ESCOLA DE COMANDO E ESTADO MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Maj Com MARIANO OSCAR **GÓMEZ**, Exército Argentino

Como construir sistemas cibernéticos resilientes avaliando as práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN na Estônia

Rio de Janeiro

2018

Maj Com MARIANO OSCAR **GÓMEZ**, Exército Argentino

Como construir sistemas cibernéticos resilientes avaliando as práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN na Estônia

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Orientador: Prof. Dra. Karina Furtado Rodrigues

Rio de Janeiro

2018

G633c Gomez, Mariano Oscar
Como construir sistemas cibernéticos resilientes avaliando as práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN/ Mariano Oscar Gomez. ―2018.
39 f. : il. ; 30 cm.

Orientação: Karina Furtado Rodrigues
Trabalho de Conclusão de Curso (Especialização em Ciências Militares). ―Escola de Comando e Estado-Maior do Exército: Rio de Janeiro, 2018.
Bibliografia: f. 29-39.

1. RESILIÊNCIA. 2. CIBERDEFESA. 3. OTAN. 4. ESTÔNIA. I. TÍTULO.

CDD 003.5

Maj Com MARIANO OSCAR **GÓMEZ**, Exército Argentino

Como construir sistemas cibernéticos resilientes avaliando as práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN na Estônia

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares.

Aprovado em de novembro de 2018.

COMISSÃO AVALIADORA

_____

Prof. Dra. Karina Furtado Rodrigues
Escola de Comando e Estado-Maior do Exército

_____

Prof. Dr. Luiz Rogério Franco Goldoni
Escola de Comando e Estado-Maior do Exército

_____

Prof. Dra. Mariana Carpes
Escola de Comando e Estado-Maior do Exército

À minha esposa Guadalupe meus filhos María Lucía e Santiago. Uma sincera homenagem pelo carinho e compreensão demonstrados durante a realização deste trabalho.

AGRADECIMENTOS

À Professora Doutora Karina Furtado Rodrigues, não só pela orientação firme e segura, como também, pelo incentivo e pela confiança evidenciada em todo momento. Sua dedicação se revestiu de capital importância para que eu pudesse realizar o trabalho com tranqüilidade e eficiência.

Ao Major de Cavalaria Guilherme Cortinhas Luchetti, por sua amizade, compreensão e apoio incondicional durante o ano todo.

Ao Instituto Meira Mattos e à Escola de Comando e Estado Maior do Exército, por ter-me permitido realizar o curso e acolhido como si fosse um oficial mais da sua Instituição.

Ao Exército Argentino pela confiança posta em mim para fazer o Curso de Comando e Estado-Maior na República Federativa do Brasil.

A Deus, pela proteção e orientação recebidas, principalmente nos momentos mais difíceis. Pela força necessária que recebi para resolver os problemas apresentados.

RESUMO

Os avanços tecnológicos e a crescente infra-estrutura digital tornaram populações inteiras dependentes de sistemas interligados e complexos, chegando na atualidade à concepção de que todos os serviços modernos dependem do uso das TIC.

A chegada e evolução do ciberespaço transformaram o mundo e revolucionou o cotidiano dos habitantes do globo. É assim que, com o aumento inevitável da dependência da tecnologia no nível global, a vulnerabilidade contra ataques sobre a infra-estrutura crítica, através do ciberespaço, também foi aumentada.

Essas ameaças se apresentam no campo de batalha moderno além do arcabouço tridimensional da campanha, acrescentando uma quarta dimensão (ciberespaço) que merece ser abordada.

Para fazer frente a essa situação, é preciso definir estratégias que possibilitem preservar os sistemas próprios (principalmente os dados) sobre a base da impossibilidade de impedir um ataque cibernético por responder geralmente a ameaça de origem e natureza inéditas.

O termo que abrange essa estratégia é a "Resiliência", e sua correta concepção permitiria que um sistema assumisse capacidades suficientes para se adaptar às ações inimigas no ciberespaço, restaurando informações até momentos antes da referida ação.

O presente estudo busca, a partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN, compreender quais são as condições causais que conduzem à resiliência de sistemas cibernéticos e como estas práticas vem se difundindo.

A partir disso, será realizada uma análise referente à possibilidade (ou não) de transferir esse modelo gerado à América Latina.

Palavras-chave: Resiliência, Ciberdefesa, OTAN, Estônia.

ABSTRACT

Technological advances and the growing digital infrastructure have made whole populations dependent on interconnected and complex systems, and nowadays they come to the view that all modern services depend on the use of ICT.

The arrival and evolution of cyberspace have transformed the world and revolutionized the daily lives of the inhabitants of the globe. Thus, with the inevitable increase in dependence on technology at the global level, vulnerability to attacks on critical infrastructure through cyberspace has also been increased.

These threats present themselves on the modern battlefield beyond the three-dimensional framework of the campaign, adding a fourth dimension (cyberspace) that deserves to be addressed.

In order to deal with this situation, it is necessary to define strategies that allow preserving the systems themselves (mainly data) on the basis of the impossibility of preventing a cyber attack by generally responding to the threat of unprecedented origin and nature.

The term encompassing this strategy is "Resilience," and its correct design would allow a system to assume sufficient capabilities to adapt to enemy actions in cyberspace, restoring information until moments before such action.

The present study seeks to understand, from the practices of the Center for Cooperative Excellence in Cyber Defense of NATO, the causal conditions that lead to the resilience of cybernetic systems and how these practices are spreading.

From this, an analysis will be carried out regarding the possibility (or not) of transferring this generated model to Latin America.

Keywords: Resilience, Cyber-defense, NATO, Estonia.

SUMÁRIO

1 **INTRODUÇÃO**

Os avanços tecnológicos e a crescente infra-estrutura digital tornaram populações inteiras dependentes de sistemas interligados e complexos. A demanda por Internet e conectividade digital requer uma crescente integração das Tecnologias de Informação e Comunicação (TIC) em produtos que anteriormente funcionavam sem essas técnicas, tais como nos sistemas de controle de barragens; sistemas de controle de tráfego; sistemas nacionais integrados de saúde; redes de distribuição de eletricidade; redes sanitárias de água e esgoto; transporte poli-modal; movimentação e tráfego aéreo; reservas de bilhetes; movimentações bancárias (como transferências e pagamentos bancários); pagamentos em lojas; depósito de salários; e até mesmo no pagamento de um estacionamento. Hoje, praticamente todos os serviços modernos dependem do uso das TIC.

A chegada e evolução do ciberespaço transformaram o mundo e revolucionou o cotidiano dos habitantes do globo. Como no mar, terra ou ar, o espaço cibernético é um domínio onde os seres humanos manobram dentro e através dele para alcançar objetivos nos espaços físicos onde vivem. Não tem fronteiras geográficas, a tecnologia é barata e está ao alcance de qualquer um, ações perniciosas são autores anônimos, e vão desde adolescentes até organizações criminosas, algumas independentes e outras são apoiadas por alguns governos.

Com o aumento inevitável da dependência da tecnologia no nível global, a vulnerabilidade contra ataques sobre a infra-estrutura crítica, através do ciberespaço, também foi aumentada. Essa infra-estrutura crítica (embora haja uma multiplicidade de definições dos conceitos) abrange o domínio virtual, universal e dinâmico, criado pelo homem, constituído por infra-estruturas de tecnologia da informação, redes e sistemas de informação e telecomunicações, incluindo as das Forças Armadas.

Como resultado da análise realizada sobre os problemas ditados pelo estado da arte em relação às operações no ambiente cibernético, é possível perceber que as ameaças que podem ser apresentadas no moderno campo de batalha realmente se estendem além do arcabouço tridimensional da campanha, acrescentando uma quarta dimensão (ciberespaço) que merece ser abordada.

Essa referência, adaptada ao objeto de estudo, é denominada "Resiliência", e sua correta concepção permitiria que um sistema de armas implantado na campanha assumisse capacidade suficiente para se adaptar às ações inimigas no ciberespaço, restaurando informações até momentos antes da referida ação.

