UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS TRINDADE
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

Gabriel Olegário

Perspectivas político-estratégicas da Guerra Híbrida:

Uma análise das respostas estratégicas da República Tcheca contra ameaças híbridas

Florianópolis
2022

Perspectivas político-estratégicas da Guerra Híbrida:

Uma análise das respostas estratégicas da República Tcheca contra ameaças híbridas

Trabalho de Conclusão do Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Relações Internacionais.
Orientadora: Prof.ª Dra. Graciela de Conti Pagliari

Florianópolis

2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Olegário, Gabriel
Perspectivas político-estratégicas da Guerra Híbrida : Uma análise das respostas estratégicas da República Tcheca contra ameaças híbridas / Gabriel Olegário ; orientadora, Graciela de Conti Pagliari, 2022.
96 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Sócio Econômico, Graduação em Relações Internacionais, Florianópolis, 2022.

Inclui referências.

1. Relações Internacionais. 2. Guerra híbrida. 3. República Tcheca. 4. Resposta-Estratégica. 5. Relações Internacionais. I. de Conti Pagliari, Graciela . II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Gabriel Olegário

Perspectivas político-estratégicas da Guerra Híbrida:
Uma análise das respostas estratégicas da República Tcheca contra ameaças híbridas

Florianópolis, 04 de março de 2022.

O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

_____

Prof. Danielle Jacon Ayres, Dr.

Universidade Federal de Santa Catarina

_____

Prof. Jessica Maria Grassi

Universidade Federal de Santa Catarina

Certifico que esta é a versão original e final do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora.

Documento assinado digitalmente
GRACIELA DE CONTI PAGLIARI
Data: 13/03/2022 14:04:04-0300
CPF: 659.263.070-15
Verifique as assinaturas em https://v.ufsc.br

_____

Prof. Graciela de Conti Pagliari, Dr.

Universidade Federal de Santa Catarina

Orientadora

AGRADECIMENTOS

O amor fraterno é um dos pilares mais importantes da nossa vida, ensinando-nos o bem e o mal, o correto e o errado, e portanto agradeço aos meus pais por pensar na minha educação, no meu bem-estar e na minha independência como ser humano. Mesmo que entre nós existam oceanos a serem percorridos, posso sentir o apoio mesmo em diferentes continentes, pois sem vocês eu nada seria.

Acredito que nós somos a soma de todas as pessoas que perpassam em nossa vida, e deixo aqui meu agradecimento a todos os professores e amigos da UFSC que sempre acreditaram no meu potencial como internacionalista. Cada conversa e cada conselho foram importantes para eu chegar nessa lauda de agradecimentos que escrevo, e se as páginas de nossas vidas são preenchidas por narrativas e histórias, agradeço por fazer parte desta.

A Universidade Federal de Santa Catarina me proporcionou possibilidades que nunca pensei que seriam possíveis, e por mais que a Universidade Pública tenha muitas falhas, é apenas com diálogo e construção que poderemos transformar o país. Penso com muito carinho e eudaimonia os cinco anos de UFSC que pude beber dessa fonte inesgotável de conhecimento, iluminando o atual caminho que percorro na busca da vida que vale a pena ser vivida.

Deixo registrado aqui também a imensa gratidão a admiração que tenho pela minha orientadora, Graciela de Conti Pagliari, que é uma entusiasta das Relações Internacionais por excelência. Obrigado por ser uma docente que exige e requer pensamento crítico, análise e dedicação tanto nas aulas quanto nas orientações para a conclusão deste trabalho.

Agradeço também à Universidade de Hradec Králové por me proporcionar um ambiente de crescimento acadêmico e profissional, em especial à Martina e ao Josef, espelhos que tento seguir pela sua sabedoria, profissionalismo, paciência e dedicação com os estudantes internacionais. Agradeço por confiarem e acreditarem na minha pessoa.

Este trabalho é dedicado a minha estadia na República Tcheca, que me abraçou e me mostrou que a vida é o que fazemos dela. Obrigado por me oferecer uma segunda casa, sempre de braços abertos e hospitaleiros prontos para me surpreender das formas mais inóspitas.

Além da República Tcheca, a conclusão desse trabalho se deu na Finlândia, na antiga capital chamada Turku. Agradeço à Finlândia, ao *Migration Institute of Finland* e a minha supervisora, minha chefe, e amiga Saara Pellander. Sem você eu nunca teria acreditado tanto no meu potencial como profissional, acadêmico e ser humano. Todas as suas palavras, cafés e cervejas compartilhados me levaram a chegar nesse momento tão especial da minha vida.

Para concluir, afirmo que a gratidão é um dos sentimentos mais corteses que podemos ter perante a vida, compreendendo as limitações do mundo e a ambivalência do cárcere imperfeito da alma. Que a nossa humildade cósmica possa cada vez mais fazer-nos acreditar nas virtudes do diálogo, dos princípios democráticos e na educação por excelência, e cada vez mais desconstruir o mito do autoritarismo necessário.

"The salvation of this human world lies nowhere else than in the human heart, in the human power to reflect, in human meekness and human responsibility."

(Vaclav Havel)

RESUMO

Desde a primeira conceituação da Guerra Híbrida, em 2009, o termo vem sendo utilizado por políticos e acadêmicos para se referir a um novo conceito de estratégia bélica. Portanto, a utilização e definição do termo se faz importante, considerando a crescente literatura no âmbito acadêmico depois de 2014, com a anexação da Criméia pela Rússia. Esta monografia tem como objetivo demonstrar quais são as perspectivas político-estratégicas da República Tcheca na questão da Guerra Híbrida, descrevendo tanto como os documentos oficiais estabelecem relações com instituições supranacionais quanto às capacidades de defesa tchecas. Desta forma, torna-se importante a análise da natureza da OTAN e da UE, e posteriormente a investigação dos documentos que versam sobre a Guerra Híbrida das duas instituições supranacionais assim como a influência na formulação de políticas de defesa da República Tcheca. Metodologicamente, esse projeto de pesquisa tem um caráter exploratório, visto que será feita uma revisão das principais capacidades de defesa da República Tcheca, com a proposta de fornecer perspectivas e novos entendimentos das defesas contra ameaças híbridas. Analisar-se-á a relevância da dimensão cibernética e três das principais ameaças híbridas elencadas no entorno estratégico da República Tcheca. Conclui-se que as respostas estratégicas centradas apenas no Estado podem ser insuficientes, e o esforço conjunto com a sociedade é necessário para buscar o objetivo da "Sociedade Tcheca Resiliente 4.0".

Palavras-chave: Guerra Híbrida, República Tcheca, Ameaças Híbridas, Estratégia de defesa nacional.

ABSTRACT

Since the first conceptualization of Hybrid War, in 2009, the term has been used by politicians and academics to refer to a new concept of war strategy. Therefore, the use and definition of the term is important, considering the growing literature in the academic field after 2014, with the annexation of Crimea by Russia. This bachelor´s thesis aims to demonstrate the political-strategic perspectives of the Czech Republic on the issue of Hybrid War, describing both how official documents establish relationships with supranational institutions and Czech defense capabilities. In this way, it becomes important to analyze the nature of NATO and the EU, and later to investigate the documents that deal with the Hybrid War of the two supranational institutions as well as the influence on the formulation of defense policies in the Czech Republic. Methodologically, this research project has an exploratory character, as a review of the main defense capabilities of the Czech Republic will be carried out, with the proposal to provide perspectives and new understandings of defenses against hybrid threats. The relevance of the cyber dimension and three of the main hybrid threats listed in the strategic environment of the Czech Republic will be analyzed. It is concluded that strategic responses centered only on the State may be insufficient, and a joint effort with society is necessary to pursue the objective of the "Resilient Czech Society 4.0"

Key words: Hybrid Warfare, Czech Republic, Hybrid Threat, National Strategy Defense.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

O conceito de Guerra Híbrida é amplo e subjetivo o suficiente para diferentes interpretações sobre como o desenvolvimento tecnológico influencia os Estados a possuírem uma alternativa à guerra convencional. Desta forma, a definição concisa da Guerra Híbrida é importante tanto para a sociedade civil quanto para órgãos governamentais de segurança nacional, principalmente na formulação de políticas e legislação que engloba um conceito que ainda está em construção e em constante mudança (CLARKE; KNAKE, 2010).

A Guerra Híbrida tornou-se uma ameaça primária para a Segurança Europeia a partir da crise da Criméia no ano de 2014, que foi entendido como um ataque com meios convencionais e irregulares de guerra. Consequentemente, o ataque foi discutido amplamente tanto nos conselhos da União Européia quanto na OTAN, sendo que os países que mais tomaram iniciativas e que se sentiram ameaçados foram os países da Europa Central e do Leste Europeu (DANIEL; EBERLE, 2022).

Após a anexação da Criméia pela Rússia, durante a conferência da OTAN em 2016, o espaço cibernético foi reconhecido como um novo domínio operacional, assim como os domínios terrestre, naval e aéreo (República Tcheca, 2020). Partindo desse princípio, o conceito de Guerra Híbrida começa a tomar forma, sendo compreendido como um pilar importante na vulnerabilização dos Estados. Nesta dimensão, tanto o uso de *soft power* pode ser utilizado para influenciar psicologicamente a população (como o uso de desinformação, fake news e propaganda) quanto o *hard power*, já que a interrupção de processos industriais ou o dano à infraestrutura crítica de um país pode ser custoso (NYE, 2010).

Portanto, estabeleceu-se como objetivo geral realizar um estudo acerca de como a República Tcheca é influenciada pela ameaça da Guerra Híbrida, analisando como o país responde em matéria de defesa ao seu entorno estratégico. Desta forma, a problemática a ser respondida é: “Quais são as respostas estratégicas da República Tcheca para as principais ameaças híbridas relacionadas ao seu entorno estratégico?”. Para responder essa pergunta, será perquirido o conceito teórico de entorno estratégico e como a República Tcheca reconhece seu entorno estratégico por meio dos documentos oficiais de defesa do país.

O conceito de resposta estratégica será compreendido como uma análise das possíveis respostas estatais e não-estatais contra ameaças híbridas. Posteriormente, será analisada a estratégia de defesa da República Tcheca assim como a devida relação existente entre as

estratégias de defesa da OTAN e da União Europeia, já que ser membro dessas organizações impõe restrições à estruturas específicas. A hipótese que sustenta esse trabalho é: "Os desafios securitários, que emergem pelas relações regionais da República Tcheca, demandam abordagens político-estratégicas que abrangem a Guerra Híbrida em seu entorno estratégico".

Para buscar uma resposta satisfatória e completa para a pergunta desse Trabalho de Conclusão de Curso, dividir-se-á em três capítulos. O primeiro versará sobre como a evolução da geração de guerras influenciada pela criação da quinta dimensão (o ciberespaço), cria a possibilidade do uso sinergético de diferentes estratégias de guerra chamada *Guerra Híbrida.* Além da conceituação, será considerado como o entorno estratégico é um elemento importante para o emprego das ameaças híbridas, e a sua devida compreensão física e virtual. Após a análise da importância do entorno estratégico, serão analisados os documentos oficiais da República Tcheca e a sua devida reorientação estratégica de defesa.

Após a análise dos documentos oficiais da República Tcheca, e analisando o conceito de *retorno à Europa,* fica evidente a importância de instituições como a OTAN e a UE no direcionamento das estratégias de defesa da República Tcheca. Portanto, foram selecionados documentos e planos estratégicos da OTAN e da UE que versam sobre a Guerra Híbrida. Após a análise das duas instituições e de documentos chaves, analisa-se as perspectivas político-estratégicas da República Tcheca, compreendendo suas capacidades de defesa e as diretrizes das instituições supranacionais que a República Tcheca faz parte.

O capítulo três tem como objetivo a seleção das ameaças híbridas que foram discutidas nos capítulos anteriores e sinalizadas como problemáticas e frequentes pelo Serviço Secreto da República Tcheca. Portanto, foram selecionadas três frequentes ameaças híbridas e após cada especificação, é esquadrinhado como a República Tcheca securitiza e se defende de ameaças híbridas.

Quanto à metodologia, este projeto de pesquisa tem um caráter exploratório e uma abordagem hipotético-dedutiva, visto que será feita uma revisão das principais capacidades de defesa da República Tcheca, com a proposta de fornecer perspectivas e possíveis novos entendimentos das defesas contra ameaças híbridas. Compreendendo a difícil mensuração de forma quantitativa das ameaças híbridas, esse trabalho se fundamentou principalmente na análise qualitativa de como a República Tcheca se defende dessas ameaças, tanto por documentos oficiais quanto por respostas estratégicas.

Por fim, os resultados da pesquisa devem ser fonte para futuras pesquisas sobre as ameaças híbridas selecionadas, pois a relevância de tais vulnerabilidades se torna crescente com a dependência da sociedade em tecnologia. Assim, este Trabalho de Conclusão de Curso inicia com uma abordagem conceitual e teórica que se fundamenta em livros e artigos científicos, principalmente de autores e de instituições de pesquisa que são especializados na temática da Segurança Europeia e da República Tcheca. A seleção da bibliografia para o segundo e terceiro capítulo se fundamenta a partir da análise de documentos oficiais ratificados por órgãos de competência supranacional (como a OTAN e a EU) e de competência nacional tcheca, com os documentos oficiais em língua inglesa que podem ser encontrados publicamente na internet ou nos websites das devidas instituições.

2 DAS GERAÇÕES DE GUERRA À MUDANÇA DO ENTORNO ESTRATÉGICO PELA GUERRA HÍBRIDA

O presente capítulo tem como objetivo discutir como a geração de guerras, influenciada pelo fator do avanço tecnológico, gera uma possível estratégia sinergética de uso de todas as gerações de guerra chamada Guerra Híbrida. Depois, será apresentado como a criação do ciberespaço influencia e molda o conceito de Guerra de quinta geração. Posteriormente, será discutido como a Guerra Híbrida não é sinônimo das guerras de quinta geração, mas resultado da evolução das gerações de guerra e compostas por todas elas.

