Teoria de Jogo estão, o início e a escalada de conflitos e guerras interestaduais, as consequências de alianças e padrões de alinhamento, a eficácia dos sistemas de defesa antimísseis e o impacto da política interna, conflitos interestaduais, a dinâmica das corridas armamentistas e o funcionamento do controle de armas, a disseminação do terrorismo, os perigos da proliferação nuclear, as implicações da democratização para a diplomacia coercitiva, as características da negociação de crises e o funcionamento da política de equilíbrio de poder. Assim podemos

[46] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010., p. 56

[47] WILLIAMS, D. Paul. **Security Studies - An Introduction**. New York: Routledge, 2008, p. 45.

[48] MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies.** New York: Routledge, 2010, p. 56.

perceber, que a literatura de Estudo de Segurança, se baseia ou foi influenciada pelo raciocínio de teoria de jogo amplamente, e essa teoria veio a ser uma parte de segurança.[49]

Com tudo isso podemos ver que todas as teorias das Relações Internacionais contribuíram em sua parte para os Estudos de Segurança. Cada uma delas tem uma parte muito importante no raciocínio do estudo. Além disso, não seria possível atingir uma segurança no mundo virtual sem a aplicação dessas teorias, pois elas também atuam no Ciberespaço e ajudam a tomar decisões corretas de modo mais efetivo para garantir a segurança e futuro desenvolvimento.

[49] WILLIAMS, D. Paul. **Security Studies - An Introduction**. New York: Routledge, 2008. p. 53.

4 SEGURANÇA CIBERNÉTICA NO MUNDO: ESTADOS UNIDOS, RÚSSIA, ISRAEL E BRASIL

Um dos assuntos mais importantes no mundo, no momento são os cibernéticos. Muitos países já começaram a aumentar o seu envolvimento neste assunto. A base dessa pesquisa não é comparar os países em questão, mas mostrar as estratégias nacionais de cada um. Foram escolhidos Estados Unidos e Rússia, como países lideres na área cibernética, e o Israel e Brasil, como novos países na área de Segurança Cibernética, que ainda estão desenvolvendo a estratégia de atuação nessa área. Além disso, Brasil é o terceiro país que mais recebe ataques cibernéticos, conforme o relatório global de Symantec. Por novas ameaças sempre estarem surgindo, é muito importante desenvolver as estratégias de atuação na área Segurança Cibernética.

4.1 Estados Unidos

O Ministério de Defesa dos Estados Unidos da América criou um órgão especial para trabalhar com os assuntos cibernéticos, chamado de Comando Cibernético dos EUA, o USCYBERCOM. A missão deles é dirigir, sincronizar e coordenar o planejamento e as operações do ciberespaço para defender e promover os interesses nacionais em colaboração com parceiros nacionais e internacionais. A superioridade militar nos domínios aéreo, terrestre, marítimo e espacial é fundamental para a capacidade de defender os interesses e proteger os valores dos EUA. A conquista de superioridade no domínio físico é, em grande parte, dependente do Ciberespaço. Depois da criação do Ciber Comando, o Ciberespaço evoluiu muito e começaram a surgir novas ameaças. A partir desse momento, os adversários dos EUA exploraram a velocidade e o volume de dados e eventos no ciberespaço para tornar o domínio mais hostil. Eles aumentaram as apostas para a nação e os seus aliados. Para melhorar a segurança e a estabilidade, eles começaram a trabalhar numa abordagem nova.[50]

A missão do comando é parar os ataques antes que eles penetrem as defesas cibernéticas ou prejudiquem as forças militares. Através de operações persistentes e integradas, eles conseguem influenciar o comportamento do adversário e introduzir incerteza em seus cálculos. Efeitos estratégicos superiores dependem do alinhamento de operações, capacidades e processos, e a

[50] US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM).

integração perfeita de inteligência com operações. Como um Comando Unificado de Combatentes, eles devem demonstrar a resolução deles contra as ameaças do ciberespaço e unificar as operações neste âmbito, com o objetivo de proteger redes, plataformas e dados. Com tudo isso, eles vão expandir as opções militares disponíveis para líderes nacionais e comandantes operacionais.[51]

Os avanços tecnológicos das duas últimas décadas, comparáveis em termos de abalo mundial àqueles que ocorreram há dois séculos, coincidiram com um novo momento de instabilidade política global após da Guerra Fria. No entanto, a maioria das forças armadas está entrando nesta era com o padrão familiar de crença de que novas ferramentas tecnológicas irão simplesmente reforçar as práticas existentes.[52]

Quando as forças armadas não acompanham o ritmo das mudanças, os países sofrem. Na Primeira Guerra Mundial, o fracasso em compreender as implicações da produção em massa levou não apenas ao massacre sem sentido, mas também ao fim dos grandes impérios e à falência de outros. A incapacidade de compreender o significado da mecanização no início da Segunda Guerra Mundial entregou vastas extensões de território às potências do Eixo e quase lhes deu a vitória. O fracasso em entender o verdadeiro significado das armas nucleares levou a uma corrida armamentista suicida e a um apocalipse mal evitado durante a crise dos mísseis de Cuba. Assim, com o avanço da tecnologia, os países têm que se conformar e evoluir também.[53]

O maior problema que os militares tradicionais enfrentam hoje é que eles estão organizados para travar grandes guerras e têm dificuldade em se orientar para lutar contra os pequenos. Às vezes, as pequenas ameaças podem ser mais importantes, principalmente no Ciberespaço. Por isso, é necessário estar preparado para qualquer ameaça, seja de larga escala ou pequena. Cada era de mudança tecnológica resultou em profundas mudanças nos assuntos militares e estratégicos. A história nos diz que esses desenvolvimentos eram inevitáveis, mas soldados e estadistas quase sempre eram muito atrasados para abraçá-los, por isso tragédias aconteciam.[54]

A Agência de Segurança Nacional é a agência responsável por todas as questões que afetam a segurança cibernética do governo dos Estados Unidos da América. A NSA integra a estrutura do Departamento de Defesa, que é equivalente ao Ministério da Defesa brasileiro. Ao contrário da CIA e da Agência de Inteligência de Defesa, ambas especializadas principalmente em espionagem

[51] US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM).
[52] ARQUILLA, John. **The New Rules of War**. In: Foreign Policy, 02 nov. 2010, p. 3
[53] US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM).
[54] ARQUILLA, John. **The New Rules of War**. In: Foreign Policy, 02 nov. 2010, p. 16

estrangeira, a NSA não realiza publicamente uma reunião de inteligência de origem humana. A agência tem uma organização co-localizada chamada Serviço Central de Segurança, que facilita a cooperação entre a NSA e outros componentes da criptoanálise de defesa dos EUA. A missão de espionagem da NSA inclui a transmissão de rádio, tanto de várias organizações e indivíduos, como também, a Internet, telefonemas e outras formas de comunicação interceptadas.[55]