Como um termo genérico, responde a um conceito usado no campo da engenharia pelo qual é chamado de resiliência de um material à energia de deformação (por unidade de volume) que pode ser recuperada de um corpo deformado quando o esforço que causa a deformação desaparece. Ou seja, seria seu limite elástico, para o qual, uma vez superado, o material não poderá mais ser recuperado e permanecerá "deformado" (CORLETTI ESTRADA, 2011).

Fazendo um paralelo com uma infra-estrutura de computador, seria apenas a capacidade de recuperar seu estado inicial depois de ter sido afetado por algum agente (capacidade "elástica"). Portanto, a resiliência cibernética pode ser definida como a capacidade de responder e se recuperar de incidentes de segurança.

O presente estudo busca, a partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN, compreender quais são as condições causais que conduzem à resiliência de sistemas cibernéticos e como estas práticas vem se difundindo.

A partir disso, será realizada uma análise referente à possibilidade (ou não) de transferir esse modelo gerado à América Latina.

1.1 PROBLEMA

A partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN, quais são as condições causais que conduzem à resiliência de sistemas cibernéticos e como estas práticas vem se difundindo?

1.2 OBJETIVOS

1.2.1 **Objetivo Principal**

Compreender, a partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN, quais são as condições causais que conduzem à resiliência de sistemas cibernéticos e sua possível transferência à América do Sul.

1.2.2 **Objetivos Específicos**

a. Compreender quais são os padrões internacionais existentes de geração de resiliência em sistemas cibernéticos;

b. Compreender como o Centro de Excelência Cooperativo de Defesa Cibernética da OTAN, na Estônia, se destaca em relação a outros padrões internacionais;

c. Delinear quais são as condições causais elementos constituintes de sistemas resilientes e suas respectivas relações de necessidade e suficiência;

d. Analisar em que medida estes parâmetros internacionais foram ou podem ser importados para os países da América Latina de maneira efetiva, conforme a literatura de Policy Transfer.

1.3 DELIMITAÇÃO DO ESTUDO

A presente investigação abrange a descrição conceitual de termos relacionados ao tema e necessários para a concepção do objeto de estudo, a aplicação daqueles elementos do desenho operacional essenciais para a implantação de um sistema resiliente, juntamente com a declaração de matrizes de risco aplicáveis à problemática proposta, e a descrição da evolução da Estônia como modelo de sistema da União Européia, quanto à segurança e defesa cibernética.

O presente estudo não abordará aspectos básicos já desenvolvidos por outros autores relacionados à defesa cibernética, cibersegurança e ciberguerra.

Da mesma forma, estudos comparativos com desenvolvimentos previstos por outras Forças Armadas serão abordados só ao respeito de aspectos básicos de utilidade para o objeto de estudo apresentado a partir deles.

No que se refere à análise do estudo de caso, será considerado exclusivamente o período de 2007 a 2018, e os aspectos fundamentais que constituem uma contribuição essencial para o problema proposto, porque é o período de desenvolvimento da Estônia logo depois do ciberataque vital recebido em abril de 2007.

1.4 RELEVÂNCIA DO ESTUDO

O mundo hoje está passando por profunda crise digital, dada a esmagadora evolução dos sistemas de computadores, a interligação de todos os tipos de dispositivos e a confluência de informações de forma indiscriminada, por meios que há não muito tempo atrás teriam sido impensáveis.

Se incorporados nestas problemáticas intenções maliciosas de todos os tipos de agentes (pessoas, robôs, organizações, etc.), o diagnóstico situacional é caótico, especialmente quando se trata de um espectro não tão explorado como é a cibernética.

Os países mais desenvolvidos do mundo em termos cibernéticos (Estados Unidos, Rússia, Alemanha, França, Espanha, Israel, Estônia, entre outros), passaram a considerar o

ciberespaço como mais uma dimensão, cujo tratamento, de 2007 até hoje, foi exponencial. Vários desses Estados chegaram a considerar a possibilidade de especificar uma nova Força Armada orientada para essa nova dimensão.

Entender como, a partir das experiências adquiridas pela Estônia em quanto à ciber-resiliência, e entendendo que a OTAN está impondo as medidas como norma de funcionamento cibernético na Europa é possível entender que cada um desses componentes do modelo precisa ser devidamente analisado e compreendido para facilitar sua aplicação fora desse ambiente controlado.

Sendo assim, América Latina é muito adolescente dessa cultura cooperativa e colaborativa que possibilite a aplicação de medidas no campo cibernético que contribuam a blindar a região como um todo, e não cada país em relação a sua particularidade geopolítica.

O presente estudo é relevante em quanto procurará identificar a importância do Centro de Excelência e Cooperação de Ciber Defesa da OTAN tem para chegar a um modelo de resiliência cibernético de nível regional. A Cooperação Européia para o estabelecimento de padrões de excelência necessários para atingir a resiliência cibernética.

Somado a isso, permitirá avaliar e ponderar o peso que é dado às resoluções regionais da OTAN para a aplicação de medidas no campo cibernético.

Ao respeito da relevância dos dados obtidos, não se limitará às conclusões do autor, mas também se amparará em especialistas na matéria para, junto com eles, arribar a um modelo de ciber-resiliência aplicável no marco do conglomerado de variáveis e condições, e sua devida catalogação.

Finalmente, dos resultados obtidos e da análise da situação regional em termos da evolução do domínio da defesa do ciberespaço e da cooperação nesta matéria, se avaliará a possibilidade (ou não) de aplicação de um modelo cibernético exportável de uma situação, um contexto diferente e mais evoluído.

2 **REFÊRNCIA TEÓRICA E METODOLÓGICA**

2.1 REFERÊNCIA TEÓRICA

As operações no ambiente cibernético têm sido consideradas no campo da campanha desde 1988, uma oportunidade em que a Internet foi vítima de um ataque com um vírus de computador, deixando o sistema totalmente vulnerável a ameaças eletrônicas. Como conseqüência deste evento, as organizações militares mais expostas e relevantes do momento

(Estados Unidos da América e OTAN) começaram a implementar medidas de contingência diante dessa nova forma de ameaça (KLIMBURG, 2014).

"O batismo de fogo" como o envolvimento de organizações militares só veio em 1998, quando as forças da OTAN foram objeto de um ataque cibernético e os Estados Unidos eram vulneráveis à detecção de acesso remoto de operadores não autorizados ou não identificados à rede de computadores do Pentágono (KLIMBURG, 2014).

No entanto, o marco histórico que despertou o interesse militar no quadro geral relativa à proteção dos sistemas informáticos remonta, a 27 de Abril de 2007, altura em que a Estônia foi alvo de um ataque cibernético sem precedentes. As páginas dos bancos ficaram saturadas, não foi possível sacar dinheiro dos caixas eletrônicos, as transações virtuais foram negadas e as páginas do governo entraram em colapso (WINTERFELD, S.; ANDRESS, J.; 2013).

O ataque afetou mais de 1.300.000 habitantes. A razão, deduzida pelo governo estônico, foi a remoção de uma estátua de bronze antiga de um soldado da União Soviética no centro de Tallinn, uma vez que para o governo russo, a estátua simbolizava seu poder geopolítico no Báltico. Além disso, como os ataques de computador eram imprevisíveis e anônimos, não havia argumento para atribuir o ataque à Rússia (WINTERFELD, S.; ANDRESS, J.; 2013).
Nas operações cibernéticas no âmbito militar, são consideradas todas aquelas executadas para interromper, negar, degradar ou destruir as informações existentes em computadores e redes de computadores, ou computadores e redes em si. Eles podem ser uma forma avançada de uso de força que precede o esforço principal no Teatro das Operações, a fim de preparar o alvo para o ataque principal. Eles podem incluir reconhecimento (mapeamento de uma rede), as posições de apoio de captura (o acesso seguro a nós ou sistemas de rede chave) e os braços pré-posicionamento ou recursos (ferramentas de implantes cibernéticos de acesso ou código malicioso) (NEWMEYER, 2015).

Além disso, eles podem ser um método para obter inteligência estrangeira fora de objetivos militares específicos, tais como entender os desenvolvimentos tecnológicos ou obter informações sobre as capacidades militares e a intenção do adversário (NEWMEYER, 2015).