Ao final da subseção serão analisadas se as ameaças híbridas transformam a geografia física irrelevante, investigando se a geografia física é intrínseca ao entorno estratégico. Por fim, será compreendido como a República Tcheca percebe o seu entorno estratégico pelos documentos oficiais, tendo em mente que a República Tcheca reconhece em seus documentos oficiais a Guerra Híbrida como existente. Portanto, para definir a geração das guerras é necessário traçar cronologicamente a evolução da guerra e os principais fatores para as suas categorizações.

2.1 Definindo a geração das guerras

Assim que o mundo passou pela recente transformação com a queda da União Soviética e a devida mudança na geopolítica com o fim do mundo bipolar, muitos grupos étnicos e nacionais rapidamente viram a oportunidade de reconhecimento e liberdade. Portanto, são das transformações que o mundo apresenta que os atores inovam seus métodos e técnicas de guerra para conseguir seus objetivos ideológicos, nacionalistas ou políticos (WILLIAMSON, 2009). Para prosseguir com a conceituação da Guerra Híbrida, será analisado como a expansão do conceito de guerra está entrelaçado com a evolução das gerações de Guerra.

Desta forma, os elementos essenciais da guerra podem ser definidos como os novos domínios de conflito, a natureza dos adversários, a natureza dos objetivos e a natureza da força - para construir uma tipologia geracional de guerra e conflito que compõem as características da quinta geração de guerra. Portanto, podemos categorizar as mudanças nas características da guerra, principalmente pela dinâmica social, econômica, política e tecnológica que o mundo presenciou (REED, 2008).

Lind (1989) tenta compreender esse fenômeno de gerações de guerra e define que as gerações podem ser interpretadas como uma mudança qualitativa dialética. Um exemplo que o próprio autor cita é entender que as forças armadas da geração prévia nunca conseguiriam derrotar as forças da nova geração. Sendo assim, as forças armadas que utilizam o ciberespaço e a guerra informacional como novas ferramentas sempre terão vantagens sobre forças armadas que não possuem ou coordenam seu domínio operacional cibernético (LIND, 1989).

Em *Another Bloody Century: Future Warfare*, Gray (2006) descreve que as características da guerra, durante um período, são influenciadas mais pelos contextos políticos, sociais, e estratégicos tais que mudanças íntegras nas ciências militares. Outro autor que desenvolve a ideia de Lind (2004) de forma contemporânea, é Hammes (2004), descrevendo que a Guerra Moderna se desenvolveu por conta das mudanças políticas, econômicas, sociais e tecnológicas que ocorreram durante o tempo nas sociedades. Dessa forma, Hammes (2004) afirma que a guerra pode ser vista pela perspectiva da tipologia geracional, descrevendo quatro tipos de geração de guerra e propõe alguns padrões e características que tentam descrever a guerra de quinta geração.

Dessa forma, de acordo com Lind (1989) e Hammes (2004), os quatro tipos de geração de guerra são facilmente reconhecíveis. Pode-se considerar o início das guerras de primeira geração com a criação dos Estados-Nações e a paz de Westphalia. Iniciava-se a era moderna da guerra a qual os Estados guerreavam contra forças armadas de outros Estados-Nações para atingir os objetivos políticos necessários com a ajuda de mosquetes, táticas de linhas e colunas, formadas principalmente por uma massa de homens (REED, 2008).

A segunda geração de guerra foi desenvolvida pelos resultados da revolução industrial, além das melhorias qualitativas e quantitativas tecnológicas em poder de fogo como mosquetes estriados, culatras, metralhadoras e a melhoria das capacidades de fogo indireto da artilharia. Cronologicamente falando, a segunda geração de guerra começou a tomar forma no final da Guerra Civil Americana e chegou ao seu zênite com as guerras de trincheiras e os massacres ocorridos na Europa durante a Primeira Guerra Mundial (REED, 2008).

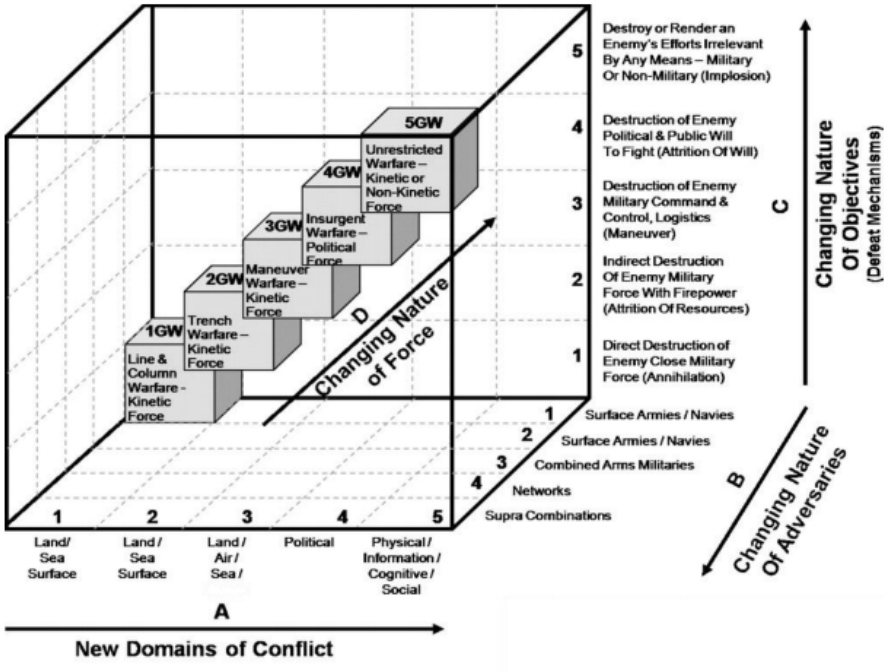
A terceira geração de guerra foi concebida pelos alemães durante a Primeira Guerra Mundial e logo depois introduzida pela Alemanha no começo da Segunda Guerra Mundial na conquista pela Europa. Desta forma, a terceira geração de guerra é caracterizada pela forças

armadas nas dimensões marítima, aérea, terrestre e informacional, tendo como foco o uso de manobras não-lineares para derrotar os inimigos por infiltração. A terceira geração de guerra tem sido uma das formas convencionais militares mais utilizadas por Estados-Nações modernos, principalmente os Estados Unidos da América (REED, 2008).

Segundo Reed (2008), as características da guerra de quarta geração concede uma vantagem dialética sobre a guerra de terceira geração e permitem que forças inferiores vençam forças superiores de tamanho ou armamento. Tal geração de guerra usa estratégia e táticas assimétricas, aplicadas por longos períodos de tempo, para desviar o foco da destruição das forças militares convencionais superiores de um inimigo - que ele não pode derrotar - e consequentemente, para a derrota da vontade política inimiga de lutar. Combina a força política de um oponente com a força política do outro. Hammes (2004) define a guerra de quarta geração como uma forma evoluída da guerra de insurgência. Tais mudanças também ocorreram na China, e dessa forma a aplicação moderna da quarta geração de guerra foi concebida por Mao Tsé Tung entre 1925-1927. A Revolução Chinesa sucedeu, derrotando as forças armadas nacionalistas de Chiang Kai-shek e instaurando um governo comunista na China.

Uma fonte primária do conceito foi identificada em um documento intitulado *Unrestricted War* dos coronéis Qiao Liang e Wang Xiangsui (2002), escrito em 1999 e publicado pelo *PLA Literature and Arts Publishing House*. O estudo lida com o que entendemos hoje por Guerra Híbrida, compreendendo o pensamento de encontrar maneiras novas de combater os oponentes e suas capacidades. É desta forma que o livro define a Guerra Irrestrita sendo uma guerra sem regras ou restrições, principalmente irrestritas e ilimitadas no sentido das regras que estão em jogo (WITHER, 2016). Portanto, a Guerra Irrestrita ignora e transcende os limites do campo de batalha e o que não é campo de batalha, entre o que são e do que não são armas, entre militares e civis, entre atores estatais e não-estatais (METZ, 2014). Desta forma, o lado que toma vantagem nesse tipo de combate são atores que não possuem capacidades iguais ou superiores às superpotências, dando oportunidades iguais para os lados combatentes do conflito.

Figura 1 - Modelo 3D do desenvolvimento das Gerações de Guerra



Fonte: Reed (2008).

Desta forma, como Lind (2004) indica, as guerras de quarta geração marcam o fim da era moderna da guerra e as guerras de quinta geração marcam o início da era pós-moderna, principalmente pelos ataques da Al-Qaeda no dia 9 de setembro de 2001. A ineficiência da guerra ao terror com medidas da guerra convencional contra células terroristas no Iraque e no Afeganistão definiram o início da era pós-moderna da Guerra. Para Liang e Xiangsui (2002) no livro *Unrestricted Warfare*, a guerra tomou conta da sociedade global de uma forma muito mais complexa, dificultando o reconhecimento e a luta contra tais ameaças modernas. Até agora, não existe nenhuma definição amplamente aceita para a quinta geração de guerra.

De acordo com Hammes (2004), alguns dos desenvolvimentos que abrangem a guerra de quinta geração são as mudanças políticas, econômicas, sociais e tecnológicas que empoderam grupos e indivíduos a lutar contra Estados-Nações. Todavia, Lind (2004) é mais pragmático na conceituação das guerras de quinta geração e afirma que não existe telescópio que possa chegar tão longe, ou seja, é muito difícil analisar como o avanço tecnológico vai alterar o futuro da Guerra. Portanto, tais grupos e indivíduos são passíveis de serem derrotados, principalmente pela implosão ou colapso de tais organizações. Os principais ataques a tais entidades compreendem a desconstrução do desenvolvimento de lideranças,

construção de alianças, divulgação pública ideológica, financiamento, materiais, proteção e apoio, recrutamento, doutrinação e treinamento de indivíduos, planejamento e alvos, movimento e operação e comunicação (LIND, 2004).

É importante pensar a possibilidade de aplicar força contra os grupos que estão dentro da Guerra de quinta geração, principalmente por que é necessário não apenas removê-los do campo de batalha físico, mas dissipar a um ponto que tais grupos não sejam mais reconhecíveis ou inexistentes, sendo importante no combate dessas ameaças. Logo, contra tais formas de ameaça a aplicação de força pode ser cinética ou não-cinética, tendo como objetivo a eliminação ou dissipação dos grupos combatentes (que podem estar combinados com atores estatais ou não) (REED, 2008).

Para Lind (2004) o conceito ainda está em construção e será necessário tempo para entendermos a definição final da guerra de quinta geração. Ainda, segundo o autor, a perda do monopólio da guerra e da organização social pelo Estado resultante do surgimento das guerras de quarta geração e o advento da Era Informacional altera tudo. Lind (2004) conclui que é impossível entendermos a complexidade das guerras de quinta geração no momento, mas que é possível traçar características em comum para as guerras modernas.

Todavia, mesmo que não possamos ter uma definição consensual das guerras de quinta geração, é ainda possível inferirmos algumas características. Desta forma, podemos compreender os domínios do conflito como:

> a) Domínio físico: O domínio tradicional da guerra a qual a força se move no tempo e no espaço. Compreende os domínios terrestre, marítimo, aéreo e espacial a qual a maioria das forças convencionais de guerra atuam;
>
> b) Domínio Informacional: O domínio o qual a informação é criada, manipulada e compartilhada, compreendendo o espaço cibernético;
>
> c) Domínio cognitivo: compreende as intenções, doutrinas, táticas, técnicas e processos existentes e onde conceitos decisivos emergem;
>
> d) Domínio Social: compreende os elementos necessários de qualquer empreendimento humano. É o domínio o qual os humanos interagem, trocam informações, compartilham entendimentos e conhecimento e fazem decisões colaborativas que compreendem também a construção da cultura, religião, valores, atitudes, crenças e decisões políticas que se relacionam com a vontade da comunidade (REED, 2008, p. 692, tradução própria).

Para Gray (2006), perigo, emprego da força, incerteza e sorte permanecerão como características da Guerra, todavia ele enfatiza que adversários inteligentes buscam vulnerabilidades nas forças armadas convencionais. Por exemplo, é muito provável que a

maioria dos inimigos dos Estados vão continuar sendo tão assimétricos quanto eles tem sido durante os últimos quinze anos.

A expansão dos domínios de guerra faz possível a expansão exponencial do conceito de campo de combate além do domínio físico, pois remove os limites geográficos e políticos, permitindo a sua onipresença. Desta forma, a compreensão dos limites do campo de batalha é importante para Liang e Xiangsui (2002), que afirmaram que ele está em todos os lugares.

Portanto, se o futuro dos conflitos será onipresente, ou seja, em todos os domínios que os Estados podem exercer poder, a conceituação da Guerra Híbrida é importante para reconhecermos quais as possíveis ameaças híbridas os Estados estão vulneráveis. A busca de uma definição não é algo meramente formal, todavia necessário para os Estados estarem em pronto-emprego para a identificação dos possíveis ataques híbridos. Essa expansão do conceito de Guerra e sua devida evolução faz com que seja possível entendermos a Guerra Híbrida tendo como base o avanço tecnológico. Desta forma, prosseguiremos com a definição de Guerra Híbrida.

2.2 Definindo a Guerra Híbrida

A conceituação de Guerra Híbrida pode ser conflituosa pela diversidade de definições possíveis, principalmente por ser um termo que ainda está sendo construído e modificado. Portanto, o desenvolvimento tecnológico e informacional são fatores importantes na modificação do conceito de Guerra Híbrida, pois as ameaças híbridas são complexas e podem ser combinadas para vulnerabilizar a soberania de um Estado (WITHER, 2016).

Para um dos primeiros estrategistas que escreveram sobre o conceito como Hoffman (2009), buscar uma definição própria para o termo Guerra Híbrida é essencial, pois apenas assim os Estados conseguem desenvolver políticas e estratégias de defesa centradas em ameaças híbridas, e dessa forma, conseguem se preparar melhor para diferentes ataques internos externos (HOFFMAN, 2009).

Para Mansoor (2012, p. 42), o termo Guerra Híbrida pode ser definido como “o uso de forças convencionais e irregulares na mesma campanha militar, os quais podem incluir tanto atores estatais e não-estatais, em busca de um objetivo político”. Todavia, uma das falhas

dessa definição é diferenciar das guerras convencionais, já que a inclusão de meios não-militares também faz parte da competição conflituosa interestatal (WITHER, 2016).