A espionagem reportada pela Agência de Segurança Nacional dos EUA sobre os líderes mundiais é um momento rico de aprendizado, pois mostra a parte inferior das relações internacionais. Espionar outros governos, incluindo os amigos, é um pilar da política externa moderna e uma ferramenta vital para proteger contra ameaças modernas à segurança, como crime internacional, terrorismo, ciberataques, tráfico de drogas, mudança climática e roubo de tecnologia. A história nos mostra que a espionagem tem sido uma parte crucial da política de segurança dos EUA por décadas, mas até mesmo as brigas mais sensíveis entre amigos podem ser resolvidas com diplomacia cuidadosa. Depois que a Colômbia se reuniu com os EUA para discutir as revelações de Snowden sobre supostas informações, os interesses de ambos os lados pareciam satisfeitos.[56]

A revolução da tecnologia da informação tornou o mundo menor e mais penetrável. A privacidade pessoal é mais difícil de manter, especialmente quando até mesmo os amigos não sentem a compulsão de agir de forma amigável quando a segurança é considerada um jogo. Pode-se argumentar que as revelações sobre a espionagem de seus líderes nacionais ofereceram uma lição construtiva para as agências de segurança do Brasil e da Alemanha, que devem tomar medidas imediatas para reduzir suas vulnerabilidades. Ou os funcionários eram muito descuidados ao lidar com comunicações seguras, ou a tecnologia deles não era tão sofisticada quanto precisa ser no mundo atual de alta tecnologia. Mas a lição mais importante desses episódios é uma antiga, que se você for espionar, não seja pego.[57]

O caso do Brasil é mais preocupante porque o relacionamento oficial não é tão próximo. Muitos na liderança atual do Brasil não veem os EUA como amigos, enquanto muitos funcionários dos EUA vêem nas políticas do Brasil uma abordagem ultrapassada de soma zero para a geopolítica

---

[55] CRUZ JÚNIOR, Samuel César da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual.** Texto para discussão. Brasília : Rio de Janeiro : Ipea, 2013. p. 15

[56] MARCELLA, Gabriel; MCILHENNY, William. **Hard Talk Forum**. In: Americas Quarterly, 8 jan. 2014.

[57] US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM).

que dificulta a colaboração. Essas percepções já representavam barreiras que precisavam ser superadas e as revelações da espionagem não ajudavam nessa situação.[58]

Durante o mandato da Presidente Dilma Rousseff, houve alguns conflitos com os EUA. A causa fundamental da relação tensa é que Washington se recusava a reconhecer que havia uma nova realidade na região, já que uma grande maioria sul-americana elegeu governos de esquerda. No estabelecimento de política externa de Washington, incluindo a maioria das fontes de análise e opinião, quase não houve reconhecimento de que uma nova estratégia poderia ser necessária. O Brasil é o maior alvo de espionagem do NSA, mas na última década do governo do Partido dos Trabalhadores, o Brasil tem se alinhado de maneira justa e consistente com os outros governos de esquerda em questões hemisféricas e relações com os Estados Unidos.[59]

A segurança dos Estados Unidos e dos aliados depende em grande parte da estabilidade internacional e da prosperidade global. A disseminação da tecnologia e das comunicações permitiu novos meios de influência e coerção. Os adversários deles continuam a expandir a sua influência ainda mais no Ciberespaço, sem nenhuma agressão física. Os Estados Unidos sempre tinham um alto limiar para resposta à atividade adversária. Os inimigos usam essa percepção para explorar as dependências e vulnerabilidades no ciberespaço e usam os sistema, processos e valores contra eles mesmos, para enfraquecer as instituições democráticas dos EUA e obter vantagens econômicas, diplomáticas e militares. Os Estados possuem recursos e paciência para sustentar campanhas cibernéticas sofisticadas para penetrar em redes bem protegidas, manipular *software*, computadores, sistemas, dados e também, destruí-os. Exatamente para este fim o Comando Cibernético deve estar um passo à frente e saber como navegar no Ciberespaço eficientemente.[60]

Atores não-estatais agressivos, como terroristas, criminosos e hacktivistas, ou seja, Grupos de *Hackers*, representam ameaças menores do que os Estados, mas ainda podem prejudicar as capacidades militares e infraestrutura crítica dos EUA, além de ameaçar vidas dos civis. O Estado Islâmico do Iraque, a Al Qaeda da Síria, e os grupos afiliados estão desestabilizando regiões inteiras, atacando os interesses globais dos Estados Unidos e colocando em risco os cidadãos no mundo todo. Esses grupos usam o ciberespaço para promover sua ideologia, inspirar seguidores e controlar operações que ameaçam o mundo inteiro. Os grupos criminosos organizados fornecem cobertura para estados e terroristas e possuem capacidades significativas para roubar dados e

[58] MARCELLA, Gabriel; MCILHENNY, William. **Hard Talk Forum**. In: Americas Quarterly, 8 jan. 2014.
[59] WEISBROT, Mark. **Washington and São Paulo:** Spying and a Fading Friendship. In: NACLA Report on the Americas, 2013.
[60] US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM).

interromper funções do governo. Os hacktivistas trabalham para expor informações confidenciais ou prejudicar os serviços do governo. Esses atores cibernéticos maliciosos frequentemente apresentam ameaças que a aplicação da lei e os meios diplomáticos não podem conter sem assistência militar. Novas vulnerabilidades e oportunidades surgem continuamente à medida que novos terrenos emergem no Ciberespaço. Nenhum alvo permanece estático, nenhuma capacidade ofensiva ou defensiva permanece efetiva e nenhuma vantagem é permanente. Um terreno cibernético bem defendido é atingível, mas continuamente em risco por causa da contínua evolução do Internet, demandando ter agilidade no Ciberespaço para estar um passo à frente dos inimigos.[61]

Um exemplo de desafio da segurança que aconteceu nos EUA é o ataque de *hackers* russos do Comitê Nacional Democrata. O evento constitui um exemplo clássico de uma falha de aviso. Tais fracassos, como atestam as ricas publicações sobre Pearl Harbor, a Guerra da Coréia, a Guerra Israelense Árabe de 1973 e os ataques terroristas do 11 de setembro, não são produto de informações insuficientes sobre a ameaça iminente. Pelo contrário, eles são o resultado da interpretação equivocada da informação disponível. A resposta dos EUA ao ataque foi moldada por uma série de sinais perdidos, respostas lentas e uma subestimativa contínua da seriedade do ataque cibernético. Embora os meios de ataques surpresa tenham mudado de aviões e tanques para contas de e-mail e redes de computadores, a dinâmica entre o iniciador do ataque e sua vítima permaneceu praticamente a mesma.[62]

Pouco era conhecido sobre o ataque, mas é possível fazer algumas observações sobre este evento. Na era da guerra convencional, as agências de inteligência foram encarregadas de responder sobre o “se”, “como”, “onde” e “quando” do ataque, mas nesse caso, a identidade do invasor em potencial era conhecida. No entanto, embora muito tenha sido escrito sobre as dificuldades envolvidas na atribuição de ataques específicos a estados específicos na era da guerra cibernética, isso não foi um problema no presente caso. O FBI já sabia que o grupo russo de espionagem cibernético conhecido como "os duques" estava hackeando os computadores do Comitê Nacional Democrata e já era conhecido que eles trabalhavam para o Serviço Federal de Segurança da Federação Russa.[63]

---

[61] US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM).