Através do espaço cibernético, a informação é transferida por meio de conteúdos e códigos (software) e o que pode ser visto como o entrelaçamento do espaço cibernético e da atividade humana, o número de seres humanos utilizando o espaço cibernético para as atividades comuns (comunicação, navegação, notícias, compras, serviços bancários, entretenimento, etc.) aumenta rapidamente. Essa rápida evolução da rede, juntamente com seu poder de conexão, gerou grandes oportunidades econômicas e sociais imprevisíveis vinte anos atrás. A dependência do ciberespaço dilui fronteiras geográficas, desvia as divisões culturais e

religiosas tradicionais, une famílias e amigos e permite o contato entre aqueles que compartilham interesses ou preocupações. O modo de comunicação mudou (HARRINGTON, A.; THEOHARY, C., 2015).

Quanto ao fato de o espaço cibernético ser transversal a todas as áreas convencionais, ou independente delas, pode-se dizer que cada terra, mar e força aérea tem aspectos cibernéticos específicos, especialmente aqueles correspondentes aos sistemas de armas em seu território. O relacionamento sensor-tiro, além da chegada e evolução do espaço cibernético, transformou o mundo e revolucionou o cotidiano dos habitantes do globo. Como no mar, terra ou ar, o espaço cibernético é um domínio onde os seres humanos manobram dentro e através dele para alcançar objetivos nos espaços físicos onde vivem. Não tem fronteiras geográficas, a tecnologia é barata e está ao alcance de qualquer um, ações perniciosas são autores anônimos, e seus autores vão desde adolescentes até organizações criminosas, algumas independentes e outras que aparecem como tais, são apoiadas por alguns governos (SILVA, 2013).

No entanto, é preciso lembrar que, hoje, confrontos e conflitos que ocorrem no ciberespaço podem não necessariamente ocorrer no contexto de uma guerra, mesmo em um confronto geral. Assim, o termo ciberguerra, conforme mencionado, é mais descritivo e representa a luta entre dois estados ou facções do mesmo, ou agentes não estatais, o que toma lugar no ciberespaço. Tampouco há um acordo internacional sobre o que deve ser considerado como operações cibernéticas que afetam a Defesa Nacional (CRUZ JÚNIOR, 2013).

Cibersegurança, entendido como uma defesa objetiva e cibernética de um meio deve garantir a liberdade de ação das operações militares no ciberespaço e apoiar a resposta coordenada entre diferentes atores, nacionais e internacionais, antes de um ataque cibernético que poderia afetar a Defesa Nacional (CORLETTI ESTRADA, 2017).

Os aspectos que influenciam a vida cotidiana em relação ao uso do ciberespaço são amplamente divulgados. Todas as ações desenvolvidas neste campo afetarão o componente armado do Poder Nacional, sob várias perspectivas (LIBICKI, 2009).

O primeiro deles é o uso da força militar convencional em resposta a um ataque cibernético massivo. Essa possibilidade é contemplada porque os países mais poderosos em aplicações cibernéticas de uso diário são apenas os mais vulneráveis nesse aspecto. Diz-se que os efeitos de um ataque cibernético massivo multiplicaram várias vezes o que aconteceu na Estônia em 2007 e que teriam os mesmos resultados devastadores que um ataque nuclear. Nem todos os países aderem a esta posição porque iria levar a um uso arbitrário da força convencional (ARDITA, 2016).

A segunda envolve o uso do poder militar convencional dos países, antes do ataque cibernético às infra-estruturas civis. O impacto sobre os civis em um ataque a uma infra-estrutura crítica pode exigir o uso imediato de forças militares para aliviar os efeitos sobre as tarefas que certamente irão exceder a ajuda humanitária, tais como prevenção de saques e vandalismo. Este uso militar forçado na ajuda humanitária pode, além disso, ser complementado por um ataque militar convencional ao país afetado, uma vez que irá distrair as tropas de outros lugares (ARDITA, 2016).

A terceira ação é dupla: luta entre redes e sistemas de rede para afetar em operações defensivas cibernéticas - ativa e passiva - e exploração, o uso de sistemas automatizados de comando e controle que fornecem energia para combater as forças (militares) inimigas. O segundo é o uso do espaço cibernético como uma ferramenta para operações de informação que buscam enganar o inimigo para tomar decisões erradas. Nestas operações de informação, a cibernética pode ser usada em operações de apoio de informação às operações, de engano militar, de guerra eletrônica e em operações de inteligência como a espionagem e decifração de chaves (ARDITA, 2016).

Muitos usos coloquiais da palavra "ataque" em referência a algum tipo de incidente cibernético, seja pública ou privada (fraude, ameaças, sabotagem, roubo de dados, ataques de denegação de serviços) não são necessariamente "ataques armados" e os efeitos do exercício do direito inerente de um Estado de se defender, podem ser contraproducentes (ARDITA, 2016).

Independentemente de qual definição é adotada, deve ficar claro que, em relação à Defesa Nacional, os ataques cibernéticos representam uma nova e crescente ameaça, que o direito internacional e a maioria das leis nacionais atuais não estão alinhados com o Direito Internacional dos Conflitos Armados, freqüentemente citado como o plexo legal competente para qualificar ataques cibernéticos como equivalentes a um ataque armado. Outros documentos internacionais existentes, como o "Manual de Tallinn 2.0 sobre Direito Internacional aplicável a operações cibernéticas", oferecem apenas proteção embrionária ou fragmentada.

Do ponto de vista militar, as capacidades a serem desenvolvidas devem permitir comando e controle, isto é, direcionar e coordenar forças nas operações. Dado que muitos desses sistemas de comando e controle dependem do ciberespaço para funcionar, e para isso eles exigem uma infra-estrutura de tecnologias da informação e as telecomunicações para transmitir as informações, eles devem ser seguros e resilientes contra ataques cibernéticos e

devem estar permanentemente em funcionamento para poder direcionar as operações (NEWMEYER, 2015).

Além disso, esses recursos devem possuir a capacidade ou suficiência para reter a liberdade de ação no ciberespaço e prevenir surpresas estratégicas nessa dimensão, dentro de um determinado período. Portanto, será necessário ter tanto habilidades cibernéticas - defensivas e de inteligência - como tecnologias da informação e as telecomunicações (ARDITA e CORLETTI ESTRADA, 2016).

Dado que a atitude ofensiva é proibida no direito internacional, todos dizem se defender contra estes ataques, embora outros, como a OTAN, usam o termo "defesa ativa", como contra-ataques de lançamento ou não os agressores. Tanto assim, que já existem Regras de Engajamento Cibernético. Um exemplo seria o que a República Argentina faz: em virtude da separação entre segurança interna e defesa externa e com a proibição absoluta de qualquer ação ofensiva, optou por falar em "defesa direta" e "defesa indireta", circunlóquios que impedem que outros países do mundo compreendam seus significados (CARRASCO, 2015).

A Agressão Cibernética deve ser confrontada por natureza e não por seu lugar de origem, de modo a diferenciar a segurança interna de ataque militar externa, é um exercício ocioso e inútil de discrição. A disparidade dos conceitos de segurança e defesa nos países da UNASUL, a diferença de significados relacionados a este novo campo, e o uso de meios assimétricos para abordar a cooperação regional impede qualquer mais do que é declamado em documentos diplomáticos de folhas (UZAL, 2014).

A natureza descentralizada da Internet significa que não existe uma autoridade única e centralizada responsável por sua gestão, o que garante que os problemas possam ser resolvidos no nível mais próximo de sua origem. No entanto, há outros que consideram que devem intervir mais em sua gestão e coordenação internacional, pois acreditam que a Internet é tão importante que deve ser considerada de interesse nacional e, portanto, se sentem obrigados a intervir (SILVA, 2013).

Finalmente, deve ficar claro que o ciberespaço e a Internet não são sinônimos, a Internet é um subconjunto menor do ciberespaço maior. A maneira pela qual a Internet é governada sempre foi um tema muito debatido (UZAL, 2014).

As operações de rede de computadores visam modificar os dados e algoritmos de uma rede ou sistema, de modo que os resultados sejam obtidos ao contrário do que se esperava. Essas operações são classificadas pela maioria dos países como ofensivas, defensivas (passivas e ativas) e exploração ou exploração de redes de computadores. Os Estados Unidos da América denominam-nos Operações de Rede de Computadores e países como Grã-

Bretanha inclui dentro deles as operações de ciber-inteligência e ciber-preparação operacional do meio ambiente (SILVA, 2013).