As guerras napoleônicas e a Alemanha nazista durante a Segunda Guerra Mundial são exemplos do uso de meios não-militares, como propaganda, desinformação e notícias falsas para ganhar vantagens sobre o inimigo. O uso de meios não-militares é associado com as novas tecnologias desenvolvidas tanto para uso militar, quanto para o uso civil, que acabam fazendo parte dos domínios operacionais que os Estados disputam poder (HOFFMAN, 2009).

Buscando formas mais robustas para definir Guerra Híbrida, o Departamento de Defesa Estadunidense publicou em 2010 um relatório chamado *Quadrennial Defense Review Report*:

> [...] As abordagens híbridas atuais podem envolver Estados adversários que acionam formas de guerra prolongadas, como forças alternativas coercitivas, ou atores não-estatais, e a utilização de conceitos operacionais e capacidades de ponta tradicionalmente associadas com Estados[...] (USA, 2010 p.8, tradução própria).

Ainda que essa seja a definição Estadunidense nos documentos oficiais do Departamento de Defesa, um dos desafios para a conceituação é que a terminologia da Guerra Híbrida acaba por se sobrepor com outros conceitos, como por exemplo - a Guerra assimétrica, não-convencional, não-linear, guerras de nova geração (quarta ou quinta geração), guerra política, guerra informacional - que acabam por dificultar a classificação entre estrategistas e estudiosos do Século XXI. A Guerra Híbrida pode ser entendida como um conceito ocidental, pois os analistas russos utilizam termos como *guerras de nova geração* ou *guerras não-lineares* quando escrevem sobre o assunto (WITHER, 2016).

Hoffman (2009) conceituou a Guerra Híbrida como uma zona entre conflitos de baixa-intensidade e conflitos de alta-intensidade, pois considera que a Guerra Híbrida esteja entre o espectro de paz e guerra. Um dos pontos centrais de tipificar a Guerra Híbrida é entender se os Estados que sofrem ataques híbridos estão em Estado de Guerra ou não. Seguindo Campbell “toda tentativa de colocar sentido no mundo e de representá-lo é sempre um ato de interpretação” (CAMPBELL, 2013, p.223). Desta interpretação, compreendemos que a tipificação do Estado de Guerra é crucial pela dinâmica que os Estados tomam a partir da interpretação da ameaça.

Com uma visão mais construtivista, Rosa Brooks sugere que “Guerra é qualquer coisa que os super-poderes dizem que é” (BROOKS, 2016, p.218). Ainda, para Brooks (2016), a humanidade sempre tentou desenvolver limites que diferenciam os tempos de guerra e os tempos de paz, todavia a contemporaneidade acaba por borrar tais limites e cada vez mais é difícil conceber o que é legal na presença ou ausência de conflitos. A crítica que a autora faz à securitização do mundo contemporâneo é que tudo se tornou guerra e os militares tornaram-se tudo, dificultando a vida em sociedade pela quantidade de ameaças que o mundo atual possui (BROOKS, 2016).

É dessa forma que os Estados Unidos não operam mais estrategicamente, assumindo a ideia de uma ameaça conhecida. A maior potência do mundo lida com uma gama de diferentes adversários, cada um com diferentes capacidades e propósitos divergentes, como por exemplo grupos violentos extremistas e suas devidas ideologias (BAYLIS, 2009).

Desta forma, o artigo 5 da OTAN que versa sobre a Segurança Coletiva precisa também abranger as ameaças híbridas, pois a OTAN precisa lidar com situações em que os países membros são pressionados por ameaças não-tradicionais (NORTH ATLANTIC TREATY ORGANIZATION, 1949). A semântica da palavra guerra e a intensidade que um ataque híbrido possui também importam ao artigo 51 da Carta das Nações Unidas, pois ela dá ao direito de legítima defesa aos Estados (UNITED NATIONS, 1949). O principal problema, todavia, é conceituar o nível exato do uso da força que as ameaças híbridas possuem para iniciar uma resposta contra.

Ainda sobre a Segurança Coletiva, um dos problemas das ameaças híbridas é que os membros da OTAN não podem responder de forma ofensiva tal ataque pela dificuldade de reconhecer e confirmar a identidade do *inimigo*, e portanto a forma a qual os países lidam com ataques híbridos são ações como identificar, mitigar, conter e retaliar o ator beligerante (AARONSON; DIESSEN; DE KERMABON; LONG; MIKLAUCIC; 2011).

Quando analisamos países individuais em confronto híbrido, é importante em termos legais definir se a Guerra híbrida concede aos Estados direitos e deveres que estão em guerra. Desta forma, a conceituação da Guerra Híbrida não é apenas uma questão puramente técnica e abstrata, mas também deve ser analisada quais direitos e privilégios os Estados possuem ou não em um ataque híbrido (ALMANG, 2019).

De uma definição clássica, Clausewitz afirmaria que a guerra é “um ato de violência para impor nossa vontade ao inimigo” (CLAUSEWITZ, 1984, p. 162). Ainda, Clausewitz (1984) escreve que a política é intrínseca na guerra, e mais contemporaneamente Bull concorda que “a Guerra é a violência organizada por unidades políticas entre si” (BULL, 1977, p. 17). Desta forma, a semântica do termo *guerra* deve ajudar a entender a natureza da Guerra Híbrida, pois se tal conflito se configura como guerra, toda a dinâmica de como os países se relacionam entre si e consigo mesmo muda.

Todavia, como dito a Guerra Híbrida pode tomar outras dimensões que não necessariamente infringem o direito internacional, por exemplo, Bachmann and Munoz Nosquera (2018) descrevem os ataques recentes Russos como *Guerra Jurídica*, pois em tais contextos a ambiguidade legal e a falhas nas leis são exploradas na busca de vantagem sobre o inimigo. Como especificado, a natureza da Guerra Híbrida é exatamente confundir os limites do uso da força e desta forma, contornar o uso do artigo 51 das Nações Unidas ou o artigo 5 da OTAN (BACHMANN; NOSQUERA, 2018).

De forma cronológica, é possível comparar o termo *Guerra Híbrida* desde a primeira conceituação feita por Hoffmann em 2009 com a declaração da Cúpula de Bruxelas em 2021, analisando que o termo ganha uma definição mais abrangente para a OTAN, compondo as ameaças convencionais, irregulares, assimétricas combinadas com o tempo e espaço (HOFFMANN, 2009; NATO, 2021). Ainda, a declaração da Cúpula de Bruxelas em 2021 é mais específica e confirma que os atores podem ser transnacionais, estatais, grupos e indivíduos operando em qualquer parte do globo. As ameaças que o documento assinala são o terrorismo, os ataques cibernéticos, insurgência, criminalidade pervasiva e a desordem generalizada (NATO, 2021). Observa-se então uma evolução do conceito de 2009 a 2021 reconhecendo os possíveis eventos que moldaram a percepção de ameaça do Estado.

Todavia, a partir de 2017 o termo Guerra Híbrida habilita os líderes militares a ganhar vantagens em cada uma de suas forças e aumentar a pressão nas vulnerabilidades do inimigo durante o conflito. Quando pensamos no curso da história, temos que vários tipos de força lutaram simultaneamente, todavia tais forças eram acionadas em locais diferentes através de uma gama de operações distintas. Já as Guerras pós-modernas e contemporâneas criam uma sinergia estratégica forte, e alguns estrategistas escrevem que é possível estender a guerra até mais longe. É essa mistura de capacidades acionadas ao mesmo tempo que é chamada de Guerra Híbrida (HOFFMAN, 2009).

Hoffman (2009) descreve que a Guerra do Líbano em 2006 pode ser exemplificada como Guerra Híbrida. Desta forma, o grupo Hezbollah lutando contra as Forças de Defesa de Israel provou que as forças armadas de Nasrallah eram altamente disciplinadas, treinadas profissionalmente e habilitadas a operar em células distribuídas em diferentes locais. O grupo Hezbollah combinou a letalidade do Estado com o fanatismo prolongado de combatentes não-convencionais, demonstrando as habilidades de atores não-estatais de estudar e conhecer as vulnerabilidades do estilo militar ocidental e criar contramedidas apropriadas. Hoffman (2009) conclui que tal conflito não foi anômalo, todavia foi um prenúncio das futuras guerras modernas.

Segundo Polyakova (2018), a Guerra Política que o Kremlin possui contra os países democráticos têm sido desenvolvidos para garantir o anonimato dos ataques. Todavia, mesmo que a Rússia seja pioneira em ferramentas de táticas assimétricas no século XXI, incluindo ataques cibernéticos e campanhas de desinformação, tais ameaças vão ser simples no futuro. O avanço tecnológico em automação, *machine learning* combinado com o crescente aumento da *big data* tem consolidado uma nova era para sofisticar, baratear e trazer mais impacto na guerra política. As expectativas para a tecnologia de um futuro próximo é a impossibilidade de distinguir entre áudios verdadeiros e falsos, vídeos e personalidades na internet. É desta forma que Estados que queiram utilizar ameaças híbridas poderão atacar democracias do ocidente de forma eficiente e prática (POLYAKOVA, 2018).

Assim como regimes autoritários aprendem um com os outros, governos ocidentais, a sociedade civil e o setor privado vão precisar estabelecer relações para compartilhar as melhores práticas de resistência. Assim como o governo dos Estados Unidos expressou sua surpresa com as novas estratégias do terrorismo em 11 de setembro de 2001, para garantir que as democracias do ocidente não acabem sendo surpreendidos novamente, o setor público e privado devem em conjunto pensar menos em reagir a ataques, mas sim em identificar e - e se preparar - para ameaças emergentes que possuem capacidades assimétricas em um futuro próximo (POLYAKOVA, 2018).

Para entendermos melhor a correlação entre as gerações de guerra e a Guerra Híbrida, o esquema apresenta como a Guerra Híbrida possui procedência dos modos convencionais e não-convencionais da Guerra. Portanto, a Guerra Híbrida é composta por atores estatais ou não-estatais que utilizam dos cinco tipos de geração de guerra para vulnerabilizar os adversários e conseguir os interesses que são desejados.

A ênfase no campo cibernético todavia pode ser compreendido com a edição do ano de 2015 do *Military Balance,* o qual define a Guerra Híbrida pelos métodos que a compõe, e dessa forma:

> o uso de ferramentas militares e não militares em uma campanha integrada, projetada para surpreender, tomar a iniciativa e obter vantagens psicológicas e físicas utilizando meios diplomáticos; informações sofisticadas e rápidas, operações eletrônicas e cibernéticas; ação militar e de inteligência secreta e ocasionalmente aberta; e pressão econômica (JAMES HACKETT, 2015, p.5, tradução própria).

Desta forma, o que distingue a definição de Guerra Híbrida das anteriores é a ênfase nos métodos não-militares do conflito, e em particular, a guerra informacional. Ainda, para Pomerantsev (2014), essa *blitzkrieg* vai além das operações de guerra informacional, pois para o autor a Rússia não apenas lida com desinformação, vazamentos, sabotagem cibernética associadas com a guerra de informação. Todavia, o objetivo dos Estados autoritários é reinventar a realidade.

É dessa forma que Bērziņš (2015) conclui que para o futuro da guerra, o campo de batalha está na *mente* dos indivíduos, já que as novas gerações de guerra são dominadas pela guerra psicológica e de informação. Desta forma, um dos objetivos que os Estados utilizam da Guerra Híbrida é exatamente reduzir a quantidade da força militar para o mínimo possível, fazendo com que as forças armadas e a população civil dos adversários apoiem o Estado que está atacando em detrimento do seu governo e do seu país.

Portanto, este trabalho compreende a relação entre as Gerações de Guerra e a Guerra Híbrida, tendo como o uso da Guerra não-convencional o principal fator no aumento das possibilidades de diferentes ataques híbridos. Ainda, este trabalho não ignora outros fatores que impulsionaram a criação do conceito de Guerra Híbrida, mas toma como principal fator o desenvolvimento de tecnologia e posteriormente a criação do domínio operacional cibernético.

Desta forma, as dimensões estratégicas do domínio cibernético são importantes para entendermos como o espaço cibernético tem um peso grande nas ameaças híbridas e na vulnerabilidade dos Estados. Na próxima seção será analisada a definição de entorno estratégico, e como ele se conecta com o mundo físico e virtual, aumentando o alcance dos Estados em atacar diferentes estruturas físicas e dados sensíveis por meio da Guerra Híbrida.

2.3 A definição de entorno estratégico

Os estudos estratégicos são conhecidos desde a antiguidade e refletem como as forças armadas atingem seus objetivos de guerra. Todavia, autores recentes têm enfatizado como os estudos estratégicos possuem aplicações nos tempos de paz e nos tempos de guerra, e desta forma os estudos estratégicos englobam muito mais que guerras e campanhas militares. Para Gray (2017) a estratégia é o uso teórico e prático, o uso da ameaça e forças organizadas para propósitos políticos.

Portanto, percebemos que não existe uma abordagem puramente militar para o uso da estratégia, já que o uso da força militar exige o conhecimento operacional da política. Um dos exemplos que temos é como os estudos estratégicos possuem uma perspectiva interdisciplinar, e dessa forma, para entender as dimensões da estratégia é necessário conhecer sobre política, economia, psicologia, sociologia, geografia assim como tecnologia, estrutura de força e tática (BAYLIS, 2006).

Desta forma, para definirmos o entorno estratégico, é necessário entender como o desenvolvimento tecnológico impacta a geopolítica de um Estado. Desta forma, Mackinder (1962) na virada do século 20 afirmou que o desenvolvimento de ferrovias era a chave para transformar a geopolítica européia na época: os Estados sem litoral poderiam se tornar potências continentais em detrimento dos Estados com litoral. Como afirmou Mackinder (1962, p.129) “Agora, assim como nas revoluções do passado, a tecnologia profundamente afeta a soberania dos governos, a economia mundial e a estratégia militar”, trazendo a ideia de que existe dinamismo entre as relações históricas e conceituais da guerra. Mackinder (1962) pode ser considerado um clássico dos estudos estratégicos por que compreendeu que o mundo está em constante mudança, e dessa forma, os formuladores de políticas e estrategistas deveriam pensar em instâncias futuras para a defesa da soberania.