[62] BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare**. In: Rar on the Rocks, 3 jan. 2017. p. 1

[63] BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare**. In: Rar on the Rocks, 3 jan. 2017. p. 1

A administração acabou decidindo por uma meia-medida atrasada, ou seja, uma advertência ao Kremlin uma semana antes da eleição pelo telefone vermelho destinado a crises nucleares. Funcionários do governo alegaram que a advertência de Obama a Putin incluía uma observação de que a lei do conflito armado se aplicava ao ciberespaço e que a Rússia seria mantida nesse padrão. Esse aviso pode ter impedido a interferência russa no próprio dia das eleições, mas não parece ter conseguido mais nada.[64]

Isso nos mostra que na era da guerra cibernética, os vírus são armas e os *firewalls* meios de defesa. Assim, as lições reais que a história tem para ensinar podem ser contra intuitivas. Enquanto os Estados Unidos sempre contaram com a advertência estratégica obtida através de meios técnicos de coleta, essa forma de coleta de inteligência foi repetidamente revelada como fútil. Assim, a ascensão da era do conflito cibernético não evita o imperativo de fontes humanas bem colocadas.[65]

As operações do ciberespaço dos EUA podem fazer contribuições positivas para o poder diplomático, proporcionando sanções rápidas, temporárias e reversíveis ou comunicando discretamente ao adversário. As capacidades do ciberespaço são fundamentais para identificar e interromper as operações de informações dos adversários deles. O Comando Cibernético não espera até que um adversário esteja dentro das redes ou sistemas deles para agir com respostas unificadas entre as agências, independentemente do setor ou da geografia. O Departamento de Defesa dos Estados Unidos está construindo a expertise operacional e a capacidade para atender aos crescentes ameaças do ciberespaço e interromper a ciber-agressão antes que esta atinja as redes e sistemas. Por meio da ação persistente e da competição mais efetiva abaixo do nível do conflito armado, eles influenciam os cálculos dos adversários, impedem a agressão e esclarecem a distinção entre comportamento aceitável e inaceitável no ciberespaço. O objetivo final do Ciber Comando dos EUA é melhorar a segurança e estabilidade do ciberespaço, bem como também proteger os valores nacionais do país.[66]

O Ciber Comando tem cinco missões principais: a) antecipar e identificar mudanças tecnológicas e explorar e operacionalizar tecnologias emergentes e inovações destrutivas de forma mais rápida e eficaz, ou seja, mais rápido que os adversários; b) desenvolver vantagens na preparação e durante operações conjuntas em conflito, bem como abaixo do limiar de conflito

---

[64] WEISBROT, Mark. **Washington and São Paulo: Spying and a Fading Friendship**. In: NACLA Report on the Americas, 2013

[65] BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare**. In: Rar on the Rocks, 3 jan. 2017. p. 2

[66] US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM).

armado; c) melhorar as opções de guerra de informação para os comandantes da Força Conjunta, como também integrar as operações do ciberespaço com as operações de informação, e unificar e direcionar inteligência para apoiar as operações no ciberespaço e as operações de informação; d) facilitar a velocidade e a agilidade das operações do ciberespaço na orientação política, nos processos de tomada de decisão, nos investimentos e nos conceitos operacionais. Alavancar os talentos, conhecimentos e produtos do setor privado, outras agências, serviços, aliados e academia; e) identificar rapidamente e compreender os avanços no ciberespaço onde quer que eles se originem e residam. Assim, o USCYBERCOM contribuirá para a dissuasão estratégica nacional, preparando, operações e colaboração com comandos, serviços, departamentos, aliados e indústrias combatentes para continuamente impedir e contestar os atores hostis do ciberespaço onde quer que sejam encontrados. Com isso eles vão atrair novos parceiros e fortalecer os laços com parceiros de missões críticas já existentes.

4.2 Rússia

A Internet e outros componentes do ciberespaço estabeleceram-se como um fator central no desenvolvimento econômico e na modernização da Rússia. A introdução das tecnologias da informação e comunicação nos processos de administração pública é a base para a construção de um Estado democrático eficaz e socialmente responsável no século XXI. Neste contexto, é necessária uma política estatal direcionada e sistemática para desenvolver o setor nacional de tecnologia da informação. A natureza transfronteiriça do ciberespaço, sua dependência de tecnologias de informação complexas e o uso ativo de sites e serviços ciberespaciais por todos os grupos de cidadãos russos definem novas oportunidades, mas ao mesmo tempo desenvolvem novas ameaças para danificar os direitos, interesses e meios de subsistência de um indivíduo, organização, órgãos estatais, para realizar ataques cibernéticos contra recursos de informações protegidos e para uso de armas cibernéticas em operações especiais e guerra cibernética, incluindo aquelas que acompanham as hostilidades tradicionais. Para combater essas ameaças, foi criada a Estratégia de Segurança Cibernética do Conselho da Federação Russa.[67]

Atualmente, a Federação Russa adotou uma série de documentos destinados a assegurar vários aspectos da segurança da informação nacional. Entre eles, a Doutrina de Segurança da

[67] COUNCIL OF THE RUSSIAN FEDERATION. Site Oficial do Conselho da Federação da Rússia. O Conceito da Estratégia de Segurança Cibernética da Federação Russa, 2014.

Informação da Federação Russa, a Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa. Mas o regulamento existente não abrange, na medida do necessário, o sistema de relações que surge no âmbito do ciberespaço, que é muito mais amplo e avançado para os documentos existentes. Para a estratégia ter sucesso é necessário ter uma identificação clara da gama de problemas que serão resolvidos como parte do trabalho nas áreas identificadas na Estratégia, por isso o ciberespaço deve ser considerado como um determinado elemento do espaço da informação com limites claros, se baseando nos padrões internacionais.