As operações ofensivas no ciberespaço podem afetar, potencialmente, qualquer coisa que envolva tecnologia da informação ou comunicações, fato que os torna instrumentos extraordinariamente flexíveis para realizar os desejos dos responsáveis pela política nacional e para os quais muitas nações, inclusive os maiores e mais poderosos do mundo, estão interessados em explorar o valor potencial deste tipo de operações (CARRASCO, 2015).

Essas operações são executadas para comprometer a confidencialidade, integridade ou disponibilidade de informações. O fato de terceiros não autorizados terem acesso a informações que não deveriam ter, como roubar registros médicos eletrônicos, implica um compromisso com a confidencialidade das informações. O fato de modificar um prontuário médico do tipo sanguíneo de um paciente que se apresenta como tipo A, quando seu tipo atual de sangue é do tipo O, compromete a integridade da informação. Assim, também tornar impossível o acesso a um arquivo médico afeta a disponibilidade de informações (KUO, 2016).

Atualmente, não apenas as Forças Armadas dos países mais desenvolvidos do mundo, mas também os emergentes estão desenvolvendo e implementando medidas para "proteger" seus próprios sistemas contra ações inimigas no ambiente cibernético e, exclusivamente, as Forças Armadas de países mais desenvolvidos, para "seguir e perseguir" inimigos reais e potenciais através da exploração do ambiente cibernético (ARDITA e CORLETTI ESTRADA, 2016).

Para conseguir sistemas robustos e seguros, as agências de defesa cibernética das Forças Armadas que as possuem têm dependências específicas de "Resiliência", projetadas para "resistir" à ação inimiga nos próprios sistemas e, para poder "retornar ao estado inicial" em um período de tempo aceitável (ARDITA e CORLETTI ESTRADA, 2016).

A correta compreensão do princípio de resiliência relacionada ao âmbito cibernético é então uma exigência a ser entendida. A abordagem de base teoria em referência com este tema, será feita a partir da análise de autores tais como ANDRESS e WINTERFELD e sua obra “Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners” (2011); CARAYANNIS e CAMPBELL e seu livro “Cyber- Development , Cyber-Democracy and Cyber-Defense; Challenges, Opportunities and Implications for Theory, Policy and Practice” (2014); CORLETTI ESTRADA com um aporte muito interessante referido às técnicas possíveis de ciber-resiliência, detalhadas na sua obra “Ciberseguridad: Una Estrategia Informático-Militar” (2017); HILL e MARION com “Introducton to Cybercrime: Computer

Crimes, Laws, and Policing in the 21 st Century" (2016); PELTON e SINGH e sua obra "Digital Defense: A Cybersecurity Primer" (2015); RELIA e seu postulado "Cyber Warfare: Its Implications on National Security" (2015); RICHARDS e "Cyber-War: The Anatomy of the Global Security Threat" (2014); ROSENZWEIG se destacando com sua obra "Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World" (2013); ROWLAND, RICE e SHENOI com sua obra "The anatomy of a cyber power" (2014); STEWART, CHAPPLE e GIBSON e "Certified Information Systems-Security Professional Study Guide" (2015); e WINTERFELD e ANDRESS com sua obra "The Basics of Cyber Warfare" (2013); entre outros autores que serão convenientemente abordados.

Nesse contexto, a Estônia se destaca como Estado ciber-resiliente, cuja evolução é considerada como um caso de estudo pelos estudiosos deste campo. È assim que pode se evidenciar nessa evolução vasta bibliografia acadêmica que servirá de base referencial teórica para a pesquisa, tal como: ANDRESS e WINTERFELD e sua obra "Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners" (2011); CARAYANNIS e CAMPBELL com "Cyber- Development, Cyber-Democracy and Cyber-Defense; Challenges, Opportunities and Implications for Theory, Policy and Practice" (2014); CARR com "Inside cyber warfare: mapping the cyber underworld" (2011); CHENG e sua obra "Cyber Dragon: Inside China´s Information Warfare and Cyber Operations" (2017); ECONOMY, POWERS e JABLONSKI com "The Real Cyber War" (2015); GRAGIDO e PIRC com "Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats" (2011); HILL e MARION com "Introducton to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century" (2016); HYSLIP com "Bit Wars: cyber crime, hacking and information warfare" (2015); JANCZEWSKI e COLARIK e sua obra "Cyber Warfare and Cyber Terrorism" (2008); RELIA com "Cyber Warfare: Its Implications on National Security" (2015); RICHARDS com "Cyber-War: The Anatomy of the Global Security Threat" (2014); RID "Cyber War Will Not Take Place-Oxford University Press" (2013); ROSENZWEIG e seu livro "Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World" (2013); SINGER e FRIEDMAN com "Cybersecurity and Cyberwar - What everyone Needs to Know" (2014); WINTERFELD e ANDRESS com "The Basics of Cyber Warfare" (2013); entre outros autores.

Imerso nesse caminho de evolução cibernética, a OTAN explorou as debilidades evidenciadas pela Estônia, criando o Centro de Excelência e Cooperação de Ciber Defesa, com o objetivo de se proteger da nova modalidade de guerra que estava se apresentando. O

referencial teórico para desenvolver essa temática será baseada, entre outros, por os seguintes autores: ANDRESS e WINTERFELD com sua obra “Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners” (2011); CARAYANNIS e CAMPBELL com “Cyber-Development , Cyber-Democracy and Cyber-Defense; Challenges, Opportunities and Implications for Theory, Policy and Practice”(2014); CARR “Inside cyber warfare: mapping the cyber underworld” (2011); RID e seu livro “Cyber War Will Not Take Place” (2013); SINGER e FRIEDMAN com “Cybersecurity and Cyberwar - What everyone Needs to Know” (2014); WINTERFELD e ANDRESS com “The Basics of Cyber Warfare” (2013).

A Europa se comportou a partir dali, e mais especificamente nos últimos 7 anos, como um adaptador e executor modelo das medidas surgidas desse Centro de Excelência e Cooperação de Ciber Defesa da OTAN, demonstrando um interesse radical na matéria, elevando consideravelmente se índice de eficiência. Será empregada como referencial teórico o seguinte: CARAYANNIS e CAMPBELL com sua obra “Cyber- Development , Cyber-Democracy and Cyber-Defense; Challenges, Opportunities and Implications for Theory, Policy and Practice” (2014); HILL e MARION com “Introducton to Cybercrime: Computer Crimes, Laws, and Policing in the 21 st Century” (2016); HOUGH, MALIK, MORAN e PILBEAM com “International Security Studies: Theory and Practice” (2013); RELIA com “Cyber Warfare: Its Implications on National Security” (2015); RICHARDS e sua obra “Cyber-War: The Anatomy of the Global Security Threat” (2014); RID com “Cyber War Will Not Take Place”(2013); ROSENZWEIG com “Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World”(2013); SINGER e FRIEDMAN com “Cybersecurity and Cyberwar - What everyone Needs to Know” (2014); WINTERFELD e ANDRESS com seu livro “The Basics of Cyber Warfare” (2013); e XUE, ROY, WAN e DAS com “Handbook on Securing Cyber-Physical Critical Infrastructure” (2012); entre outros.

A partir dessa evolução é que a América do Sul começa se conscientizar da relevância deste novo modelo de segurança e, a partir da motivação individual de países como o Brasil ou a Colômbia, inicia o caminho da ciberdefesa e cibersegurança. Como baseamento teórico serão referenciadas as obras do CRUZ JÚNIOR com “A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégicas dos Estados Unidos, Rússia e Índia para o Espaço Virtual” (2013); GUEDES DE OLIVEIRA, DE CONTI PAGLIARI, MARQUES, PORTELA e BENTO FERREIRA NETO com sua obra “ Guia de Defesa Cibernética na América do Sul” (2017); SANTOS, CARVALHO e CAVALCANTE com “Segurança de infraestruturas críticas no Brasil (2017); entre outras.