Assim, Mackinder (1962) afirma sobre formuladores de políticas que:

> Eles devem ter uma visão global e uma prontidão rápida para enfrentar emergências, pois nunca foi mais verdadeiro do que neste mundo recém-fechado que nossa estabilidade é apenas equilíbrio, e a sabedoria reside na administração magistral do imprevisto; eles também devem ter um poder treinado de julgar valores e ser capazes de visões de longo prazo na formulação de políticas para o futuro; e eles, é claro, ainda precisarão de uma compreensão do momento com o qual o Homem e seu ambiente vêm do passado para o presente (MACKINDER, 1962, p. 130, tradução própria).

Para Lonsdale (2004), a relação entre tecnologia e geopolítica é intrínseca, e para a maioria das teorias geopolíticas a premissa é que a tecnologia ajuda a influenciar a

geopolítica. Desta forma, Lonsdale (2004) demonstrou que o quinto domínio operacional (por ele chamado de infosfera) possui estratégias diferentes. Pensar na infosfera, portanto, é pensar na constituição de um domínio como meio a chegar a outros, como a esfera econômica, social, política e militar.

Para Martin Libicki (2009), o papel central da informação na guerra é resultado dos avanços tecnológicos e mudam como os Estados expressam seu poderio bélico. Portanto, guerra híbrida pode ser cada vez mais caracterizada como um jogo de "esconde-esconde" tal que uma demonstração de força contra força (LIBICKI, 2009). Desta forma, a estratégia dentro do campo cibernético se baseia em uma nova realidade geopolítica, pois o ciberespaço não possui fronteiras. Todavia, Keohane e Nye (1998) afirmam que a informação não perpassa num vácuo existencial, mas sim em um espaço político já ocupado. Se tal espaço político já está ocupado e dominado pelos Estados, a dimensão estratégica de como os países se relacionam nesse domínio é caracterizado pelo dinamismo, requerendo constante vigilância para proteger e assegurar a integridade e o fluxo de informação (KEOHANE; NYE, 1998).

Com uma abordagem mais estratégica e em conjunto com a teoria desenvolvida por Corbett (2009) é possível fazer uma comparação da soberania do poder marítimo e do poder na infosfera, já que tais dimensões estratégicas são impossíveis de serem controladas por completo (CORBETT, 2009). Tomando em consideração, que o controle da infosfera é baseado na habilidade de um Estado ou ator suceder em uma campanha digital e ao mesmo tempo prevenir que a campanha digital de outro adversário tenha sucesso.

É exatamente por isso que o poder cibernético necessita que o inimigo também esteja conectado na mesma rede, já que ataques como a guerra cultural, ataques semânticos, captura de inteligência acontecem pela conectividade entre as partes (LONSDALE, 2004). É paradoxal, mas ao mesmo tempo é necessário que os adversários possuam conectividade e tecnologias pares para serem atacados.

Desta forma, operar e dimensionar na quinta dimensão estratégica possui vantagens e limitações. Tendo como objetivo mensurar o poder cibernético na geopolítica e em suas dimensões físicas para um país, é necessário analisar a estratégia que tal país possui. Para Lonsdale (2004), se a revolução informacional realmente suceder e transformar a geografia física dos Estados irrelevantes, isso implicará a inutilização das formas militares físicas de poder. Outra opção, e a qual tal trabalho se baseia, é entender que objetivos estratégicos serão entrelaçados com as forças militares tradicionais em conjunto com o uso do campo

cibernético para garantir que o adversário não tenha vantagens na defesa de sua soberania. Portanto, os fatores geográficos são importantes, já que tropas e equipamentos necessitam ser transportados, e dessa forma a distância, os efeitos do terreno e o clima importam quando se pensa no entorno estratégico no século XX e XXI (LONSDALE, 2004).

Clausewitz acreditava que em matéria de decidir um conflito, reconhecia que a vantagem assimétrica entre os lados beligerantes poderia decidir a batalha (CLAUSEWITZ, 1984). É dessa forma que Libicki (2009) postula que o poder informacional possa anular as expressões físicas de poder do adversário, já que as forças tradicionais armadas em conjunto com a precisão de munições guiadas trariam a inevitável vitória.

Para Libicki (2009), a Guerra Estratégica Informacional é uma forma de ataque que envolve o poder informacional em conjunto com poderes terrestres, aéreos, marítimos ou espaciais para destruir alvos ou mover tropas. Neste caso, para cumprir a promessa de transformar a geopolítica irrelevante, seria necessário que a Guerra Informacional fosse o único fator decisório na vitória de uma guerra. Se este fosse o caso, as guerras estariam só na dimensão cibernética, todavia ainda não existiu qualquer conflito que se desse apenas na infosfera.

O entorno estratégico na era informacional acaba por criar um paradoxo. De um lado temos países encorajados a se envolver cada vez mais em crises e problemas, independentemente da sua localização geográfica. Por outro lado, os países tendem a ter posturas mais isolacionistas. Exemplificando, é custoso para países enviar forças militares para zonas de crise ou de guerra, todavia o poder informacional abre a oportunidade de influenciar eventos sem a presença direta e de uma forma mais discreta. A globalização faz com que estados se interessem mais por trocas econômicas, culturais e políticas, e é dessa mesma forma que Estados têm o interesse de participar em eventos e crises que não necessariamente estão em seu entorno estratégico físico (BAYLIS, 2002).

Wohlstetter (1968) quando pontua que ser capaz de projetar poder em certa área ou em certo ator, não significa que os Estados o fazem. Quando pensamos no entorno estratégico dos países e a dimensão cibernética, é importante analisarmos que o processo-decisório doméstico também faz parte da geopolítica, e é por isso que Estados utilizam de políticas racionais para ganhar vantagens ou influenciar de qualquer modo regiões do mundo que possuem interesses.

Ainda, em várias ocasiões o poder informacional atua em conjunto com outros instrumentos físicos de poder, pois os seres humanos existem e operam no mundo físico. Desta forma, a geografia continua a ser importante, lembrando que cada vez mais a infosfera e a informação é territorializada, pensando na ideia de que todos os utensílios domésticos e profissionais cada vez mais se conectam com o espaço cibernético, como por exemplo geladeiras modernas. Portanto, podemos pensar na infosfera refletindo a tradicional realidade geopolítica, de um ponto de vista estratégico (BAYLIS, 2006).

Contudo, o entorno estratégico se transforma, pois com o poder informacional pode ser projetado globalmente sem nenhum recurso da geografia física. Desta forma, como dito acima, é possível que o entorno estratégico caminhe para uma realidade geopolítica diferente: tendo a geografia física refletida na infosfera, assim como a infosfera refletida na geografia física (LONSDALE, 2004).

Para Nye (2011), o ciberespaço não vai substituir o espaço geográfico e não vai eliminar a soberania estatal, todavia a difusão de poder no ciberespaço vai coexistir e complicar o exercício do poder destes Estados na quinta dimensão. Desta forma, a infraestrutura física da internet continua conectada com a geografia e os governos são soberanos destes espaços geográficos, portanto a localização geográfica importa como recurso do domínio cibernético.

Os governos podem tomar passos para subsidiar infraestrutura, ensino da informática e proteger as propriedades intelectuais para encorajar o desenvolvimento das capacidades dentro de suas fronteiras. O fornecimento de bens públicos, incluindo um ambiente regulado e legal, pode estimular o crescimento comercial das capacidades cibernéticas. Por exemplo, uma reputação que pode ser vista como legítima, benigna e competente pode melhorar o *soft power* de governos com outros atores no domínio cibernético. Ainda, a geografia física é importante pois serve como base para os governos exercerem coesões legais de controle. Por exemplo, depois dos protestos em Xinjiang em 2009, o governo Chinês desconectou 19 milhões de usuários da internet, não permitindo o envio de mensagens de texto, telefonemas internacionais e o acesso à internet, com exceção de alguns websites governamentais (NYE, 2011).

Os Estados que desejam se conectar e ao mesmo tempo estarem protegidos contra ameaças híbridas devem buscar flexibilidade e mecanismos para criar respostas rápidas em políticas, instituições, escolhas tecnológicas e planos de capital humano. Ainda, as

instituições econômicas e de defesa dos Estados estão agora dependentes do ambiente cibernético e vulneráveis a ataques criminais e disruptivos. Como Mackinder (1962) utiliza da metáfora que os Estados podem ser compreendidos como organismos biológicos, pensando no entorno estratégico e nas capacidades de defesa dos Estados, não necessariamente a sobrevivência é baseada no mais forte, no maior ou no mais agressivo, mas sim no mais adaptável ao meio. Desta forma, a lição que Rattray (2001) e os clássicos dos estudos estratégicos querem nos mostrar é que a habilidade de aprender, cooperar quando lucrativo e competir quando necessário são forças fundamentais para os Estados que buscam poderio cibernético.

Portanto, a conceituação e a compreensão das novas dimensões estratégicas são necessárias para o direcionamento das políticas de defesa e diretrizes que busquem o aprimoramento das capacidades de defesa. A definição de entorno estratégico é essencial para explorar o discurso da República Tcheca e compreender como o Estado da República Tcheca compreende seu entorno estratégico. A compreensão do entorno estratégico nos faz analisar que possivelmente a melhor estratégia da República Tcheca seria se adaptar aos avanços tecnológicos e as diferentes possibilidades futuras de guerra. Prosseguiremos analisando como a mudança do paradigma de defesa da República Tcheca influenciam as respostas estratégicas.

2.3.1 O entorno estratégico da República Tcheca: mudança do paradigma de defesa

Para analisarmos o entorno estratégico da República Tcheca, será necessário considerarmos os fatos históricos que moldaram as atuais percepções de defesa nacional. Neste caso, a República Tcheca (e a Europa Central, de forma mais abrangente) redirecionou seus valores geopolíticos após a Guerra Fria, iniciando um processo de ocidentalização (CADIER, 2019). Segundo Cadier (2019), esse processo de ocidentalização é mais conhecido como *retorno para a Europa*, uma visão aceitando a democracia liberal, o capitalismo e as estruturas políticas euro-atlânticas que eram vistas como soluções contemporâneas para as questões geopolíticas.

Desta forma, desde 1993, o entorno estratégico da República Tcheca possui três principais pilares que se desenvolvem na forma de desafios. O primeiro concerne a adequação dos padrões da europa ocidental de mudança do entorno estratégico e das mudanças na

política interna, econômica e na transformação social. O segundo está relacionado com a implementação da política de defesa, que na maior parte do tempo encontra dificuldades por não estar sendo financiado adequadamente, resultando num setor de defesa que possui meios insuficientes e a defasagem das capacidades de defesa. O terceiro pilar está associado com a evolução do conceito de Forças Armadas da República Tcheca, mais especificamente, o papel das forças armadas era primariamente a defesa do território nacional que contemporaneamente se converte (depois dos anos 90) seu papel em Forças Expedicionárias que possui em seu conceito principal a defesa coletiva e provedor de know-how para gestão de crises internacionais (seguindo a mesma estratégia da OTAN, como analisado no capítulo 2) (PROCHÁZKA, CHALUPOVÁ, 2017).

Compreendendo as mudanças que o país vem passando e os desafios atuais, a introdução do documento de Segurança Estratégica da República Tcheca de 2015 cita que "No mundo atual cheio de crises, a República Tcheca tem naturalmente de enfrentar um enorme número de desafios. O desenvolvimento econômico e social é a nossa preocupação principal e imediata" (REPÚBLICA TCHECA, 2015, sp). Portanto, a República Tcheca compreende que as preocupações imediatas (desenvolvimento econômico e social) apenas vão progredir caso os interesses estratégicos sejam promovidos, tais como:

> segurança e estabilidade, especialmente na zona euro-atlântica, prevenir e gerenciar conflitos locais e regionais e mitigar seus impactos, manter o papel estabilizador global da ONU e aumentar sua eficiência, fortalecer a coesão e eficiência da OTAN e da UE e manter um e ligação transatlântica credível, reforço da parceria estratégica OTAN-UE, incluindo o reforço da cooperação no desenvolvimento complementar das capacidades de defesa e segurança, desenvolver o papel da OSCE na prevenção de conflitos armados, na democratização e na construção de confiança e segurança mútuas, um regime de controle de armas convencionais funcional e transparente na Europa, apoiar e desenvolver a cooperação regional, apoiar a estabilidade internacional por meio da cooperação com países parceiros, apoiar a democracia, as liberdades fundamentais e os princípios do estado de direito, salvaguardar a segurança interna e proteger a população, salvaguardar a segurança econômica da República Tcheca e fortalecer o competitividade da economia, salvaguardar a segurança energética, de matérias-primas e alimentar da República Checa e uma nível adequado de reservas estratégicas, salvaguardar a segurança cibernética e a defesa da República Checa, prevenção e supressão de ameaças de segurança que afetam a segurança da República Checa e seus aliados (REPÚBLICA TCHECA, 2015, p.8, tradução própria).

Analisando o documento de Estratégia de Defesa de 2015 e correlacionando com Procházka e Chalupová (2017), três tendências que concernem o entorno estratégico foram elencados, a primeira tendência concerne que os riscos de invasões ou conflitos militares diretos contra a República Tcheca são baixos, todavia não se pode descartar a possibilidade do

uso da força em conjunto com os aliados da OTAN ou membros da UE. Esse ponto é sustentado pelo declínio geral de segurança e estabilidade dos flancos da Europa e nos países vizinhos da UE que podem ter forma em ameaças de natureza militar clássica ou na forma de Guerra Híbrida. Além disso, a dependência cada vez maior do Estado e da sociedade Tcheca em tecnologia gera vulnerabilidades as quais possíveis

> tentativas unilaterais de alguns Estados para criar suas próprias esferas de influência através de uma combinação de pressões políticas, econômicas e militares e atividades de inteligência podem ser considerado uma ameaça; essas pressões e atividades ocorrem também no ciberespaço (REPÚBLICA TCHECA, 2015, p. 8, tradução própria).