A estratégia deve basear-se em três conceitos principais. Primeiro, no espaço de informação, que é um campo de atividade relacionado à formação, criação, transformação, transferência, ao uso e armazenamento de informações que têm impacto na consciência individual e pública. Segundo, na segurança da informação, que é o estado de proteção de um indivíduo, organização e estado, seus interesses de ameaças destrutivos e outros impactos negativos no Ciberespaço. Terceiro, deve basear-se na Segurança Cibernética efetiva, que é um conjunto de condições sob as quais todos os componentes do ciberespaço são protegidos de quaisquer ameaças, impactos e ataques com meios mais eficazes possíveis.

Um exemplo de ataques cibernéticos da Rússia é o que aconteceu contra a Estônia em 2007. Uma onda de três semanas de ataques cibernéticos maciços ao pequeno país báltico da Estônia é a primeira incidência conhecida de tal ataque a um Estado, que causou alarme em toda a aliança ocidental, com a OTAN examinando com urgência a ofensiva e suas implicações. Enquanto a Rússia e a Estônia estavam envolvidas em sua pior disputa desde o colapso da União Soviética, por causa de uma discussão que surgiu sobre a remoção do Memorial de bronze do Soldado de Guerra soviético em Tallinn, o país foi submetido a uma barragem de guerra cibernética, desativando os sites de ministérios do governo, partidos políticos, jornais, bancos e empresas. A OTAN enviou alguns de seus maiores especialistas em terrorismo cibernético para Tallinn para investigar e ajudar os estonianos a reforçar suas defesas eletrônicas.[68]

As relações entre o Kremlin e o Ocidente tornaram-se piores há anos, pois a Rússia estava se empenhando em amargas disputas não só com a Estônia, mas com a Polônia, Lituânia, República Tcheca e Geórgia, ou seja, todas as antigas partes da União Soviética ou ex-membros do Pacto de Varsóvia. A ofensiva eletrônica piorou as relações entre os países. Com sua reputação de proeza eletrônica, os estonianos foram rápidos em organizar suas defesas, principalmente fechando os sites

[68] TRAYNOR, Ian. **Russia accused of unleashing cyberwar to disable Estonia**. In: The Guardian Brussels, 17 maio 2007.

e endereços de internet sob o ataque estrangeiro, a fim de tentar mantê-los acessíveis aos usuários domésticos. Os ataques cibernéticos foram claramente motivados pela relocação do memorial soviético da Segunda Guerra Mundial pelos Estonianos.[69]

A crise desencadeou uma onda dos ataques de DDoS. Os ataques chegaram de todo o mundo, mas autoridades estonianas e especialistas em segurança de computadores dizem que, particularmente na fase inicial, alguns invasores foram identificados por seus endereços na internet, alguns dos quais eram de origem russa e até instituições estatais russas foram detectadas. Os funcionários da OTAN, familiarizados com o trabalho dos especialistas, disseram que era fácil para eles, com outras organizações e provedores de internet, rastrear e identificar os invasores. Assim, a OTAN ajudou muito a Estônia para contornar esta situação.

Para conseguir responder os ataques cibernéticos, a Aliança Mundial de Tecnologia da Informação e Serviços começou a funcionar mais ativamente. Ela é um consórcio de associações da indústria de tecnologia da informação e comunicações em todo o mundo. O vigésimo terceiro Congresso dessa associação vai acontecer na cidade Yerevan, que é o capital da Armênia, em outubro de 2019. O assunto desse encontro será, "Cumprindo a Promessa da Era Digital - O Poder da Descentralização", que é muito importante para o futuro da Segurança Cibernética também.[70]

A Estratégia de Segurança da Federação Russa tem quatro missões importantes. Primeira, é eliminar as lacunas existentes na regulamentação da segurança cibernética da Federação Russa. Segunda, é criar motivos para a inclusão das estruturas civis e organizações empresariais no grupo dos atores e órgãos estatais que trabalham para garantir a segurança cibernética da Federação Russa. Terceira, é sistematizar as ações de todas as partes interessadas, a fim de aumentar o nível de segurança cibernética do país. E a quarta missão, é formular um modelo de ameaças à segurança cibernética para a Federação Russa, bem como orientações e medidas para combatê-las, ou seja, fazer simulações de ataques e contra-ataques. Uma das tarefas centrais no campo da Segurança Cibernética é o desenvolvimento de critérios e métodos para avaliar a eficácia dos sistemas de defesa e meios de garantir a segurança da informação.[71]

---

[69] BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare**. In: Rar on the Rocks, 3 jan. 2017

[70] COUNCIL OF THE RUSSIAN FEDERATION. Site Oficial do Conselho da Federação da Rússia. **O Conceito da Estratégia de Segurança Cibernética da Federação Russa**, 2014.

[71] COUNCIL OF THE RUSSIAN FEDERATION. Site Oficial do Conselho da Federação da Rússia. **O Conceito da Estratégia de Segurança Cibernética da Federação Russa**, 2014.

Os princípios básicos da estratégia são muito importantes, sendo elas o princípio da garantia dos direitos e liberdades constitucionais de um cidadão no domínio da obtenção e utilização da informação. O *princípio da máxima proteção* do indivíduo ou organização inclui aquelas que asseguram o funcionamento da infraestrutura de informação crítica, agências governamentais em termos de operação de recursos de informação, de redes e de telecomunicações no ciberespaço. O *princípio da cooperação construtiva* de todos os sujeitos da sociedade da informação, ou seja, dos indivíduos, das organizações e do Estado para garantir segurança cibernética. O *princípio do equilíbrio* entre a determinação da responsabilidade e da Segurança Cibernética tem diferentes restrições. E o *princípio de priorização dos riscos* de segurança cibernética de acordo com a probabilidade de ameaças cibernéticas.[72]

A Federação Russa criará um grupo de trabalho para o desenvolvimento da Estratégia de Segurança Cibernética, com a participação de representantes do Conselho de Segurança da Federação Russa, que é o órgão executivo federal autorizado no campo da segurança. Contará também com a ajuda dos órgãos estaduais de supervisão e controle, empresas comerciais, empresas com participação estatal e organizações estatais. O grupo especializado de trabalho garante o desenvolvimento da Estratégia de acordo com os padrões internacionais, que é posteriormente aprovado por um ato regulamentar do Governo da Federação Russa. A estratégia foi criada por causa da crescente ameaça no Ciberespaço e para o meio de proteção da sociedade russa e do país. No momento o conceito de Segurança Cibernética não está sendo usada nos documentos oficiais da Federação Russa, mas a Estratégia vai colocar este conceito como principal, nos assuntos que envolvem a defesa do Ciberespaço.[73]

4.3 Israel

O governo de Israel estabeleceu uma visão para que Israel seja uma nação líder no aproveitamento do ciberespaço como um motor de crescimento econômico, bem-estar social e segurança nacional. A estratégia nacional de segurança cibernética de Israel é, em primeiro lugar, um meio de concretizar a visão cibernética de Israel, mantendo o ciberespaço seguro e confrontando as várias ameaças cibernéticas, de acordo com os interesses nacionais do país. Além