Mas infelizmente o contexto regional de cooperação não é o suficientemente maduro e competente como para conseguir o ambiente de cooperação necessário para lograr a eficiência devida, sendo o exemplo da Europa e da OTAN um caso efetivo de cooperação no âmbito cibernético. Para isso, a pesquisa se baseará em referências teóricas tais como ERBSCHLOE com "Information Warfare - How to Survive Cyber Attacks" (2001); HILL e MARION com "Introducton to Cybercrime: Computer Crimes, Laws, and Policing in the 21 st Century" (2016); HOUGH, MALIK, MORAN e PILBEAM e sua obra "International Security Studies: Theory and Practice" (2014); JANCZEWSKI e COLARIK com "Cyber Warfare and Cyber Terrorism" (2008); MCQUADE com "Encyclopedia of Cybercrime" (2009); RELIA e o livro "Cyber Warfare: Its Implications on National Security" (2015); RICHARDS com "Cyber-War: The Anatomy of the Global Security Threat" (2014); ROSENZWEIG com sua obra "Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World" (2013); SINGER e FRIEDMAN com "Cybersecurity and Cyberwar - What everyone Needs to Know" (2014); e WOLFSON com "DIGITAL The Birth of the Cyber Left" (2014).

Mas para poder entender as variáveis que levaram à Estônia a se constituir como um estado ciber-resiliente, e poder pensar em como articular um modelo que seja aplicável fora da Europa, é necessário interpretar o mecanismo causal que gerou essa eficiência, particularizando cada causa componente segundo a sua relevância.

Mas das condições causais que a literatura identifica como necessárias para obter essa resiliência, quais são as que conduzem à resiliência de um sistema cibernético? Essa é a grande pergunta que deve ser respondida para criar o modelo de resiliência desejado.

Dentro dessas condições causais é possível identificar as seguintes:

- Gestão de risco e de mudanças; medidas preventivas e corretivas. Segundo BEAUDOIN, JAPKOWICZ, e MATWIN (2009), a gestão de risco atinge o equilíbrio certo entre o custo das medidas adotadas e o benefício hipotético para a sua implementação. Ou seja, este tipo de gestão é quando se trata de ameaças. O gerenciamento de mudanças se refere à identificação de mudanças a serem feitas e os impactos organizacionais que devem ser tidos em conta para o processamento adequado. Ou seja, este tipo de gestão é quando se trata da evolução da exposição a eventos externos. E as medidas preventivas são as decisões a serem adotadas como resultado da gestão de risco que não tem tido possível ser evitado ou que se tem previsto evitar no futuro, sendo que as corretivas são aquelas que são realizadas para eliminar a causa de um problema.

- Conhecimento profundo da organização (interna e externamente). SENGE (2006) afirma que alcançar o conhecimento real e profundo da organização é uma condição fundamental. Ciber resiliência requer adaptabilidade e sobrevivência, por isso, é necessário conhecer a organização e o ambiente. Visão crítica interna e externa da organização. A organização tem para programar redundância em seus sistemas, seus funcionários e seus processos. É para evitar expor cada um desses elementos da organização para a mesma ameaça. Em conclusão, o balanço de riscos entre todos os elementos da organização.
- Capacidade e participação no nível da organização de gerenciamento de tomada de decisão. Segundo o detalhe das partes componentes de uma organização e dos níveis que possui uma estrutura organizacional que estabelece MINTZBERG (1989), se confere que, para um sistema consiga atingir o seu estado de resistência, é necessária uma liderança harmoniosa e sinérgica de todos os níveis e componentes da organização em causa. Requer-se de capacidade operacional no que se refere a medidas no campo cibernético (gestão de risco, mudança, medidas preventivas e corretivas), a sensibilização do pessoal e liderança adequada nos mais altos níveis da organização é necessária para trazer à realidade medidas a tomar.
- Capacidade de antecipar a crise (CERT). Segundo NEWMEYER (2015) essas capacidades são a chave para a resiliência. As Equipes de Resposta de Emergência (CERT) são compostas por especialistas em cibersegurança e tem a responsabilidade de desenvolver preventiva e reativa a todos os tipos de incidentes relacionados à segurança dos sistemas informáticos.
- Simplificação de sistemas de informação para reduzir processos e interfaces. Analisando a teoria de PELTON e SINGH (2015) a estrutura, a base de arquitetura dos sistemas materiais e relações humanas devem ser tão simples quanto possível. Simplificar é um conceito que se refere a conseguir alguma coisa se torna mais simples, ou seja, menos complexa, difícil ou complicada. Dada a complexidade inerente aos sistemas informáticos, quanto mais simples sejam os sistemas, menores são os processos e interfaces, menos vulnerabilidades e violações de segurança serão geradas. Organizações mais simples são as que têm menos processos, em menos unidades, com menos sistemas, com menos interfaces entre eles.
- Processos contínuos e operacionais em qualquer circunstância. Segundo CORLETTI ESTRADA (2017), todo sistema informático é composto de infra-estrutura, hardware, software e processos, cada um com um nível de interferência particularizado, afetando em maior ou menor medida, o bom funcionamento da plataforma. Mas todos eles trabalham sinergicamente para que, como um todo, possam se transformar em um sistema resiliente. Mas esse processo deve ser contínuo e operado sob quaisquer circunstâncias, distinguindo os

processos que são essenciais e devem realizar escala de prioridades para o momento de ser temporariamente suspensos.

- Garantir regulamentos nas infra-estruturas críticas. Os autores ROWLAND, RICE e SHENOI (2014), definem às infra-estruturas críticas como aquelas instalações, redes, serviços e equipamentos físicos e de tecnologia da informação cuja perturbação ou destruição teria um impacto maior sobre o funcionamento eficaz das instituições estatais e autoridades públicas. É por isso que é necessário que essas infra-estruturas críticas sejam adequadamente reguladas e padronizadas para garantir a proteção necessária.

- Estrutura de sistema de informação (hardware e software). Segundo ECONOMY, POWERS e JABLONSKI (2015) é necessário assegurar o desenho da segurança cibernética dos elementos que suportam os processos da organização. Exigência de compra (hardware e software) de sistemas padronizados. Funcionalidade e fiabilidade dos sistemas de tecnologia da informação e comunicações. Aumentar o nível de demanda para compra de equipamentos sem dividir a parte funcional da segurança do produto.

- Desenvolvimento de exercícios e modelos de simulação. Analisando aos autores CARAYANNIS e CAMPBELL (2015) a simulação é necessária para verificar o nível de resiliência cibernético do sistema, a eficácia das medidas tomadas, e a avaliação da velocidade de resposta, a realização de exercícios e modelos de simulação, tanto seja no interior como no exterior do sistema, é necessária.

- A atualização do quadro legal. Segundo o "Tallinn Manual on the International Law Appicable to Cyber Warfare" (2011) é necessário harmonizar a legislação do ambiente cooperativo de políticas de segurança de rede e informações, bem como o estabelecimento de autoridades nacionais para a coordenação e ativação de CERT.

- Cooperação privada, estadual, nacional e regional. RICHARDS (2014) desenvolve o conceito que a cooperação entre as autoridades e agências de corpos de segurança e defesa é fundamental. Promover a cooperação e o intercâmbio de informações entre a indústria e os serviços de segurança cibernética.

- Ferramentas de desenvolvimento e melhoria contínua da segurança cibernética. Segundo RELIA (2015) tem que ter principalmente em conta as ferramentas de desenvolvimento e melhoria militares, de inteligência e de aqueles que suportam sistemas de comunicação estrategicamente importantes. Este último, em cooperação com os operadores privados. Para este tipo de ferramentas é desejável que a produção nacional tanto seja para gerar o know-how de conhecimento, bem como para aperfeiçoar a blindagem no quadro local.