A segunda tendência conversa com a primeira, já que como analisamos na mudança do paradigma de defesa da República Tcheca, as Forças Armadas Tchecas se preparam cada vez mais para se transformarem em Forças Expedicionárias. Desta forma, a segunda tendência é que o entorno estratégico da República Tcheca acaba por se definir além da fronteiras nacionais e da UE, reconhecendo que quaisquer conflitos globais podem gerar consequências para a República Tcheca. O documento de Segurança Estratégica da República Tcheca afirma que "um dos aspectos característicos do ambiente atual é que nossa segurança pode ser diretamente afetada pela instabilidade e pelos conflitos existentes muito além das fronteiras da Europa" (REPÚBLICA TCHECA, 2015, p. 10). Desta forma, a República Tcheca abrange um espectro muito maior de gerenciamento de crises com uma combinação de ferramentas militares e civis, além dos meios diplomáticos, legais e econômicos (REPÚBLICA TCHECA, 2015).

A terceira tendência está associada com a ambição crescente de alguns atores no entorno estratégico tcheco estão prontos para usar a força militar em busca de seus interesses em detrimento da estabilidade de outros países. Portanto, segundo o documento de Segurança Estratégica

> As aspirações desses atores estão associadas a um aumento substancial de suas capacidades militares, incluindo capacidades cibernéticas ofensivas, armas de destruição em massa e seus meios de entrega, e com sua crescente demanda por matérias-primas essenciais, atividade nos mercados financeiros, luta por influência em áreas estratégicas e promoção cada vez mais agressiva de suas ambições políticas em fóruns internacionais (REPÚBLICA TCHECA, 2015, p. 10, tradução própria)

Além disso, outra consequência da aspiração desses atores é a desestabilização do entorno estratégico da OTAN, da UE e da República Tcheca, resultando em conflitos que violem os direitos humanos, incluindo direitos políticos, sociais e ambientais. Tais atores

(estatais ou não) normalmente violam a ordem internacional e os princípios básicos do Direito Internacional em busca de poder.

2.4 Conclusões preliminares

O presente capítulo buscou definir a genealogia da Guerra Híbrida e a sua devida relação com as gerações de guerra. Desta forma, temos que a Guerra híbrida não é sinônimo do conceito de guerra de quinta geração, e sim é composta pelas cinco gerações de guerra definidas por Reed.

Portanto, compreender a Guerra Híbrida é importante na busca de uma definição para criar respostas e políticas de defesa, principalmente quando pensamos na securitização da quinta dimensão operacional - o espaço cibernético. Por conseguinte, um dos pontos principais foi compreender as limitações e possibilidades da cibernética, pois o domínio digital será provavelmente o campo de batalha num futuro próximo. Este trabalho não ignora que as outras dimensões operacionais - terrestre, marítima, aérea e espacial - não são importantes para a compreensão da Guerra Híbrida, todavia a ênfase dada no espaço cibernético é resultado da importância que o avanço tecnológico teve no século XXI.

Alguns autores dos estudos estratégicos afirmavam que a cibernética - ou o espaço cibernético - iria deixar irrelevante a geografia física, todavia por ora vimos que os ataques mais recentes mostram que a geografia física ainda é importante para compreender o entorno estratégico de cada Estado. Ou ainda, é pela existência da cibernética que novas ameaças podem ser securitizadas nos outros domínios operacionais.

Desta forma, quando analisamos o entorno estratégico da República Tcheca e seus interesses nacionais, podemos verificar que as suas perspectivas são influenciadas pelo seu território nacional, a União Europeia, a OTAN e regiões afastadas que possuem instabilidade. Os documentos compreendem que regiões instáveis, como as regiões do Norte da África e o Afeganistão também podem desestabilizar a segurança europeia, tomando iniciativas como a manutenção da paz. Ainda, o próprio documento assinala um certo redirecionamento do entorno estratégico, já que a dependência da República Tcheca em tecnologia pode gerar vulnerabilidades.

Para darmos início ao segundo capítulo, é necessário pontuarmos a influência que as instituições como a OTAN e a UE possuem perante a República Tcheca. Desta forma, para buscarmos uma compreensão melhor da defesa estratégica da República Tcheca, será primeiro analisado como essas instituições moldam a criação de estratégias e capacidades de defesa contra as possíveis ameaças híbridas.

3 PERSPECTIVAS POLÍTICO-ESTRATÉGICAS SOBRE A GUERRA HÍBRIDA PELA OTAN, UE E REPÚBLICA TCHECA

Este capítulo procura abordar a influência da OTAN e da União Europeia nos documentos de defesa da República Tcheca depois de 1993. A escolha temporal do ano de 1993 até 2022 foi escolhida pela dissolução da Tchecoslováquia, ou seja, serão analisados os documentos que compreendem o Estado-nação da República Tcheca que entrou em vigor no dia primeiro de janeiro de 1993.

Considerando que a República Tcheca tem fortes relações históricas com diferentes comunidades de segurança, será primeiro analisado como os documentos sobre a Guerra Híbrida da OTAN e a UE influenciam os documentos oficiais de defesa da República Tcheca. Para tanto, será explorado a distinta natureza das instituições da OTAN e da UE, e posteriormente as novas estratégias e planos que as instituições possuem perante ameaças híbridas. A decisão de escolha dos documentos foi baseada na hierarquia e relevância no quesito de estratégias contra a Guerra Híbrida. Os documentos da OTAN escolhidos foram a declaração da Cúpula de Bruxelas, que foi escolhida porque, segundo oficiais da OTAN, essa declaração deve dar base para o documento de defesa mais importante, o Conceito Estratégico de 2022. A escolha de não analisar o Conceito Estratégico de 2010 da OTAN foi pela pouca relevância que a Guerra Híbrida tem no documento, e mais especificamente, o documento não cita nenhuma vez o termo Guerra Híbrida ou ameaças híbridas. Após, foi analisado o *Readiness Action Plan* que é um plano estratégico da OTAN que a República Tcheca se relaciona com seus interesses nacionais, principalmente pelo aumento do poder dissuasório no flanco leste[1] da OTAN.

Após os documentos da OTAN, o documento da UE escolhido foi a Estratégia Global que é um dos documentos mais importantes para o pilar da União para a *Política Comum de Segurança e Defesa*. Como ele é mais recente, ele versa sobre a Guerra Híbrida e sobre os eventos que desestabilizaram o leste europeu, além do uso extensivo do termo Guerra Híbrida, todavia sem uma definição do documento. Posteriormente, da mesma forma que foi analisada o plano *Readiness Action Plan*, será analisado o Quadro comum em matéria de luta contra as ameaças híbridas que é um compilado de propostas e ações que os Estados membros devem seguir para diminuir sua vulnerabilidade contra ameaças híbridas.

[1] O flanco leste pode ser compreendido como as fronteiras entre os países do Leste Europeu com seus vizinhos adjacentes

Após a análise dos documentos, serão enfatizadas as capacidades de defesa que a República Tcheca possui contra ameaças híbridas em geral, e por último será analisado as expectativas que os discursos e documentos oficiais possuem contra a Guerra Híbrida e as preparações que atualmente são feitas na prevenção desses ataques híbridos.

3.1. Definições e perspectivas político-estratégicas da OTAN e da UE

O discurso e a prática emergente da OTAN e da União Europeia em contra-atacar a Guerra Híbrida procura provar a sua contínua relevância na era contemporânea. Desta forma, a partir da análise dos documentos é possível entender que tanto a OTAN quanto a UE possuem dificuldades em lidar com a ambivalência das ameaças híbridas. Portanto, a securitização então emerge como uma resposta à incerteza gerada por essas novas ameaças, com a promessa de dar aos cidadãos dos países do hemisfério norte possibilidades de mitigar a ansiedade gerada pela incerteza da Guerra Híbrida e obter respostas mais específicas (ABULOF, 2014).

Para irmos mais a fundo e entendermos como as políticas estratégicas são conduzidas, é necessário compreender o permanente estado de prevenção, que por si só indica a coleta preventiva de todos os tipos de dados, possivelmente infringindo a privacidade dos indivíduos em nome da segurança nacional. É dessa lógica da precaução que caracteriza a luta contra um grande tamanho das ameaças híbridas, todavia ao mesmo tempo infringindo os direitos fundamentais de privacidade de indivíduos e instituições. Portanto, a contemporaneidade faz com que "as decisões são [...] tomadas não no contexto da certeza, nem mesmo do conhecimento disponível, mas de dúvida, premonição, pressentimento, desafio, desconfiança, medo e ansiedade" (EWALD, 2002, p. 294). Desta forma, a Guerra Híbrida sendo fruto da contemporaneidade também pode ser compreendida dentro de um contexto onde as políticas de defesa dos países acabam por refletir a incerteza.

Pensando de forma contemporânea, por mais que a UE e a OTAN possuam diferentes naturezas institucionais, é importante lembrar que a UE é uma parceira essencial da OTAN. Desta forma, as duas instituições possuem quase os mesmos membros associados que utilizam suas capacidades e recursos que são desenvolvidos para a UE são também empregados em missões da OTAN e vice-versa. Por definição, os 24 membros da UE têm partilhado os mesmos interesses e trabalham em conjunto em todas as missões que a OTAN

opera. Portanto, olhando para o passado as duas instituições aprenderam as mesmas lições, e olhando para o futuro, elas veem o mesmo conjunto de problemas em comum a serem solucionados (MÄLKSOO, 2018).

Para evidenciar esse esforço conjunto das duas instituições, a Alta Representante para a União Europeia e os Negócios Estrangeiros e para a Política de Segurança, em conjunto com a Comissão Europeia, no passado dia 13 de Junho de 2018, no evento o qual se definem as linhas de ação estratégica para combater as ameaças híbridas. No seu comunicado de imprensa, a Alta Representante declarou o seguinte:

> Em tempos de novos desafios em todo o mundo, estamos reforçando nosso trabalho na União Europeia para combater ameaças híbridas – seja no campo da cibernética, da desinformação ou da contra-inteligência. Juntamente com nossos Estados Membros e parceiros, como a OTAN, estamos trabalhando para fortalecer nossas capacidades para enfrentar esses desafios e aumentar nossa resiliência a riscos químicos, biológicos, radiológicos e nucleares, para proteger efetivamente nossos cidadãos (COMMISION, 2018, s/p, tradução própria).

O discurso acima pode evidenciar dois pontos cruciais, o primeiro mostra o quão desafiador as novas ameaças se apresentam para os membros da UE e da OTAN, e o segundo ponto evidencia que a capacidade de resposta reside essencialmente na resiliência conjunta dos Estados membros que possuem membresia nas duas organizações, que é o caso da República Tcheca (PEREIRA, 2018).

Desta forma, essa seção pretende compreender alguns pontos das diferenças substanciais das naturezas entre a OTAN e a UE e seus devidos esforços conjuntos, e como essas instituições influenciam a estratégia de defesa da República Tcheca. Portanto, antes de analisar como os documentos e estratégias de defesa da OTAN e da UE influenciam os documentos da República Tcheca, serão analisadas as políticas estratégicas e o caráter das duas instituições.

3.1.1 Princípios e Política Estratégica da OTAN contra ameaças híbridas

A OTAN foi criada no dia 4 de abril de 1949, em Washington D.C, e durante todo o período da Guerra Fria, o comando operacional da OTAN era limitado ao artigo 5 que versava sobre a defesa coletiva. Após a Guerra Fria, a Aliança vem se transformando numa organização de gerenciamento de segurança, trazendo ao debate formas mais abrangentes da discussão sobre sua natureza de segurança e defesa (SPERLING; WEBBER, 2018). Portanto, com o desaparecimento da ameaça soviética, a OTAN sofreu uma profunda reorientação da

estratégia e da doutrina da Aliança, principalmente com as guerras civis nos Bálcas, seguido pelos ataques de 11 de setembro de 2001. Seguindo essa lógica de reorientação, alguns pontos notáveis são: a proteção dos indivíduos assim como do Estado, considerando uma gama de outros riscos além do conflito armado, e construindo uma resposta abrangente que inclui atores civis e militares que refletem a natureza do desafio de segurança após o fim da Guerra Fria (SPERLING; WEBBER, 2018).

Segundo Sperling e Webber (2018), a reorientação da OTAN também altera o seu caráter operacional e sua jurisdição geográfica. Em outras palavras, a OTAN tem gradualmente alterado sua postura defensiva para uma organização expedicionária com expansão geográfica de suas missões. Quando analisamos de forma qualitativa a capacidade de adaptação da OTAN para diferentes configurações de mundo, a Aliança tem demonstrado que consegue se adaptar a diferentes entornos estratégicos e ameaças, afirmado por James Sperling and Mark Webber (2018) que a aliança está envolvida em um processo incessante de transformação, da própria estrutura e organização, de operações, parcerias e membros.

Algumas evidências podem ser essenciais para sustentar essa ideia de constante adaptação da Aliança às circunstâncias, como por exemplo o debate persistente de estratégia e sobre a importância das divergências existentes dentre os membros da OTAN, as quais influenciaram os documentos de estratégia em 1991, 1999, 2010 e os debates das diferentes percepções de ameaça. Então quando analisamos as operações que incluem a Bósnia, Kosovo, Afeganistão, Líbia e outras operações marítimas, é muito improvável pensar em tais operações como ameaças existenciais para todos os membros da OTAN, e é dessa forma que os membros da OTAN divergem em matéria de encontrar uma estratégia comum para essas operações (SPERLING; WEBBER, 2018).

Desta divergência e tendo em conta a situação atual do ambiente de segurança internacional, a questão de como os Estados membros da OTAN possuem diferentes percepções de ameaça, capacidades e interesses, neste caso, como gerenciar os principais desafios estratégicos contemporâneos acaba sendo de extrema importância (MÄLKSOO, 2018).

Para sermos mais específicos, os desafios que surgiram no flanco leste da OTAN em 2014 tem renovado o interesse da Aliança no poder de dissuasão e na defesa coletiva. Esse interesse se torna visível quando os ministros de defesa da OTAN concluíram que a Aliança

deve renovar e colocar mais ênfase nas capacidades de dissuasão e defesa coletiva (NORTH ATLANTIC COUNCIL, 2021).

A seleção dos documentos foi feita baseada na importância que os documentos têm contra a guerra híbrida, no caso da OTAN foi selecionada a Declaração da Cúpula de Bruxelas e o *Readiness Action Plan*, os quais versam sobre perspectivas e planos estratégicos. Pensando na UE, foi selecionado a Estratégia Global e o Quadro comum em matéria de luta contra as ameaças híbridas que foram escritos pensando sobre possíveis desdobramentos da crise da Ucrânia.