[72] BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare**. In: Rar on the Rocks, 3 jan. 2017
[73] Idem.

disso, a estratégia visa garantir a continuidade do papel de Israel na arena internacional, como líder em inovação tecnológica e como parceiro ativo nos processos globais de formação do ciberespaço. A estratégia nacional de segurança cibernética é a base conceitual e prática para alcançar esses objetivos.[74]

O primeiro marco no desenvolvimento dos esforços nacionais de segurança cibernética de Israel foi estabelecido em 2002, quando o governo israelense autorizou a Autoridade Nacional de Segurança da Informação (NISA) a instruir e proteger sistemas computadorizados vitais de organizações civis públicas e privadas selecionadas. O próximo e principal marco foi o estabelecimento, em janeiro de 2012, do Serviço Nacional de Cibersegurança de Israel (INCB) subordinado diretamente ao Primeiro Ministro, após uma resolução governamental de agosto de 2011. O INCB foi encarregado de elaborar a política nacional e estratégia do Estado, promovendo os processos nacionais, desenvolvendo capacidades cibernéticas nacionais e fortalecendo a liderança de Israel no campo. A estratégia de segurança cibernética de Israel é baseada em um conceito genérico de operações para segurança cibernética nacional, ou seja, uma estrutura conceitual para todos os esforços e funções do estado no contexto da segurança cibernética nacional. Essa estrutura inclui ações diretas do Estado para enfrentar ameaças cibernéticas e esforços indiretos que visam incentivar e apoiar atividades de segurança no setor privado e colaborar com ele.[75]

O conceito de operações define três camadas operacionais: Robustez Cibernética Agregada, Resiliência Cibernética Sistêmica e Defesa Cibernética Nacional. A abordagem de três camadas deriva da natureza única da ameaça cibernética e do papel central das organizações privadas na obtenção da segurança cibernética nacional. As três camadas diferem uma da outra em seus objetivos, no papel do Estado e nas relações entre o Estado e as organizações privadas. A primeira camada, robustez cibernética é a capacidade das organizações e processos para continuar operando, apesar de uma rotina de ameaças cibernéticas, repelindo e impedindo a maioria dos ataques. Este é o nível muito básico de segurança cibernética.[76]

O Estado de Israel estabeleceu uma meta para elevar o nível geral de robustez cibernética como um meio de evitar danos de alto nível e reduzir o risco cumulativo. A segunda camada no

[74] ISRAEL. Prime Minister's Office. National Cyber Directorate. **Israel National Cyber Security Strategy In Brief**. Set. 2017
[75] BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare**. In: Rar on the Rocks, 3 jan. 2017
[76] ISRAEL. Prime Minister's Office. National Cyber Directorate. **Israel National Cyber Security Strategy In Brief**. Set. 2017

conceito de operações é a capacidade sistemática de confrontar ataques cibernéticos antes, durante e depois de incidentes, impedindo-os de se espalhar e reduzir seus danos cumulativos à nação. Enquanto a primeira camada é focada na redução de ataques a priori, independentemente de qualquer evento específico, essa camada é orientada por eventos por definição. A resiliência sistêmica pode ser alcançada por meio de processos estatais que incentivam o compartilhamento de informações, geram e disseminam informações valiosas e auxiliam as organizações durante incidentes cibernéticos.

A terceira camada se baseia numa campanha de nível nacional, que é necessária contra ameaças severas, realizadas pelos atacantes determinados e ricos em recursos, que representam um grave perigo para a nação. As campanhas nacionais de defesa incorporam esforços defensivos para conter tais ataques e suas ramificações, juntamente com esforços ativos para confrontar as fontes das ameaças. Assim, podemos perceber que a abordagem de três camadas de Israel, oferece uma solução totalizante, levando em conta as diferenças no nível de risco, a natureza da ameaça e o grau de clareza.[77]

Autoridade Nacional de Segurança Cibernética (NCSA), é uma agência operacional, com a segurança cibernética como sua única preocupação, mas é uma instituição civil em sua natureza, cooperando principalmente e abertamente com o setor privado. O NCSA serve como um centro de conhecimento nacional, um principal regulador cibernético e um centro operacional para o gerenciamento de incidentes cibernéticos. Para a garantia de segurança cibernética, o Governo do Israel criou o *National Cyber Bureau*, que tem duas missões principais: a) pesquisa, desenvolvimento e implementação de capacidades e tecnologias de segurança em nível nacional, incluindo plataformas de compartilhamento de informações seguras e eficientes; b) fortalecer a base nacional de ciência e tecnologia no ciberespaço, ou seja, promover a inovação industrial, apoiar a pesquisa acadêmica, aumentar o capital humano do país no campo cibernético e fomentar um ecossistema para enriquecimento mútuo.[78]

Assim, o ciberespaço é uma esfera global e a segurança cibernética é um desafio global. O Estado de Israel vê a cooperação internacional como um elemento crítico para estabelecer o ciberespaço como uma esfera de atividade segura, livre e global, bem como um componente complementar em seus próprios esforços nacionais de segurança cibernética.

---

[77] BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare**. In: Rar on the Rocks, 3 jan. 2017

[78] ISRAEL. Prime Minister's Office. National Cyber Directorate. **Israel National Cyber Security Strategy In Brief**. Set. 2017

O principal objetivo de uma estratégia nacional de defesa cibernética do Governo do Israel é manter a continuidade funcional do estado. Um segundo objetivo é permitir que as autoridades israelenses competentes decidam e implementem operações contra inimigos no espaço cibernético e cinético, com confiança na capacidade do Estado de resistir a um ataque cibernético. Na estratégia de defesa, existem três diferentes tipos de ataques. Primeiro tipo, é a ameaça persistente avançada (APT), onde ocorre a penetração na profundidade do sistema de computador de uma organização e uso ou criptografia dos dados do sistema. O segundo tipo, é um ataque rápido e superficial, que tem resultados imediatamente reconhecíveis e visa alterar o site ou impedir o acesso a ele e aos serviços que ele fornece no espaço cibernético, um exemplo disso é o ataque de DDoS. O terceiro tipo é um ataque à infraestrutura, que danifica componentes de *hardware*, causando danos irreparáveis e até perda de dados.[79]

Para combater esses tipos de ataque é possível tomar as seguintes ações:

- Construir o sistema com uma combinação de ferramentas e recursos que não exijam informações e conhecimentos prévios de componentes e métodos de ataque, com um sistema de recursos avançados baseado em conhecimento anterior, especificamente para defesa contra-ataques de APT.
- Implementar a troca de informações interorganizacionais de relatórios sobre ataques. Formular uma avaliação nacional contínua e ampla do status cibernético por organizações como a Equipe Nacional de Resposta a Emergências de Computadores (CERT).
- Estabelecer equipes de resposta rápida, usando pesquisas e dados sobre ferramentas de ataque e grupos de ataque. Cooperar com organizações comerciais de defesa e inteligência, como também, com organismos internacionais.[80]