- A proteção física do patrimônio tecnológico. DONALDSON, SIEGEL, WILLIAMS e ASLAM (2014) consideram que os sistemas de infra-estruturas empregados em cibersegurança representam um ponto extremamente vulnerável como portas de entrada para o sistema ou como peças necessárias para o funcionamento harmonioso. A proteção física de tal patrimônio tecnológico também é essencial para alcançar a resistência desejada.
- Formação e especialização de capital humano. Segundo HOUGH, MALIK, MORAN e PILBEAM (2015), e necessária a formação contínua e permanente de capital humano para adquirir a experiência necessária para a tarefa. Ambiente profissional qualificado e com níveis extremos de conhecimento sobre as diferentes capas de segurança.
- Implementação e atualização das estratégias de ciber-resiliência (ciclo de vida). CORLETTI ESTRADA (2017) considera que essas estratégias devem ser aplicadas à segurança de rede, nós e áreas, formando uma defesa cibernética em profundidade e altura. Planos de gestão de segmentação e serviços de rede. Estratégias tais como seguir e prosseguir ou proteger e proceder. Ou seja, todo o procedimento e as ações apropriadas para a implementação que salvaguarde e permitirá que a organização possa retornar a um estado operacional no menor tempo possível. Então será necessário adaptar todo o conjunto de medidas que estão disponíveis para a organização em intervalos apropriados (ciclo de vida).
- Dotação orçamental suficiente. Em referência com essa condição, a maioria da bibliografia consultada reforça a necessidade de contar com o orçamento adequado para a renovação e atualização de recursos humanos e materiais contínua para garantir a resiliência do cyber.

Todos esses condicionantes devem ser avaliados por expertos e especialistas no campo cibernético para definir qual seria o modelo de ciber-resiliência mais eficiente para ser implementado.

Mas a história demonstra que um modelo aplicável numa região determinada pode não dar certo em outra região, por diversas questões subjacentes, tanto endógenas como exógenas nesse ambiente. É por isso, que empregando a técnica de Policy Transfer, tomando como referência ao DOLOWITZ e MARSH (2000), se procurará transferir esse modelo à América do Sul, cuja realidade é suficientemente diferente à da Europa como para que possa ser importada diretamente.

Na sua obra, DOLOWITZ e MARSH afirmam que o marco atual se organiza em torno das seguintes perguntas:

- Por que os atores participam em transferência de políticas?
- Quem são os atores clave envolvidos no processo de transferência de políticas?
- O que se transfere e de onde se extraem lições?

- Quais são os diferentes graus de transferência?
- Que restringe ao estado em instalar o processo de transferência de políticas?
- Como é o processo de transferência de políticas relacionadas com a política de “êxito“ ou a política do “fracasso”?

A realidade da UNASUL e do Conselho de Segurança Sulamericano distam muito da realidade da OTAN. A UNASUL na atualidade não possui presidente, não está gerando normativa nenhuma, e vários dos seus países membros estão em suspenso de continuar com sua participação nessa organização. Essa realidade regional, que dista muito do esperado e do ambiente em que vêm se aplicando as medidas de segurança cibernéticas detalhadas (Europa), é que se pretende trabalhar para arribar em conclusões de relevância.

2.2 METODOLOGIA

Esta seção apresentará a metodologia que solucionará os problemas a serem pesquisados, identificando as atitudes necessárias para atingir os objetivos elencados. Para isso haverá uma seqüência organizada em: Tipo de Pesquisa, Universo e Amostra e Coleta de Dados.

Portanto, utilizando a Taxionomia de Vergara (2009), por meio de uma pesquisa qualitativa, procurou-se compreender as evidências da situação do estado da arte no mundo (em caráter geral) referido ao ambiente cibernético, a necessidade entender e criar um modelo ciber-resiliente à luz das experiências adquiridas pelo Centro de Excelência e Cooperação de Ciber Defesa da OTAN, e a possibilidade (ou não) de exportar esse modelo à América Latina.

2.2.1 TIPO DE PESQUISA

Para a realização do presente trabalho, as publicações mais recentes apresentadas no mundo referentes ao objeto de estudo serão exploradas e analisadas para extrair conclusões de ordem descritivas que possibilitem a posterior análise da realidade regional da América do Sul aos efeitos de contribuir à criação de um modelo que seja aplicável conseguindo assim a melhor articulação lógica possível para detectar as vulnerabilidades dos próprios sistemas diante das ameaças cibernéticas.

Será empregado como ferramenta metodológica o Mapeamento de Processos (Process Tracing) para, a partir da análise dos mecanismos causais, darmos solução ao problema de pesquisa.

O process tracing emerge como método para se auferir o poder explicativo de estudos históricos através da sistematização clara das evidências, seguindo alguns preceitos contidos na tradição quantitativa, abrangendo questões como a equifinalidade, gerando explicações para mecanismos causais e validando hipóteses. Em última instância, consiste em um conjunto de ferramentas e testes para investigar inferências causais a partir de dados qualitativos. FURTADO RODRIGUES, STROPPA RODRIGUES (2017).

Mesmo a pesquisa seja eminentemente qualitativa, também será empregue o método qualitativo a partir da realização de questionários a expertos e especialistas para, logo da análise dos resultados, arribarmos em conclusões sobre a relevância de cada componente do mecanismo causal criado.

MAHONEY e GOERTZ (2006) afirmam que a pesquisa quantitativa é aquela da que se recolhe e analisam dados quantitativos sobre variáveis. A pesquisa qualitativa evita a quantificação. Os pesquisadores qualitativos fazem registros narrativos dos fenômenos que são estudados mediante técnicas como a observação participante e as entrevistas não estruturadas. A diferencia fundamental entre as metodologias é que as quantitativas estudam a associação ou relação entre variáveis quantificadas e a qualitativa o faz em contextos estruturais e situacionais.

A pesquisa qualitativa tenta identificar a natureza profunda das realidades, seu sistema de relações, sua estrutura dinâmica. A pesquisa quantitativa tenta determinar a força de associação e correlação entre variáveis, a generalização e objetivação dos resultados a traves de uma amostra para fazer inferência em uma população da qual toda amostra procede. Trás o estudo da associação e correlação pretende, a sua vez, fazer inferência causal que explique por que as coisas acontecem ou não de uma forma determinada.

Também será empregada a técnica baseada na literatura de “Policy Transfer” para intentar trazer o modelo gerado para a Europa à região de América Latina e corroborar sua compatibilidade ou incompatibilidade e, em vista à realidade regional, procurar as adaptações necessárias se for o caso.

O Policy Transfer é amplamente entendido como um processo mediante o qual o conhecimento das políticas, disposições administrativas, instituições e idéias em um sistema político (passado ou presente) se utilizam no desenvolvimento de características similares em outro (BENSON, 2000).

2.2.2 UNIVERSO E AMOSTRA

O universo pesquisado será composto por os atores estatais (Forças Armadas Argentinas, Brasileiras, Colombinas, Espanholas, Inglesas e Alemãs), inter-estatais (OTAN, UNASUR) e não estatais (Centro de Excelência Cibernética de Estônia) que interferem significativamente no ambiente cibernético, entre o período 2007 até 2018. A amostra utilizada segue a linha não probabilística por não contemplar procedimentos estatísticos, justificada pela gama de fontes de pesquisa disponíveis a serem utilizadas.

2.2.3 COLETA DE DADOS

Para o Primeiro, Segundo e Quarto Objetivos Específicos, a pesquisa será realizada por meio de busca bibliográfica em livros, revistas especializadas e artigos acadêmicos, observações das participações em conferências e seminários.

Para o Terceiro Objetivo Específico, serão coletados os dados a partir da distribuição de um questionário para especialistas e expertos na área da Ciberdefensa. Os resultados obtidos serão analisados para arribar a conclusões de relevância.

3 **CRONOGRAMA**

Atividade	**2018**			**2019**		
	Abr / Mai	**Jun / Ago**	**Sep / Dic**	**Ene / Mar**	**Abr / Jul**	**Ago / Nov**
Confecção do pré-projeto de pesquisa	X					
Depósito do pré-projeto de pesquisa	X					
Levantamento e Seleção de bibliografia	X	X	X	X	X	
Depósito do Projeto de Pesquisa	X	X	X			
Pesquisa bibliográfica e documental	X	X	X	X	X	
Análise e Consolidação dos dados bibliográficos	X	X	X	X	X	
Análise dos dados da pesquisa	X	X	X	X	X	
Qualificação				X		
Confecção dos capítulos		10%	30%	55%	80%	100%

Confecção da conclusão				20%	60%	100%
Avaliação pela banca						X
Depósito da Monografia						X

REFERÊNCIAS

_____. **Protecting Our Future - Educating a Cibersecurity Workforce**. Columbia: Hudson Whitman Exelsior Collage Press, 2013.

_____. **Cybersecurity - Protecting Critical Infraestructures from Cyber Attack and Cyber Warfare**. Florida: CRC Press Taylor and Francis Group, 2015.