3.1.1.1 Declaração da Cúpula de Bruxelas 2021

Como afirmado no início do capítulo, a escolha da análise do documento oficial da declaração da Cúpula de Bruxelas de 2021 é importante porque é o evento que precederá o documento mais importante (Conceito Estratégico) que será divulgado em 2022. Como ainda reiterado, deu-se preferência para analisar a última cúpula da OTAN ao invés do Conceito Estratégico pela relevância que o conceito da Guerra Híbrida tem tomado nas reuniões da OTAN.

Desta forma, a OTAN assegura a sua tradição e reitera as ameaças e os desafios da OTAN é a Cúpula de Bruxelas, afirmando que,

> Nós, os Chefes de Estado e de Governo dos 30 Aliados da OTAN, reunimo-nos em Bruxelas para reafirmar a nossa unidade, solidariedade e coesão, e para abrir um novo capítulo nas relações transatlânticas, num momento em que o ambiente de segurança que enfrentamos é cada vez mais complexo. A OTAN continua a ser a base da nossa defesa coletiva e o fórum essencial para consultas e decisões de segurança entre os Aliados. A OTAN é uma Aliança defensiva e continuará a lutar pela paz, segurança e estabilidade em toda a área euro-atlântica. Continuamos firmemente comprometidos com o Tratado de Washington, fundador da OTAN, incluindo que um ataque contra um Aliado seja considerado um ataque contra todos nós, conforme consagrado no Artigo 5. Continuaremos a buscar uma abordagem de 360 graus para proteger e defender nossa segurança e cumprir as três tarefas principais da OTAN: defesa coletiva, gestão de crises e segurança cooperativa (NORTH ATLANTIC COUNCIL, 2021, s/p, tradução própria).

Portanto, analisamos com a declaração que os princípios da OTAN continuam os mesmos, todavia com o redirecionamento para uma aliança que possa ser expedicionária. Como analisamos durante o primeiro capítulo, a interpretação e os atos de fala são importantes nas Relações Internacionais, principalmente pensando em como as ameaças podem ser variadas. Desta forma, a OTAN no documento acusa países e determinadas formas

de influência, principalmente com o fator agravante da pandemia COVID-19, como podemos analisar a seguir,

> Enfrentamos ameaças multifacetadas, competição sistêmica de poderes assertivos e autoritários, bem como crescentes desafios de segurança para nossos países e nossos cidadãos de todas as direções estratégicas. As ações agressivas da Rússia constituem uma ameaça à segurança euro-atlântica; o terrorismo em todas as suas formas e manifestações continua a ser uma ameaça persistente para todos nós. Atores estatais e não estatais desafiam a ordem internacional baseada em regras e buscam minar a democracia em todo o mundo. A instabilidade além de nossas fronteiras também está contribuindo para a migração irregular e o tráfico de pessoas. A crescente influência da China e as políticas internacionais podem apresentar desafios que precisamos enfrentar juntos como uma Aliança. Envolveremos a China com o objetivo de defender os interesses de segurança da Aliança. Somos cada vez mais confrontados por ameaças cibernéticas, híbridas e outras assimétricas, incluindo campanhas de desinformação, e pelo uso malicioso de tecnologias emergentes e disruptivas cada vez mais sofisticadas. Avanços rápidos no domínio espacial estão afetando nossa segurança. [...] Nos reunimos em um momento em que a pandemia do COVID-19 continua testando nossas nações e nossa resiliência. Os militares da OTAN e aliados apoiaram a resposta civil à pandemia, garantindo nossa defesa coletiva e a eficácia de nossas operações (NORTH ATLANTIC COUNCIL, 2021, s/p, tradução própria).

Como analisamos nas definições e perspectivas, o documento afirma que a OTAN vem se adaptando continuamente com a mudança do seu entorno estratégico. Desta forma, a agenda da OTAN para o futuro complementa e constrói as adaptações políticas e militares, fortalecendo também a habilidade da OTAN contribuir para as suas três principais forças-tarefas. A declaração é bastante específica, acusando países como a China e Rússia de possuir ambições no âmbito internacional. Além disso, é importante notar que a declaração cita a pandemia como obstáculo à construção de uma sociedade resiliente, e afirmando que os militares da OTAN sofrem mais dificuldades para conduzir as operações durante a pandemia (NORTH ATLANTIC COUNCIL, 2021).

Além disso, um termo que é reiterado é o aumento da resiliência dos sistemas de informação, portanto, é importante considerar o que o documento considera como sociedade resiliente,

> Observando que a resiliência continua sendo uma responsabilidade nacional, adotaremos uma abordagem mais integrada e melhor coordenada, consistente com nosso compromisso coletivo sob o Artigo 3 do Tratado do Atlântico Norte, para reduzir vulnerabilidades e garantir que nossos militares possam operar efetivamente em paz, crise e conflito. Os Aliados desenvolverão uma proposta para estabelecer, avaliar, revisar e monitorar os objetivos de resiliência para orientar as metas de resiliência e os planos de implementação desenvolvidos nacionalmente. Caberá a cada indivíduo determinar como estabelecer e cumprir as metas nacionais de resiliência e os planos de implementação, permitindo fazê-lo em um continente compatível com suas respectivas competências, estruturas, processos e obrigações nacionais e, quando aplicável, as da União Europeia (NORTH ATLANTIC COUNCIL, 2021, s/p).

A declaração acima passa a ser importante por alguns pontos. Desta forma, a OTAN afirma que a responsabilidade das ameaças híbridas recai sobre os Estados, todavia a organização compreende que é necessário uma resposta integrada e conjunta contra ameaças híbridas para fortalecer a Aliança. Essa integração e resposta conjunta também recai sobre a União Europeia, por exemplo, demonstrando que a UE é uma aliada importante para a construção de capacidades de defesa capazes de aumentar a resiliência dos Estados. Como a declaração é recente, mais planos e propostas devem ser firmadas nos próximos anos, todavia pensando em planos estratégicos, o *Readiness Action Plan* acaba sendo uma resposta importante para o aumento da resiliência e criação de dissuasão no flanco leste da OTAN (NORTH ATLANTIC COUNCIL, 2021).

No documento, a Rússia é citada diversas vezes, sendo acusada de violar a lei internacional e as responsabilidades que os Estados possuem no âmbito internacional. Portanto, a declaração é clara quando afirma que a Aliança "continuará a responder à deterioração do ambiente de segurança, aprimorando a nossa postura de dissuasão e defesa, inclusive por meio de uma presença avançada na parte leste da Aliança" (NORTH ATLANTIC COUNCIL, 2021, s/p). É aqui que o plano estratégico *Readiness Action Plan* tange a parte dissuasória, já que a OTAN afirma que não é uma ameaça ofensiva para outras regiões do mundo, apenas tem a intenção de manter os princípios fundadores nos países membros.

Agora, mais especificamente, a declaração cita duas vezes a República Tcheca. A primeira concerne convocar a Rússia a resignar a República Tcheca e os Estados Unidos como *países hostis* de seus relatórios das relações exteriores, além de se abster de tomar quaisquer outras medidas incompatíveis com a Convenção de Viena sobre Relações Diplomáticas. Além disso, o documento afirma que está em total solidariedade com a República Tcheca e outros Aliados que foram afetados por ameaças híbridas, neste caso, interferência política e ciberespionagem (NORTH ATLANTIC COUNCIL, 2021).

Agora que já analisamos a importância da última cúpula reunida pela OTAN e as perspectivas estratégicas da OTAN, será analisado como tais perspectivas estratégicas são projetadas em planos estratégicos pela mesma instituição. Pensando na relevância do poder dissuasório e da ameaça no flanco leste, o *Readiness Action Plan* é o plano estratégico mais relevante das últimas décadas, assim como afirmou o Secretário-Geral da OTAN, e será analisada na subseção seguinte (ARNOLD, 2016).

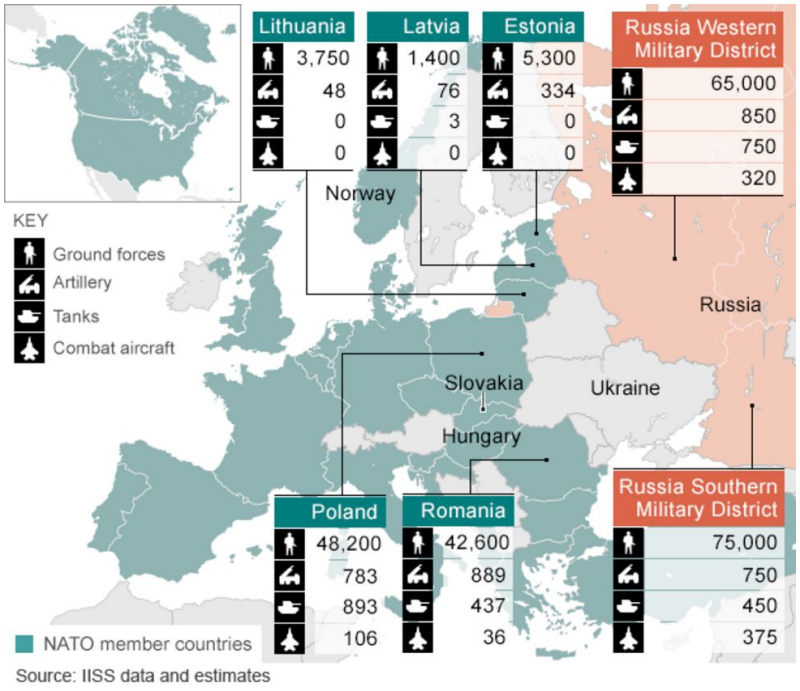
3.1.1.2 *Readiness Action Plan 2014*

O plano de ação que visa as novas estratégias da OTAN contra ameaças híbridas se chama *Readiness Action Plan*. Foi desenvolvido e aprovado durante a Cúpula de Gales em 2014, um dos principais impulsionadores da transformação na estratégia de dissuasão e defesa da Aliança. Segundo a ficha técnica do *Readiness Action Plan*, o plano foi criado para garantir a prontidão da organização em resposta rápida a quaisquer ameaças que venha das implicações estratégicas da Rússia, além de responder a ameaças que compreendam o Oriente Médio e o Norte da África (NORTH ATLANTIC TREATY ORGANIZATION, 2016).

Segundo a ficha técnica emitida pela OTAN, o documento é dividido em *insurance measures* que abrangem medidas que protegem e asseguram o poder de dissuasão dos países da Europa Central e do Leste Europeu, e *adaptation measures* que aumentam as forças de resposta da OTAN e ainda criam pequenos quartéis-generais multinacionais chamados de *NATO Force Integration Units* na Bulgária, Estônia, Hungria, Lituânia, Letônia, Polônia, Romênia e Eslováquia (NORTH ATLANTIC TREATY ORGANIZATION, 2016).

Para analisarmos de uma forma mais visual como a OTAN se prepara com o *Readiness Action Plan* no Centro e Leste Europeu, podemos visualizar o aumento das tropas da OTAN no mapa abaixo.

Figura 2 - Quantidade de tropas em *NATO Force Integration Units*



Fonte: Pereira (2018).

Ainda, o *Readiness Action Plan* é um pilar de sustentação para o novo conceito estratégico da OTAN que deve ser publicado em 2022 tendo como nome oficial em inglês *Strategic concept: Assured Security; Dynamic Engagement* (NORTH ATLANTIC TREATY ORGANIZATION, 2016). Um dos pontos que o documento foca é que o maior alargamento da OTAN para o flanco sul e leste, requerendo uma nova estratégia que possa abranger as novas ameaças que o novo entorno estratégico da OTAN possui. Portanto, de acordo com a OTAN, um dos pontos que deve ser enfatizado é o novo entorno estratégico pela alargamento da instituição,

> A terceira tarefa central da OTAN é servir como meio transatlântico para consultas de segurança e gestão de crises ao longo de todas as questões que a Aliança enfrenta. Como único elo contratual entre a América do Norte e a Europa, a OTAN continua a ser o local essencial para essas funções e para o cumprimento dos compromissos de segurança e defesa comuns de seus membros. Esta tarefa reflete as dimensões políticas e militares da Aliança e merece mais atenção à luz da diversidade das ameaças à segurança de hoje e a ampla perspectiva dos atuais membros da organização. Afinal, quando o último Conceito Estratégico foi escrito, a Aliança tinha muito menos membros com linhas costeiras nos mares Adriático, Negro e Báltico (NORTH ATLANTIC TREATY ORGANIZATION, 2016, tradução própria).

Dessa forma, o *Readiness Action Plan* tem no seu cerne o aumento do poder de dissuasão, sendo que todas as iniciativas foram elogiadas pelo Secretário-Geral da OTAN,

Jens Stoltenberg, e definidas como “o fortalecimento mais importante de nossa defesa coletiva em décadas” (ARNOLD, 2016, p. 86). Para o poder dissuasório, também está previsto o estabelecimento de uma unidade de *Very High Readiness Joint Task Force (VJTF)* – uma *força de ponta de lança* de cerca de 20.000 soldados, dos quais cerca de 5.000 são forças terrestres – é capaz de ser empregada dentro de dois a três dias onde for necessário. O *VJTF* é composto por componentes aéreos, marítimos e SOF (NORTH ATLANTIC TREATY ORGANIZATION, 2016).

Além disso, o *Readiness Action Plan* assegura os países do leste europeu a presença constante da OTAN, com forças aéreas, terrestres e marítimas em contínua em base rotativa, sendo que a questão de financiamento da OTAN também será resolvida com um Acordo para reverter a tendência de declínio dos orçamentos de defesa dentro da aliança. Os aliados que já cumpriam a meta da OTAN de gastar dois por cento de seu produto interno bruto em defesa se comprometeram no País de Gales de que continuariam com tal política de defesa (NORTH ATLANTIC TREATY ORGANIZATION, 2016). A República Tcheca, como será analisado posteriormente, não cumpre com os orçamentos de 2% do seu PIB, tendo sua tendência para o investimento em defesa para 2021 ao redor de 1,46% (EURACTIV, 2021).