Assim, podemos perceber que a segurança cibernética de Israel recai em vários ministérios do governo e organizações do setor privado. A continuidade funcional de Israel tornou-se ainda mais dependente da tecnologia em geral e da atividade no ciberespaço em particular. As missões principais do país são desenvolver uma nova abordagem para a segurança cibernética, iniciando um tipo de cooperação sem precedentes entre o governo e o setor privado e dedicar esforços nacionais para melhorar a preparação cibernética e mitigar as consequências de incidentes ou

[79] SIBONI, Gabi; ASSAF, Ofer. **Guidelines for a National Cyber Strategy**. Tel Aviv: Institute for National Security Studies, 2016.
[80] Idem.

ataques. Assim, vendo a segurança cibernética como um mecanismo de crescimento econômico, o governo a identificou como um setor onde Israel tem uma vantagem competitiva baseada em pesquisa de ponta e experiência prática única.

4.4 Brasil

Atualmente o Brasil é a sexta maior economia do mundo, onde gigantescos campos petrolíferos ultra profundos foram descobertos nos últimos anos. O Brasil está novo na área de segurança cibernética e, no momento, não tem a capacidade necessária de entrar nesse quadro e competir com países como Estados Unidos. Mas a área está em pesquisa pelos especialistas brasileiros e podemos perceber um grande progresso. O Brasil é confrontado com uma ampla variedade das chamadas ameaças cibernéticas, incluindo fraudes *on-line*, cibercrime e vigilância digital. Cada uma dessas ameaças é diferente em seu modo.

A maior preocupação para as autoridades brasileiras é, possivelmente, o roubo e a divulgação de informações oficiais sensíveis. No Brasil, o governo, incluindo o Itamaraty, as forças de segurança, o exército, bem como empresas privadas e públicas, como, por exemplo, a Petrobras, são regularmente alvos de ataques cibernéticos dos hacktivistas. Além disso, o governo brasileiro está testemunhando ataques crescentes contra sistemas e redes estatais. As causas principais desses ataques são as desigualdades generalizadas na América Latina e a manipulação generalizada de informações pelas autoridades.[81]

Os Assuntos da segurança cibernética estão sendo discutidos pelo Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR), e todas as questões da defesa nessa área estão sendo conduzidos pelo Centro de Defesa Cibernética, que é uma parte do Exército do Brasil, que em sua vez esta conectada com o Ministério da Defesa. Assim, podemos ver que existe uma grande hierarquia na tomada de decisões sobre Segurança Cibernética, e sem passar pela Presidência da Republica, uma determinada ação não vai ser realizada.[82]

A principal função da Agência Brasileira de Inteligência é investigar ameaças reais e potenciais à sociedade e ao governo brasileiro, defendendo o Estado Democrático de Direito, a

[81] DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing Cyber Security in Brazil:** Threats and Responses. Botafogo, RJ: Instituto Igarapé, 2014. p. 12

[82] CRUZ JÚNIOR, Samuel César da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual.** Texto para discussão. Brasília : Rio de Janeiro : Ipea, 2013. p. 21

soberania brasileira e a eficácia do poder público. O foco das agências de inteligência parece estar se movendo lentamente da gestão da dissensão interna para o foco em ameaças externas e apoio à democracia da nação. A ABIN, principalmente atua em ambas correntes de inteligência e contrainteligência, assim protegendo os dados sensíveis, além disso, promove o desenvolvimento dos projetos da segurança de comunicação.[83]

O Brasil ainda não tem nenhum documento que estabelece as diretrizes de uma estratégia nacional de segurança cibernética. Isso significa que ainda não existem objetivos, metas e responsáveis que sejam estabelecidos, sendo um desafio muito importante para o país. É necessário estabelecer uma estratégia viável, para conseguir competir futuramente nessa área. A Estratégia Nacional de Defesa trouxe diretrizes conectadas com o Ciberespaço, enfatizando a importância de fortalecer as estratégias espaciais cibernéticas e nucleares do Brasil.[69]

Existe uma hierarquia de instituições estatais envolvidas no gerenciamento da segurança cibernética brasileira. No topo da pirâmide está o Escritório Presidencial para Segurança Institucional (EPSI). Em contato direto com o Presidente, o EPSI é um órgão fundamental do governo encarregado de lidar com todos os aspectos relacionados à segurança cibernética, como também aos assuntos militares e de defesa cibernética. Uma outra instituição importante para a segurança cibernética brasileira é o Departamento de Polícia Federal (DPF), sob a supervisão do Ministério da Justiça (MJ). Seu principal papel é a aplicação da lei em nível federal, mas também possui unidades dedicadas à segurança cibernética. Da mesma forma, a Agência Brasileira de Inteligência (ABIN), além de se engajar em monitoramento de mídias sociais, desenvolveu competências criptográficas para proteger instituições públicas.[84]

O Marco Civil é basicamente uma carta de Direitos para a Internet brasileira e a primeira desse tipo no mundo. O Marco Civil estabelece princípios fundamentais para a Internet, incluindo liberdade de expressão, neutralidade da rede e proteção da privacidade. O projeto foi aprovado em abril de 2014 no Congresso Nacional, e deverá fortalecer e preservar os direitos dos usuários. Um dos elementos-chaves na modelagem da cibersegurança que está sendo discutido atualmente no Marco Civil é o chamado registro de log. O registro de log é um mecanismo fundamental para investigação cibernética e análise relacionada com crimes. Esse elemento permite que os provedores de conteúdo e os provedores de serviços da internet mantenham os registros de conexão

[83] Idem, p. 21.
[84] DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing Cyber Security in Brazil:** Threats and Responses. Botafogo, RJ: Instituto Igarapé, 2014. p. 20.

do usuário do seu site, para que possam ser revisados pelas autoridades. A intenção original do Marco Civil era estabelecer garantias constitucionais e salvaguardas relacionadas à gestão do ciberespaço no Brasil, mas ele se tornou também um impulso para a legislação agressiva de prevenção do crime cibernético. Com isso, foi estabelecido que é ilegal a invasão de dispositivos de Tecnologias de informação, obter dados privados, bem como interferir ou interromper serviços de TI.[85]