_____. **Cyber Security : Analytics , Technology and Automation**. London: Springer, 2015.

_____. **The Virtual Battlefield: Perspectives on Cyber Warfare. Cryptology and Information Security Series**. 3rd Volume ed. Amsterdam: IOS Press, 2009.

_____. **Cyberinfrastructure Technologies and Applications**. New York: Nova Science Publishers, Inc., 2009.

_____. The State of Industrial Cybersecurity 2017. **Business Advantage - Intelligence Insight Innovation**, 2017.

_____. **Cyber Warfare: Building the Scientific Foundation**. New York: Springer, 2015.

_____. **Intelligent Methods for Cyber Warfare**. New York: Springer, 2015.

_____. **The Oxford Handbook Of International Relations**. New York: Oxford University Press, 2008.

_____. **Problems and Methods in the Study of Politics**. New York: Cambridge University Press, 2004.

_____. **Cyberwar and Information Warfare**. London: Wiley, 2011.

_____. **Cyber Situational Awareness: Issues and Research**. New York: Springer, 2010.

_____. **Tallinn Manual on the International Law Appicable to Cyber Warfare**. New York: Cambridge University Press, 2013.

_____. **The Virtual Battlefield: Perspectives on Cyber Warfare**. Amsterdam: IOS Press, 2009.

_____. **Cyber Security and Privacy**. Athenas: Springer, 2014.

_____. Critical Infraestructure Protection II IFIP. Oklahoma: Springer, 2008.

_____. Path to Cyber Resilience: Sense, Resist, React. **EY´s 19th Global Information Security Survey 2016-2017**, 2017.

_____. **Critical Infrastructure: Reliability and Vulnerability**. New York: Springer, 2007.

_____. **The Oxford Handbook of Quantitative Methods - Volume 2 Statistical Analysis**. Volume 2- ed. New York: Oxford University Press, 2013.

_____. **An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks**. New York: Springer, 2011.

_____. **The Oxford Handbook of Quantitative Methods - Volume 1 Foundations**. New York: Oxford University Press, 2013.

_____. **Advances in Information Security: Global Initiatives to Secure Cyberspace. An Emerging Landscape**. New York: Springer, 2009.

_____. **Cyberspace and National Security - Threats, opportunities and Power in a Virtual World'**. Washington, DC: Georgtown University Press, 2012.

_____. **Cyberspace Security and Defense: Research Issues**. [s.l.] NATO Sciences Series, 2004.

_____. **Cyber Defense and Situational Awareness**. New York: Springer, 2014.

_____. **Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners**. Washington, DC: Elsevier, 2014.

_____. **Cyber Warfare: Building the Scientifics Foundation**. New York: Springer, 2015.

ALLEN, G.; CHAN, T. Artificial Intelligence and National Security. **Belfer Center for Science and International Affairs**, p. 132, 2017.

ANDRESS, J.; WINTERFELD, S. **Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners**. Amsterdam: Elsevier, 2011.

ARDITA, J. CORLETTI ESTRADA, Alejandro. **Ciberdefesa Nacional.** Madrid, Espanha: Darfe.es, 2016.

BEACH, D. **Process- Tracing Methods : Foundations and Guidelines**. First ed. Michigan, United States of American: The University Michigan Press, 2013.

BEACH, D. It ' s all about mechanisms – what process-tracing case studies should be tracing should be tracing. **New Political Economy**, v. 3467, n. February, 2016.

BEAUDOIN, L.; JAPKOWICZ, N.; e MATWIN, S. **Autonomic Computer Network Defence Using Risk State and Reinforcement Learning**. New York: Cryptology and Information Security Series, vol.3, pp.238-248, 2009.

BENNET, B. **Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infraestructure and Personnel**. New Jersey: Wiley - Interscience, 2007.

BENSON, D. ¿Qué hemos aprendido de Investigación de la transferencia de políticas? Dolowitz y Marsh Revisited. v. 2011, p. 366–378, 2011.

BÜTHE, T. Temporality Seriously : Modeling History. **The American Political Science Review**, v. 96, n. 3, p. 481–493, 2012.

CARAYANNIS, E. G.; CAMPBELL, D. F. J. **Cyber- Development , Cyber-Democracy and Cyber-Defense; Challenges, Opportunities and Implications for Theory, Policy and Practice**. New York: Springer, 2014.

CARRASCO, L. **Ciber-Resiliencia.** Madrid, Espanha: Instituto Espanhol de Estudos Estratégicos, 2015.

CHENG, D. **Cyber Dragon: Inside China´s Information Warfare and Cyber Operations**. Denver: Praeger, 2017.

COLLIER, D. Understanding Process Tracing. **PS: Political Science and Politics**, v. 4, n. 4, p. 823–830, 2011.

CORLETTI ESTRADA, A. **Estratégia de segurança informática por camadas, aplicando o conceito de Operação Militar por Ação Retardante**. Madrid, Espanha: Tese de Doutorado Universidade Nacional de Educação a Distância - Escola Técnica Superior de Engenharia Informática, 2011.

CORLETTI ESTRADA, A. **Ciberseguridad: Una Estrategia Informático-Militar**. Primeira ed. Madrid: DarFe, 2017.

CRUZ JÚNIOR, S. A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégicas dos Estados Unidos, Rússia e Índia para o Espaço Virtual. **Governo Federal - Secretaria de Assuntos Estratégicos da Presidência da República**, 2013.

DOLOWITZ, D. P.; MARSH, Y. D. Learning for abroad : The rule of policy transfer in the actual politics decitions. v. 13, n. 1, 2000.

DONALDSON, S.; SIEGEL, S.; WILLIAMS, C.; ASLAM, A. **Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats**. New York: [s.n.].

EASTON, D.; JOHN, G.; GRAZIANO, L. **The Debelopment of Political Science - A comparative survey**. London: Routledge, 1991.

ECONOMY, T. P.; POWERS, S. M.; JABLONSKI, M. **The Real Cyber War**. Urbana, Chicago and Sprinfield: University of Illinois Press, 2015.

ERBSCHLOE, M. **Information Warfare - How to Survive Cyber Attacks**. New York: Mc Graw Hill Education, 2001.

EVERA, S. VAN. **Guide to Methods for Students of Political Science**. London: Cornell University Press, 1997.

FALLETI, T. A Sequential Theory of Descentralization: Latin American Cases in Comparative Perspective. **American Journal of Political Science**, v. 99, n. 3, p. 327–346, 2005.

FIGONI, P. **BAKING Exploring the Fundamentals of Baking Science**. Second Edi ed. New Jersey: John Wiley and Sons, Inc., 2008.

FITZGERALD, C. W.; BRANTLY, A. F. Subverting reality: The role of propaganda in 21st century intelligence. **International Journal of Intelligence and CounterIntelligence**, v. 30, n. 2, p. 215–240, 2017.

FRANKE, T. L. How Technology Will Shape Our Future: Three Views of the Twenty-First Century. v. 2008, n. 2, 2008.

FURTADO RODRIGUES, K.; STROPPA RODRIGUES, I. Process tracing: o método, inovações e perspectivas para o campo da Administração Pública. **V Encontro Brasileiro de Administração Pública - Universidade Federal de Viçosa**, p. 15, 2017.

GAMERO, A. **Cyber Conflicts in International Relations: Framework and Case Studies.** Estados Unidos: Seminario sobre “Cyber International Relations”, 2014.

GEERS, K. **Strategic Cyber Security. NATO Cooperative Cyber Defense Centre of Excelence**. Estônia: Seminário, 2011.

GEORGE FRIEDMAN. **The next 100 years. A Forecast for the 21. century**. [s.l: s.n.].

GEORGE, A. L.; BENNETT, A. Case studies and theory development in the social sciences. **Case Studies and Theory Development in the Social Sciences**, v. 70, p. 331, 2005.

GERRING, J. **Case Study Research - Principles and Practicles**. New York: Cambridge University Press, 2007.

GOERTZ, G. **Social Science Concepts - A Users Guide**. New Jersey: Princeton University Press, 2006.

GRAGIDO, W.; PIRC, J. **Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats**. New York: Elsevier, 2011.