O plano todavia possui seus próprios desafios, como descrito por Arnold (2016), e dois desafios foram selecionados para serem mais discutidos em como tal estratégia é influenciada pela Guerra híbrida. O primeiro desafio estratégico compreende que o flanco leste possui uma presença em massa de tropas estadunidenses, ao lado das tropas do Reino Unido. Segundo Arnold, as tropas europeias que participam dos exercícios táticos, normalmente retornam para seus países de origem. Desta forma, nas palavras de Steven Pifer (2014),

> Putin parece decidido a desafiar a aliança. A escassez de botas europeias no terreno pode levar o Kremlin a uma conclusão perigosa: que aliados importantes podem não estar preparados para cumprir seu compromisso sob o Artigo 5 da OTAN de defender os países bálticos. As consequências podem ser desastrosas (PIFER, 2014, p.19, tradução própria).

Agora, outro problema que surge é com o poder dissuasório e o artigo 5 da OTAN sob as ideias de Glenn Snyder (1959) que introduziu a diferença entre dois tipos de dissuasão: através da *ameaça da punição* e a *dissuasão por negação*. A dissuasão por *ameaça da punição* é quando o adversário é desencorajado a fazer uma ação particular pela ameaça de receber custos e retaliações, que são mais que os ganhos relativos da ação prevista. Um dos exemplos é a retaliação nuclear em resposta a alguma agressão. Em contraste, a *dissuasão por*

negação é uma estratégia que busca deter uma ação, tornando o sucesso inviável ou improvável, negando assim a um potencial agressor a confiança em atingir seu objetivo. Exemplificando, capacidades de poder dissuasório por negação é um termo inter-relacionado com a capacidade de defesa.

Para Arnold (2016), o *Readiness Action Plan* apenas fortalece a capacidade da OTAN de dissuasão por punição, com pouco incremento oferecido para a capacidade de negação. Como analisamos no capítulo 1, o *Readiness Action Plan* acaba por ser ineficaz em ataques híbridos que não seja acionado o artigo 5 da OTAN, compreendendo que atores estatais ou não-estatais tem o interesse de causar danos nas vulnerabilidades dos países com a intenção do artigo 5 não ser acionado. Portanto, caso o artigo 5 da OTAN seja inutilizado, é improvável o emprego das forças do *Readiness Action Plan*, como no caso da Ucrânia em 2014. O maior desafio, portanto, é a identificação legítima dos ataques híbridos e a atribuição legal contra perpetradores, para que caso seja necessário o *Readiness Action Plan* possa ser empregado com o acionamento do artigo 5.

3.1.2 Princípios e Política Estratégica da UE contra ameaças híbridas

A UE vem passando por diferentes transformações, como no caso da possibilidade de alargamento para outros países candidatos, como a Albânia, a Macedônia do Norte, Montenegro, Sérvia e Turquia ou a própria questão do Brexit. Neste caso, a polarização geopolítica do mundo acaba por interferir em como os países membros e candidatos da UE pensam em coordenar seus interesses para garantir a defesa de suas soberanias. Desta forma, as ameaças crescentes no mundo podem ser uma oportunidade para que façam os países europeus cooperarem para garantir sua posição estratégica no mundo, algo que possivelmente se encontrava solucionado desde o final da Guerra Fria (NORTH ATLANTIC TREATY ORGANIZATION, 2021).

Em termos práticos, a preocupação com as ameaças híbridas fez com que o conceito de guerra empiricamente fosse mais aceitável para a UE. Embora a guerra continue a ser normativamente inaceitável, a discussão pública de práticas concretas para combater várias ameaças híbridas como parte do paradigma de combate à guerra híbrida está longe de ser um tabu para a UE nos dias de hoje (ARNOLD, 2016).

Todavia, a UE é uma instituição que se advoga com uma narrativa própria de antípoda da Guerra, e desta forma existe um objetivo político em evitar o conceito de guerra nos documento de defesa da UE. Uma das razões históricas de entender por que a UE tem essa posição pacifista é pelo seu passado sangrento caracterizado principalmente pelas duas guerras mundiais (DELLA SALA, 2018). Portanto, a UE pode estar mais preparada para lidar com esses tipos irregulares de guerra, pois historicamente as concepções de segurança sempre foram muito mais amplas baseadas no indivíduo e na segurança humana ao invés da existência de um foco específico na abordagem militar (MANNERS, 2002).

Para iniciarmos a análise dos documentos de defesa da União Europeia, é necessário compreendermos que a UE atribui a responsabilidade no combate às ameaças híbridas aos estados membros, já que a maioria das vulnerabilidades nacionais são específicas de cada país (UNIÃO EUROPEIA, 2016a). Todavia, não podemos ignorar por completo as funções da UE no combate às ameaças híbridas, tendo em conta que o papel da UE é conceber uma resposta coordenada a fim de desenvolver a solidariedade europeia, a assistência mútua e todo o potencial do Tratado de Lisboa (UNIÃO EUROPEIA, 2016a). Portanto, a UE define que a segurança interna e externa da própria união está cada vez mais conectada,

> A União Europeia vai promover a paz e garantir a segurança dos seus cidadãos e do seu território. Isto significa que os europeus, ao trabalhar com parceiros, devem possuir as capacidades necessárias para se defenderem e cumprirem os seus compromissos de assistência mútua e de solidariedade consagrados nos Tratados. [...] A segurança interna e externa estão cada vez mais interligadas: nossa segurança doméstica supõe um interesse paralelo pela paz em nossas regiões vizinhas e circunvizinhas. Implica um interesse mais amplo na prevenção de conflitos, promovendo a segurança humana, abordando as causas profundas da instabilidade e trabalhando para um mundo mais seguro (UNIÃO EUROPEIA, 2016, p.7, tradução própria).

Portanto, a UE tenta influenciar a República Tcheca e os seus devidos países membros a obter um controle epistemológico sobre o espectro de ameaças híbridas por meio de ações de conscientização que devem melhorar a resiliência dos Estados-Membros para responder a ameaças comuns (UNIÃO EUROPEIA, 2016a). A UE se esforça no sentido de construir resiliência tais como a proteção da infraestrutura crítica; adaptação e desenvolvimento das capacidades de defesa necessárias; proteção da saúde pública e da segurança alimentar; melhora da segurança cibernética em várias esferas; visando o financiamento de capacidades de defesa contra ameaças híbridas; combate à radicalização e a violência causada pelo extremismo; aumento da cooperação com países terceiros (UNIÃO EUROPEIA, 2016a).

Ainda, na Estratégia Global da UE, os eventos chaves que transformaram a opinião europeia sobre as ameaças foi a radicalização e violência extremista com as lições aprendidas com as ações russas contra a Ucrânia nos últimos anos. Os dois pontos que foram analisados e que podem ser relevantes do discurso da UE e da prática emergente no combate às ameaças híbridas são a comunicação estratégica e a resiliência, com prevenção, resposta a crises e recuperação de ameaças híbridas atuando como objetivos suplementares. Resiliência é definida no combate às ameaças híbridas como "a capacidade de resistir ao estresse e recuperar-se, fortalecida dos desafios" (UNIÃO EUROPEIA, 2016a, p.5). Este objetivo foi concebido para promover a resiliência da UE e dos Estados-Membros, bem como dos parceiros (UNIÃO EUROPEIA, 2016a). Portanto, a UE tem como principal estratégia,

> implementar uma abordagem multidimensional por meio do uso de todas as políticas e instrumentos disponíveis voltados para a prevenção, gestão e resolução de conflitos. Mas o escopo da abordagem abrangente será expandido ainda mais. A UE irá, por conseguinte, seguir uma abordagem multifásica, atuando em todas as fases do ciclo de conflito. Investiremos na prevenção, resolução e estabilização, e evitaremos o desligamento prematuro quando uma nova crise eclodir em outro lugar. Por último, nenhum destes conflitos pode ser resolvido apenas pela UE. Buscaremos uma abordagem multilateral envolvendo todos os atores presentes em um conflito (UNIÃO EUROPEIA, 2016a, p. 32, tradução própria).

Existe um objetivo político em ignorar explicitamente o conceito de guerra nos documentos de defesa da UE, já que é importante para sustentar a continuidade da fundação da instituição que se advoga com uma narrativa própria de antípoda da Guerra. Portanto, é natural que a UE tenha a tendência de abordar conflitos com a perspectiva de gerenciamento de crise.

Após uma breve análise dos documentos que versam sobre as ameaças híbridas, foi escolhido para essa monografia a análise da Estratégia Global publicada em 2016 e do Quadro comum em matéria de luta contra as ameaças híbridas. Foram selecionados esses documentos pelo teor político-estratégico da Estratégia Global, trazendo claras definições sobre as perspectivas de defesa da UE contra ameaças híbridas e o Quadro comum em matéria de luta contra as ameaças híbridas por ser um documento de cunho prático, ou seja, não será analisada cada ação que a UE sugere que os Estados sigam, mas para compreender a ação conjunta que os Estados membros da UE necessitam seguir para construir resiliência e aumentar a conscientização dos diversos setores que podem estar vulneráveis a estes ataques.

3.1.2.1 Estratégia Global da EU

Na introdução da Estratégia Global da UE (2016a), o documento afirma que ele começa *em casa.* O que o documento quer dizer com isso é que a União Europeia tem permitido aos cidadãos desfrutar de segurança, democracia e prosperidade sem precedentes. Todavia, ameaças como o terrorismo, as ameaças híbridas, a volatilidade econômica, as mudanças climáticas e a insegurança energética colocam em risco a sociedade e o território da União Europeia.

O documento afirma que

> Um nível adequado de ambição e autonomia estratégica é importante para a capacidade da Europa de promover a paz e a segurança dentro e fora das suas fronteiras. Portanto, intensificaremos nossos esforços em defesa, cibernética, contraterrorismo, energia e comunicações estratégicas. Os Estados-Membros devem traduzir na prática os seus compromissos de assistência mútua e solidariedade consagrados nos Tratados. A UE intensificará a sua contribuição para a segurança coletiva da Europa, trabalhando em estreita colaboração com os seus parceiros, começando pela OTAN (UNIÃO EUROPEIA, 2016a, s/p, tradução própria).

Analisando o parágrafo acima, compreende-se que os documentos afirmam os compromissos de assistência mútua e solidariedade que incluem desafios de dimensões internas e externas, ou seja, ataques terroristas e híbridos, securitização e menos dependência energética, crime organizado e gerenciamento externo das fronteiras. O documento afirma que para os desafios listados, a OTAN permanece como primeira estrutura para a maioria dos membros da UE, todavia afirma que as relações OTAN-EU não devem prejudicar a segurança e defesa dos membros que não estão na aliança. Até 2022, seis membros da UE não fazem parte da OTAN: Áustria, Chipre, Finlândia, Irlanda, Malta e Suécia (NORTH ATLANTIC TREATY ORGANIZATION, 2021).

Segundo o documento, o aprofundamento da cooperação com a OTAN será feito de modo complementar, sinergético e que respeite as estruturas institucionais, a inclusão e a autonomia de decisão das instituições e dos Estados. Portanto, o direcionamento da Política Externa da UE não possui uma única direção, em contraste, o documento afirma que “A política externa da UE não é uma performance solo: é uma orquestra que toca a partir da mesma partitura. Nossa diversidade é um grande trunfo, desde que estejamos unidos e trabalhemos de forma coordenada” (UNIÃO EUROPEIA, 2016a, p.47).

Nos termos de segurança, o terrorismo, os ataques híbridos e o crime organizado não conhecem fronteiras, ou seja, é necessário um esforco transnacional para tais ameaças. Esse esforço conjunto exige ligações institucionais mais estreitas tanto para ações externas quanto para a garantia da liberdade, segurança e justiça internas. Desta forma, será promovido esse

estreitamento de relações através de reuniões conjuntas do Conselho e grupos de trabalho conjuntos entre o SEAE e a Comissão Europeia (UNIÃO EUROPEIA, 2016a).

Portanto, as instituições ligadas à política de defesa da União Europeia possuem as seguintes estratégias que devem colocar em prática enquanto a Estratégia Global estiver em vigor,

> A política de defesa também deve estar mais bem ligada às políticas que abrangem o mercado interno, a indústria e o espaço. Os esforços dos Estados-Membros também devem ser mais combinados: a cooperação entre os nossos serviços policiais, judiciários e de informações deve ser reforçada. Temos de utilizar todo o potencial da Europol e da Eurojust e dar um maior apoio ao Centro de Informações da UE. Devemos alimentar e coordenar a inteligência extraída das bases de dados europeias e colocar as TIC – incluindo a análise de big data – ao serviço de uma consciência situacional mais profunda. Os nossos cidadãos precisam de uma melhor protecção também em países terceiros através de planos de contingência conjuntos e exercícios de resposta a crises entre os Estados-Membros (UNIÃO EUROPEIA, 2016a, p.50, tradução própria).

Ainda, o documento é recente o suficiente para versar sobre os desafios estratégicos que a relação com a Rússia propõe para a ordem de segurança europeia. Portanto, o documento afirma que uma abordagem consistente e unida deve permanecer na política da UE perante a Rússia, sendo que quaisquer mudanças de posturas entre a UE e a Rússia estarão baseadas no direito internacional e nos princípios subjacentes à ordem de segurança europeia, incluindo o Ato Final de Helsinque e a Carta de Paris (UNIÃO EUROPEIA, 2016a).

3.1.2.2 Quadro comum em matéria de luta contra as ameaças híbridas

O documento foi proposto pelo *Foreign Affairs Council* em 2015, desta forma o Alto Representante, em estreita cooperação com os serviços da Comissão e a Agência Europeia de Defesa, e em consulta com os Estados-Membros da UE, comprometeu-se a apresentar este quadro conjunto com propostas acionáveis para ajudar a combater as ameaças híbridas e promover a resiliência da UE e dos Estados-Membros, bem como dos parceiros da organização internacional (UNIÃO EUROPEIA, 2016b).

O documento afirma o mesmo proposto pela Estratégia Global, que a responsabilidade principal está com os Estados-membros da UE, uma vez que cada país possui vulnerabilidades distintas. Todavia, a proposta do documento se refere mais às ameaças comuns que todos os Estados-membros podem estar vulneráveis, já que existem alvos que podem visar redes e infraestruturas transfronteiriças. Essas ameaças podem ser abordadas de

forma mais eficaz com uma resposta coordenada a nível da UE, utilizando as políticas e instrumentos da UE, com base na solidariedade europeia, na assistência mútua e em todo o potencial do Tratado de Lisboa (UNIÃO EUROPEIA, 2016b).