As forças armadas estão fazendo uma séria tentativa de expandir seu papel de ator-chave na definição da direção dos assuntos brasileiros. Enquanto o sistema democrático do Brasil continua amadurecendo, os militares também estão sendo reestruturados e buscando um novo papel no futuro interno e externo do Brasil. Somente em 2008 a segurança cibernética foi incluída na doutrina das Forças Armadas, e em 2010 foi criado o CDCiber, para coordenar as ações de defesa digital. Ele está localizado entre os níveis estratégico e operacional da arquitetura de defesa cibernética do Brasil. O principal objetivo dele é oferecer proteção a redes militares e governamentais. O CDCiber tem à sua disposição um simulador de guerra cibernética, um laboratório para análise de código malicioso virtual e quase cem oficiais treinados em segurança cibernética.[86]

O governo Brasileiro deve encorajar um amplo debate com uma estratégia clara de comunicação sobre os requisitos da segurança cibernética e quais formas isso poderá tomar. É também necessária uma reflexão mais crítica sobre a forma e o conteúdo de estratégias e medidas eficientes para envolver as ameaças cibernéticas. Melhor coordenação entre as forças policiais estaduais para melhor antecipar e responder ao crime cibernético é essencial. Quando respondendo ao um ataque cibernético é necessário ter uma melhor coordenação, e enquanto respondendo a um ataque específico, não se podem esquecer demais tipos.[87]

Em suma, pode-se ver que essa área é ainda nova para o Brasil, medidas certas estão sendo tomadas pelo governo, mas ainda há muita incerteza. Foram criados múltiplos órgãos de defesa e segurança cibernética, mas é necessário mais desenvolvimento. O Ciberespaço está sempre crescendo e, com isso, muito esforço é necessário para conseguir se sustentar nessa área e poder

---

[85] DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing Cyber Security in Brazil:** Threats and Responses. Botafogo, RJ: Instituto Igarapé, 2014. p. 20

[86] HUREL, Louise Marie; LOBATO, Luisa Cruz. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**. Botafogo, RJ: Instituto Igarapé, 2018.

[87] DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing Cyber Security in Brazil:** Threats and Responses. Botafogo, RJ: Instituto Igarapé, 2014. p. 30

competir com países como Estados Unidos, Rússia e até Israel. O Brasil está trabalhando perto desses países para melhorar a sua abordagem para, num futuro próximo conseguir melhorar a sua posição no Ciberespaço e competir com os lideres da internet, bem como combater o crime cibernético com os melhores meios possíveis.

CONCLUSÃO

O mundo está sob constante mudança e com isso a tecnologia está ficando mais avançada. Com todos os avanços tecnológicos, vêm também múltiplos perigos e ameaças, sendo que muitos cientistas dizem que o avanço tecnológico é algo muito perigoso e que em longo prazo poderia criar muitos problemas para a humanidade. Base dessa teoria é que muitas organizações estão trabalhando para criar inteligência artificial, que, saindo do controle, poderia criar um futuro muito sombrio.

A base dessa pesquisa foi mostrar como o Ciberespaço pode ser algo bom e algo muito perigoso no mesmo tempo. Sem dúvida, a internet trouxe muitos benefícios para a humanidade, mas também virou um instrumento que pessoas podem usar para fins prejudiciais. Muitos países estão trabalhando a fim de explorar e entender melhor o Ciberespaço, para conter e combater as ameaças que surgirem, mas não é possível prever qual vai ser o próximo perigo.

Com as crescentes ameaças de *hackers* sofisticados, o setor de segurança cibernética está passando por uma mudança em termos de *design* e implementação de produtos e serviços de segurança. Percebendo a impraticabilidade de intervenções humanas contínuas para rastrear e contra-atacar ameaças, os líderes da indústria estão focados no uso de inteligência artificial (IA) para fortalecer seus produtos e serviços de segurança. Enquanto a IA fornece uma série de benefícios em termos de automatizar todo o processo, desde a identificação de ameaças até a tomada de medidas preventivas, por outro lado, pode abrir as portas para muitas vulnerabilidades, fornecendo oportunidades para os *hackers* explorarem a inteligência artificial e criar algoritmos destrutivos que suportem sua intenção.

A segurança cibernética está agora na vanguarda das discussões sobre políticas e planejamento de futuros conflitos. De muitas maneiras, a ameaça cibernética nivelou o campo de jogo, e isso apresenta preocupações únicas para os Estados Unidos e seus aliados. O governo dos EUA tem conhecimento que com avanço tecnológico nessa área, muitos dos seus adversários vão chegar ao mesmo nível de conhecimento e isto causará diversas ameaças, o que pode até significar uma Guerra cibernética no futuro. Assim, uma estratégia cibernética que possa deter com credibilidade potenciais inimigos é cada vez mais necessária, assim como as formas de manter os sistemas críticos defendidos. Para atingir isso, os EUA devem trabalhar intensivamente na infraestrutura crítica e manter um limite para que os grupos terroristas e os poderes menores como, por exemplo, a Coréia do Norte e Irã, não tenham a capacidade de manter o país em risco por meio

de ataques cibernéticos. Sem duvida, os EUA são os líderes na área de Segurança Cibernética e estão fazendo o possível para se manter na liderança, mas países como Rússia, China e Israel não estão distantes de atingir a mesma meta.

O Ciberespaço é ainda uma área nova para o Brasil. Muitas tentativas foram feitas para se inserir nessa área de melhor modo possível. Foi criado o CDCiber, para coordenar as ações de defesa digital, que possui um simulador de guerra cibernética, um laboratório para análise de código malicioso virtual em sua disposição. O país está sendo alvo de ataques cibernéticos quase todos os dias, mas com um sistema de segurança cibernética pouco avançada, nem todos os ataques estão sendo localizados e contidos. A Unidade de Combate ao Cibercrime (URCC) da Polícia Federal é a principal autoridade responsável pela prevenção e resposta ao cibercrime, mas muitas vezes, eles estão focando em um tipo de ameaça só, assim ignorando quase completamente todos os outros tipos. Mas apesar de todas as dificuldades que o Brasil está enfrentando nessa nova área, há progresso para conseguir melhorar a sua estratégia e conseguir, no futuro, competir com países como EUA.

Conforme abordado neste trabalho, podemos perceber que o destino do Ciberespaço, da Segurança Cibernética, ainda é desconhecido. Sem dúvida, no futuro haverá novas ameaças e, provavelmente, guerras entre países no nível cibernético, mas isso não impedirá que o mundo continue evoluindo. Muitos países estão cooperando para atingir a paz na área do Ciberespaço e isso fortaleceu a amizade entre eles. Assim, a Segurança Cibernética é uma área muito importante para todos, possibilitando criar laços mais fortes entre os países e seus aliados. As Relações Internacionais têm uma importância muito grande nessa área, pois sem ela, seria difícil imaginar a segurança.

REFERÊNCIAS

ARQUILLA, John. **The New Rules of War**. In: Foreign Policy**,** 02 nov. 2010. Disponível em: < https://foreignpolicy.com/2010/02/11/the-new-rules-of-war/>. Acesso em: 15 abr. 2019.