GUEDES DE OLIVEIRA, M.; DE CONTI PAGLIARI, G.; MARQUES, A.; PORTELA, L.; BENTO FERREIRA NETO, W. **Guia de Defesa Cibernética na América do Sul**. Pernambuco: Editora UFPE, 2017.

GUIGNON, C. **Heidegger and the problem of knowledge**. Indiana: Hackett Publishing Company, 1983.

HARRINGTON, A.; THEOHARY, C. **Cyber Operations in DOD Policy and Plans: Issues for Congress. Congressional Research Service. CRS Report – Prepared for Members of Commitees of Congress.** Estados Unidos: Congresso dos Estados Unidos, 2015.

HILL, J.; MARION, N. **Introducton to Cybercrime: Computer Crimes, Laws, and Policing in the 21 st Century**. California: Praeger, 2016.

HOUGH, P; MALIK, S.; MORAN, A.; PILBEAM, B. **International Security Studies: Theory and Practice**. London, 2015.

HYSLIP, T. S. **Bit Wars: cyber crime, hacking and information warfare**. [s.l.] Cover Art, 2015.

JANCZEWSKI, L.; COLARIK, A. **Cyber Warfare and Cyber Terrorism**. New York: Information Science Reference, 2008.

KELLSTEDT, P.; WHITTEN, G. **The Fundamentals of Political Science Reserarch**. Second Edi ed. New York: Cambridge University Press, 2013.

KLIMBURG, A. **National Cyber Security: Framework Manual**. Estonia: NATO Cooperation Cyber Defense Centre of Excelence, 2014.

KNAPP, E. **Industrial Network Security: Securing Critical Infraestructure Networks for Smart Grid, SCADA, and Other Industrial Control System**. New York: Elsevier, 2011.

KRAMER, F.; STARR, S.; WENTZ, L. **Cyberpower and National Security. Center for Technology and National Security Policy.** Estados Unidos: National Defense University Press, 2009.

KUHN, T. **The Structure of Scientific Revolutions**. 3rd. ed. Chicago: The University of Chicago Press, 1996.

KUO, M. **Cibersecurity in US Asia Policy**. Estados Unidos: The Diplomat, 2016.

LEE, N. **Counterterrorism and Cybersecurity: Total Information Awareness**. New York: Springer, 2013.

LIBICKI, M. **Ciberdeterrence and Cyberwar**. Estados Unidos: Rand Corporation, 2009.

LINKOV, I. (ED.). **Managing Critical Infrastructure: Decision Tools and Applications for Port Security**. San Francisco: Springer, 2006.

MAHONEY, J; RUESCHEMEYER, D. **Comparative Historical Analysis in the Social Sciences**. New York: Cambridge University Press, 2003.

MAHONEY, J.; GOERTZ, G. A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research. n. 0093754, p. 227–249, 2006.

MAHONEY, J. Process Tracing and Historical Explanation. **Security Studies**, n. July, 2015.
MAUDE, F. La Estrategia de Seguridad Cibernética del Reino Un Proteger y promover el Reino Unido en un mundo digital. 2011.

MCQUADE, S. C. **Encyclopedia of Cybercrime**. London: Greenwood Publishing Group, 2009.

MINTZBERG, H. **Mintzberg on Management: Inside our Strange Word of Organizations**. New York, The Free Press, 1989.

MORETTIN, P. **Estadística Básica**. 6ta Ed ed. São Paulo: Editora Saraiva, 2010.

NEMATI, H.; YANG, L. **Applied Cryptography for Cyber Security and Defense : Information Encryption and Cyphering**. New York: Information Science Reference, 2011.

NEWMEYER, K. **Ciberespaço, Cibersegurança e Cyberwar**. Lima, Perú: II Simpósio Internacional de Segurança e Defesa, 2015.

NETO, O., A.; COSSIO RIDRIGUEZ, J., C. O novo método histórico-comparativo e seus aportes à ciência política e à administração pública. **Revista de Administração Pública**, v. 50, n. 6, p. 1003–1027, 2016.

PELTON, J.; SINGH, I. **Digital Defense: A Cybersecurity Primer**. New York: Springer, 2015.

PIEDRA, D. Lecciones de aprendizaje, transferencia de políticas y la difusión internacional de la política Ideas. **Centrer for the Study of Globalisation and Regionalisation**, p. 41, 2001.

RELIA, S. **Cyber Warfare: Its Implications on National Security**. New Delhi: Vij Books India Pvt Ltd, 2015.

RICHARDS, J. **Cyber-War: The Anatomy of the Global Security Threat**. London: Palgrave Pivot, 2014.

RID, T. **Cyber War Will Not Take Place -**. New York: Oxford University Press, 2013.

RITCHIE, J.; LEWIS, J. **Qualitative Research Practice - A guide for Social Science Students and Researchers**. London: SAGE Publications, 2003.

ROSENZWEIG, P. **Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World**. California: Praeger, 2013.

ROWLAND, J.; RICE, M.; SHENOI, S. The anatomy of a cyber power. **International Journal of Critical Infrastructure Protection**, v. 7, n. 1, p. 3–11, 2014.

SAMPIERI, R.; FERNÁNDEZ COLLADO, C.; BAPTISTA LUCIO, P. **Metodología de la Investigación**. 6ta Ed ed. México DF: Mc Graw Hill Education, 2014.

SANTOS, D.; CARVALHO, B.; CAVALCANTE, S. **Segurança de infraestruturas críticas no Brasil**. Brasilia: [s.n.].

SAXONHOUSE, A. **Fear of Diversity: The Birth of Political Science in Ancient Greek Thought**. Chicago: The University of Chicago Press, 1992.

SCHNEIDER, B. **Battlefield of the Future: 21St Century Warfare**. Third Edit ed. Alabama: Air University Press, 2001.

SEAWRIGHT, J.; GERRING, J. Case Selection Techniques in Case Study Research. **Political Research Quarterly**, v. 61, n. 2, p. 294–308, 2008.

SENGE, P. **La quinta disciplina en la práctica: estrategias y herramientas para construir la organización abierta al aprendizaje.** Buenos Aires, Ediciones Granica S.A, 2006.

SILVA, C. E. M. V. DA. A transformação da guerra na passagem para o século XXI. Um estudo sobre a atualidade do paradigma de Clausewitz. p. 158, 2003.

SILVA, H. **Ataques virtuais e segurança informática**. Buenos Aires, Argentina: Escola Superior de Guerra Naval, 2013.

SINGER, P; FRIEDMAN, A. **Cybersecurity and Cyberwar - What everyone Needs to Know**. New York: Cambridge University Press, 2014.

SOUZA, C. F. DE. **Relações Federativas de Poder: Uma análise histórico-comparativa do Brasil**. [s.l.] FGV - EBAPE, 2017.

STARBUCK, W. **The Production of Knowledge - The Challenges of Social Science Research**. New York: Oxford University Press, 2006.

STEWART, J. M.; CHAPPLE, M.; GIBSON, D. **Certified Information Systems-Security Professional Study Guide**. Seventh Ed ed. Indiana: Sybex- A Willey Brand, 2015.

TEUMIM, D. **Industrial Network Security**. Second ed. [s.l.] ISA, 2010.

UZAL, R. **Cyber War: um desafio para a Defesa Nacional.** Buenos Aires, Argentina: Revista de Visão Conjunta Nº 7, 2014.

WATTS, B. **Clausewitzian Friction and Future War**. Revised Ed ed. Washington, United States of American: Institute for National Strategic Studies - National Defense University, 2004.

WICKHAM-CROWLEY, T., P. A qualitative comparative approach to latin American revolutions. **International Journal of Comparative Sociology**, v. 32, n. 1–2, p. 82–109, 1991.

WINTERFELD, S.; ANDRESS, J. **The Basics of Cyber Warfare**. [s.l.] Elsevier, 2013.

WOLFSON, T. **DIGITAL The Birth of the Cyber Left**. Urbana, Chicago and Sprinfield: University of Illinois Press, 2014.

WROBEL, L.; WROBEL, S. **Disaster Recovery Planning for Communications and Critical Infrastructure**. Boston: Artech House, 2009.

XUE, M.; ROY, S.; WAN, Y.; DAS, S. **Handbook on Securing Cyber-Physical Critical Infrastructure**. [s.l.] Elsevier, 2012.