BAR-JOSEPH, Uri. **A Heterodox Conclusion on Intelligence Failures in the Age of Cyberwarfare.** In: Rar on the Rocks, 3 jan. 2017. Disponível em: <https://warontherocks.com/2017/01/a-heterodox-conclusion-on-intelligence-failures-in-the-age-of-cyberwarfare/>. Acesso em: 15 abr. 2019.

CAVELTY, Myriam Dunn. **Cybersecurity Contemporary Security Studies**. Oxonia, UK: Oxford University Press, 2012.

CHANG, Y. C. Lennon; GRABOSKY, Peter. The governance of cyberspace. In: **Regulatory Theory: Foundations and applications**. Canberra, Australia: ANU Press, The Australian National University, 2017.

COUNCIL OF THE RUSSIAN FEDERATION. Site Oficial do Conselho da Federação da Rússia. **O Conceito Da Estratégia De Segurança Cibernética da Federação Russa**, 2014. Disponível em: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>. Acesso em: 15 abr. 2019.

CRUZ JÚNIOR, Samuel César da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Texto para discussão. Brasília : Rio de Janeiro : Ipea, 2013.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing Cyber Security in Brazil:** Threats and Responses. Botafogo, RJ: Instituto Igarapé, 2014. Disponível em: <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf>. Acesso em: 10 mar. 2019.

HEINEGG, Wolff Heintschel von. Territorial Sovereignty and Neutrality in Cyberspace. **International Law Studies**, v. 89, 2013. Disponível em: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1027&context=ils>. Acesso em: 08 mar. 2019.

HOPPING, Clare, SHEPHERD, Adam, WINDE, Davey. **What is cyber warfare?** In: ITPro, 12 dez. 2018

HUREL, Louise Marie; LOBATO, Luisa Cruz. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**. Botafogo, RJ: Instituto Igarapé, 2018.

ISRAEL. Prime Minister's Office. National Cyber Directorate. **Israel National Cyber Security Strategy In Brief**. Set. 2017. Disponível em: <http://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf>. Acesso em: 20 mar. 2019.

LEWIS, A. James. **A Note on the Laws of War in Cyberspace**. In: CSIS, 25 abr. 2010. Dispoível em: <https://www.csis.org/analysis/note-laws-war-cyberspace>. Acesso em: 09 abr. 2019.

MARCELLA, Gabriel; MCILHENNY, William. **Hard Talk Forum**. In: Americas Quarterly, 8 jan. 2014.

MAUER Victor, CAVELTY Myriam Dunn. **The Routledge Handbook of Security Studies**. New York: Routledge, 2010.

NYE, Joseph S. **Cyber Power**. Cambridge, USA: Harvard Kennedy School, 2010.

SIBONI, Gabi; ASSAF, Ofer. **Guidelines for a National Cyber Strategy**. Tel Aviv: Institute for National Security Studies, 2016.

SINGER, Peter Warren, FRIEDMAN, Allan. **Cybersecurity and Cyberwar**. Oxonia, UK: Oxford University Press 2014.

THE History Of Cyber Security — Everything You Ever Wanted To Know. In: Sentileone, 10 mar. 2018. Disponível em: <https://www.sentinelone.com/blog/history-of-cyber-security/>. Acesso em:

TRAYNOR, Ian. **Russia accused of unleashing cyberwar to disable Estonia**. In: The Guardian Brussels, 17 maio 2007. Disponível em: <https://www.theguardian.com/world/2007/may/17/topstories3.russia>. Acesso em: 17 mar. 2019.

US CYBER COMMAND. Site oficial do Ciber Comando dos EUA (USCYBERCOM). Disponível em: <https://www.cybercom.mil/About/Mission-and-Vision/>. Acesso em: 10 fev. 2019.

WEISBROT, Mark. **Washington and São Paulo**: Spying and a Fading Friendship. In: NACLA Report on the Americas, 2013. Disponível em: <https://nacla.org/news/2014/1/30/washington-and-s%C3%A3o-paulo-spying-and-fading-friendship>. Acesso em: 13 mar. 2019.

WILLIAMS, D. Paul. **Security Studies - An Introduction**. New York: Routledge, 2008

GLOSSÁRIO

Ciberespaço: é uma tecnologia digital interconectada e difundida. É o ambiente virtual em que ocorre a comunicação pelas redes de computadores. Ainda não tem uma definição certa desse termo.

Conflito: implica conflito de interesse. A base do conflito pode variar, mas é sempre uma parte da sociedade. Base de conflito - pessoal, racial, de classe, casta, política e internacional.

Guerra Cibernética: é o uso ou a segmentação em um ambiente de batalha ou guerra de computadores, sistemas de controle on-line e redes. Envolve tanto operações ofensivas quanto defensivas relativas à ameaça de ataques cibernéticos, espionagem e sabotagem.

Hacker: é qualquer especialista em informática que use seu conhecimento técnico para superar um problema ou criá-lo.

Hacktivistas: é um grupo de hackers que usa tecnologia para promover uma agenda política ou uma mudança social. Com raízes na cultura hacker e na ética dos hackers, seus fins estão muitas vezes relacionados à liberdade de expressão, aos direitos humanos ou aos movimentos de liberdade de informação.

Hardware: inclui as partes ou componentes físicos e tangíveis de um computador, como gabinete, unidade central de processamento, monitor, teclado, armazenamento de dados do computador, placa gráfica, placa de som, alto-falantes e placa-mãe.

Internet: é o sistema global de redes de computadores interconectados que usam o conjunto de protocolos de Internet para vincular dispositivos em todo o mundo.

Malware: é qualquer software projetado intencionalmente para causar danos a um computador, servidor, cliente ou rede de computadores. O malware faz o estrago após ser implantado ou introduzido de alguma forma no computador de um alvo e pode assumir a forma de código executável, scripts, conteúdo ativo e outros softwares.

Ransomware: é um tipo de malware da criptovirologia que ameaça publicar os dados da vítima ou bloqueia perpetuamente o acesso a ela, a menos que um resgate seja pago.

Relações Internacionais: é o estudo da interconexão entre política, economia e direito em nível global.

Segurança Cibernética (Cibersegurança): é a proteção de sistemas de computador contra roubo ou danos ao hardware, software ou dados eletrônicos, bem como a interrupção ou desorientação dos serviços que eles fornecem.

Software: é uma coleção de dados ou instruções de computador que informam ao computador como funciona.

Terrorismo Cibernético: é o uso da Internet para conduzir atos violentos que resultem em, ou ameaçam, a perda de vidas ou danos corporais significativos, a fim de obter ganhos políticos ou ideológicos por meio de ameaça ou intimidação.

Vírus: é um tipo de software malicioso que, quando executado, se replica modificando outros programas de computador e inserindo o seu próprio código.