Portanto, o documento prevê que a cooperação entre a OTAN e a UE pode ser estreitada no que condiz a intensificação da coordenação na área de defesa contra ameaças híbridas. No que tange a coordenação, a proposta segue uma resposta estratégica seguindo esses elementos: melhorar a conscientização, construir resiliência, prevenir, responder a crises e se recuperar (UNIÃO EUROPEIA, 2016b).

O documento Quadro comum em matéria de luta contra as ameaças híbridas foi concebido para fornecer uma base sólida para apoiar os Estados-Membros no combate coletivo às ameaças híbridas, apoiado por uma vasta gama de instrumentos e iniciativas da UE. Desta forma, o documento que possui 18 páginas na versão em inglês e pode ser resumido como uma estrutura conjunta que traz junto políticas e propostas de vinte e duas ações operacionais que visam:

> a) aumentar a sensibilização estabelecendo mecanismos específicos para o intercâmbio de informações entre os Estados-Membros e coordenando as ações da UE para fornecer comunicação estratégica;
>
> b) construir resiliência abordando potenciais setores estratégicos e críticos, como segurança cibernética, infraestruturas críticas (Energia, Transporte, Espaço), proteção do sistema financeiro contra uso ilícito, proteção da saúde pública e apoio aos esforços para combater o extremismo violento e a radicalização;
>
> c) prevenir, responder à crise e recuperar, definindo procedimentos eficazes a seguir, mas também examinando a viabilidade de aplicação da cláusula de solidariedade (artigo 222.º TFUE) e da cláusula de defesa mútua (art. 42.º, n.º 7, TUE), em caso de ocorre um ataque híbrido grave e variado;
>
> d) intensificar a cooperação e coordenação entre a UE e a NATO, bem como outras organizações parceiras, num esforço comum para combater as ameaças híbridas, respeitando os princípios de inclusão e autonomia do processo de tomada de decisão de cada organização (UNIÃO EUROPEIA, 2016b, s/p, tradução própria).

Como descrito, o documento foca em duas propostas principais: construir conscientização e resiliência. No quesito da conscientização, é proposto estabelecer mecanismos específicos para trocar informações com os membros da UE e focar em comunicação estratégica, aumentando a conscientização e fornecendo contribuições para os processos de avaliação de risco de segurança que apoiam a formulação de políticas nos níveis nacional e da UE. Sendo um pouco mais específico, a criação de

> Uma *Fusion Cell* da UE no Centro de Informações e Situação da UE (EU INTCEN) do Serviço Europeu para a Ação Externa (SEAE) oferece um foco único para a

> análise dos aspectos externos das ameaças híbridas. A *Fusion Cell* recebe, analisa e partilha informações classificadas e de fonte aberta de diferentes partes interessadas do SEAE, da Comissão e dos Estados-Membros especificamente relacionadas com indicadores e alertas relativos a ameaças híbridas. Em articulação com os organismos relevantes da UE e a nível nacional, a *Fusion Cell* analisará os aspectos externos das ameaças híbridas que afetam a UE e a sua vizinhança, a fim de analisar rapidamente incidentes relevantes e informar os processos estratégicos de tomada de decisão da UE, incluindo fornecer contribuições para as avaliações de risco de segurança realizadas a nível da UE (UNIÃO EUROPEIA, 2016b, s/p, tradução própria).

A proposta para construir resiliência possui áreas específicas de foco, como por exemplo a segurança cibernética, infraestrutura crítica, proteção do sistema financeiro contra uso ilícito e esforços para combater o extremismo violento e a radicalização. Para cada uma dessas áreas, a implementação das respostas estratégicas acordadas pela UE e pelos Estados-membros é um passo fundamental para reforçar a defesa nessas áreas. Um dos exemplos é a construção do *Centro Europeu de Excelência para Combater Ameaças Híbridas*, focando na pesquisa de como estratégias híbridas têm sido aplicadas, e como encorajar o desenvolvimento de novos conceitos e tecnologias dentro do setor privado e industrial para ajudar os Estados-membros construir resiliência (UNIÃO EUROPEIA, 2016b).

Após analisarmos até agora os principais documentos da OTAN e da UE, será analisado como os documentos influenciam a estratégia de defesa da República Tcheca contra ameaças híbridas. Portanto, compreende-se que ser membro das duas organizações traz responsabilidades por sua membresia, algo que será compreendido na próxima subseção.

3.2 Princípios e Política Estratégica da República Tcheca contra ameaças híbridas

Nesta subseção dois pontos são importantes para a compreensão holística da Estratégia de Defesa da República Tcheca contra ameaças híbridas. A primeira parte vai focar nos documentos oficiais ratificados pelo governo da República Tcheca, de autoria do ministério das Relações Exteriores ou do ministério da Defesa.

Para a segunda parte, será analisada a capacidade e a estratégia de defesa da República Tcheca, ou seja, quais são os recursos e as possíveis estratégias que a República Tcheca possui para aumentar a qualidade de suas respostas estratégicas contra ameaças híbridas.

3.2.1 Documentos de defesa da República Tcheca contra ameaças híbridas

Para iniciarmos a análise dos documentos de segurança da República Tcheca é necessário compreendermos que tais documentos são fortemente orientados pela a OTAN e a UE, principalmente pelo já exposto no início da seção (KORAN, 2013). Portanto todos os documentos estratégicos atuais se baseiam explicitamente ou implicitamente que ser membro da OTAN e da UE é a melhor garantia para a Segurança Nacional da República Tcheca. Consequentemente, o motivo pelo qual a República Tcheca confia nas instituições de segurança ocidentais fornece uma percepção importante das ameaças à segurança na República Tcheca e na política de segurança tcheca (REPÚBLICA TCHECA, 2015). Como podemos observar na Estratégia de Defesa de 2017, observamos que

> A Estratégia de Defesa é baseada na legislação nacional que regula a defesa, particularmente a Constituição Tcheca, tratados internacionais e atos relevantes. Decorre da Estratégia de Segurança da República Tcheca e reflete o Conceito Estratégico da OTAN, a Estratégia Global da UE e outros documentos nacionais, internacionais e aliados relevantes [...] De acordo com o Tratado do Atlântico Norte, as Forças Armadas Tchecas participam na preparação para a defesa colectiva do território dos aliados da OTAN, que inclui exercícios de treino, envolvimento nos procedimentos de planeamento da defesa da OTAN e participação em operações destacadas. As Forças Armadas também estão envolvidas em atividades para manter a paz e a segurança (REPÚBLICA TCHECA, 2017, p.6, tradução própria).

De forma cronológica as Estratégias de Segurança de 1999, 2001 e 2003 foram adotadas no contexto da integração gradual da República Tcheca nas estruturas de segurança ocidentais. Outro fator que integrou a República Tcheca à OTAN e a UE foi a experiência ativa que envolveu a resolução dos conflitos armados no Bálcãs na década de 90, tanto parte das missões de manutenção da paz da ONU quanto das operações de apoio da paz da OTAN. O documento da Estratégia de Segurança da República Tcheca de 2011 começou a ser escrito em 2010, o contexto sendo fornecido pelas questões de segurança no Afeganistão, o conflito armado russo-georgiano de 2008 e uma discussão sobre a adaptação do sistema de segurança tcheco em resposta às enchentes que ocorreram em 2006, 2009 e 2010 (KRIZ, 2021).

Ainda, outro estímulo externo mais importante que levou à atualização da Estratégia de Segurança da República Tcheca foi a adoção do novo Conceito Estratégico da OTAN em Lisboa em 2010. Essa estratégia enfatizou fortemente as ameaças à segurança que não representam maiores riscos para a própria República Tcheca, mas estavam associadas a um grau de risco para seus aliados dentro da OTAN. Na prática, isso significa que o terrorismo internacional se tornou a ameaça número um à segurança, com a proliferação de armas de

destruição em massa em segundo lugar, que não eram agendas primárias para a defesa nacional da República Tcheca (KRIZ, 2021).

A formulação da política de segurança nacional na República Tcheca é de responsabilidade do governo, tendo o Conselho de Segurança Nacional como principal órgão formulador de políticas de defesa (REPÚBLICA TCHECA, 2015). Esse conselho tem como principal função avaliar os riscos potenciais para o Estado, que podem criar um Estado de emergência; e submeter ao governo as propostas necessárias para diminuir ou eliminar esses riscos. Ainda, o aparato político-burocrático de defesa, os ministérios da Relações Exteriores e do Interior são importantes para contribuir na formulação das políticas e respostas contra as ameaças híbridas (KRIZ, 2021).

3.2.1.1 Estratégia de Segurança da República Tcheca de 2015

A Estratégia de Segurança da República Tcheca de 2015 que está vigente atualmente foi adotada no contexto de várias ameaças híbridas e eventos na política internacional. Descrevendo o contexto, houve a anexação da Ucrânia pela Rússia, que no documento é chamada de Guerra Híbrida. Outro ponto principal foram os ataques cibernéticos que os Estados membros da OTAN nos países bálticos sofreram (REPÚBLICA TCHECA, 2015).

A Estratégia de Segurança da República Tcheca de 2015 traz uma perspectiva que foca na cooperação internacional, pois o "enfraquecimento do mecanismo de segurança cooperativa e dos compromissos políticos e jurídicos internacionais na área de segurança é uma ameaça à segurança mais séria" (REPÚBLICA TCHECA, 2015, p. 13). Embora a Rússia não seja explicitamente mencionada nesse documento, a ideia é desenvolvida a partir das recentes estratégias utilizadas pela Rússia e dessa forma, o argumento afirma que para os Estados atingirem seus objetivos eles podem utilizar de instrumentos híbridos como "propaganda usando meios de comunicação tradicionais e novos, operações de inteligência de desinformação, ataques cibernéticos, pressões políticas e econômicas e o envio de militares não identificados" (REPÚBLICA TCHECA, 2015, p. 13). A percepção tcheca de defesa nesse documento possui uma abordagem centrada no Estado e também no indivíduo, observando uma crescente abordagem abrangente a partir de documentos produzidos por instituições internacionais de segurança, como a OTAN e a UE. De acordo com a atual Estratégia de

Segurança da República Tcheca de 2015, os interesses estratégicos que se relacionam com as possíveis ameaças híbridas são os seguintes:

> segurança e estabilidade, especialmente na área euro-atlântica; prevenção e gestão de conflitos locais e regionais e mitigação de seus impactos; manter o papel estabilizador global da ONU e aumentar sua eficiência; reforçar a coesão e a eficiência da OTAN e da UE e manter uma ligação transatlântica funcional e credível; reforçar a parceria estratégica OTAN, incluindo o reforço da cooperação no desenvolvimento complementar das capacidades de defesa e segurança; desenvolver o papel da OSCE na prevenção de conflitos armados, na democratização e na construção da confiança e segurança mútuas; um regime de controle de armas convencionais transparente e funcional na Europa; apoiar e desenvolver a cooperação regional; apoiar a estabilidade internacional por meio da cooperação com países parceiros; apoiar a democracia, as liberdades fundamentais e os princípios do Estado de Direito; salvaguardar a segurança interna e proteger a população; salvaguardar a segurança económica da República Tcheca e reforçar a competitividade da economia; salvaguardar a segurança energética, das matérias-primas e dos alimentos da República Tcheca e de um nível adequado de reservas estratégicas; salvaguardar a segurança e defesa cibernética da República Tcheca; prevenir e suprimir ameaças à segurança que afetam a segurança da República Tcheca e de seus aliados (REPÚBLICA TCHECA, 2015, p.3, tradução própria).

O conceito de Guerra Híbrida não apenas ganha certa popularidade na opinião pública, todavia as campanhas híbridas ou ameaças híbridas ganham relevância depois de 2012 nos principais documentos de segurança da República Tcheca como a Estratégia Nacional de Defesa de 2017, a Estratégia Nacional de Combate à Interferência Híbrida de 2021, além dos relatórios públicos da agência de inteligência da República Tcheca. Ainda, novas instituições foram estabelecidas, como o *Centro contra Terrorismo e Ameaças Híbridas* dentro do Ministério do Interior em 2017, e a *Comissão Permanente Parlamentar sobre Ameaças Híbridas* em 2020.

A Estratégia de Segurança Tcheca descreve que a República Tcheca está pronta para defender sua soberania contra métodos de guerra híbridos utilizados por Estados revisionistas que

> combinam meios militares convencionais e não convencionais com ferramentas não militares tais como a propaganda usando meios de comunicação tradicionais e novos, operações de inteligência de desinformação, ataques cibernéticos, pressões políticas e econômicas e implantação de militares não identificados (REPÚBLICA TCHECA, 2015, p.13, tradução própria).

O documento de 2015 faz várias referências sobre o flanco leste da OTAN, principalmente por que é a área que mais se torna conflitiva para o entorno estratégico Tcheco. Portanto, para compreendermos cronologicamente o desenvolvimento da Estratégia, seguiremos para a Estratégia de Defesa da República Tcheca de 2017.

3.2.1.2 Estratégia de Defesa da República Tcheca de 2017

Na Estratégia de Defesa da República Tcheca de 2017 que está atualmente vigente, a República Tcheca busca alcançar uma abordagem de segurança abrangente, que vá além da estrutura da segurança militar pura. Portanto, a abordagem da segurança abrangente é um princípio central da OTAN e da UE que é também afirmado na Estratégia de Defesa tendo como

> O princípio central da segurança da República Tcheca é salvaguardar a segurança do indivíduo e proteger sua vida, saúde, liberdade, dignidade humana e propriedade. Para colocar esse princípio em prática com sucesso, é necessário salvaguardar a segurança das instituições governamentais, incluindo sua plena capacidade operacional, e desenvolver processos e ferramentas que reforcem a segurança e a proteção da população. Garantir a segurança é principalmente dever do Governo; no entanto, a cooperação ativa dos cidadãos tchecos, incluindo pessoas jurídicas e indivíduos, com as autoridades da administração pública também é uma parte desejável do esforço para reduzir a probabilidade de as ameaças se materializarem. Isso fortalece a resiliência geral da sociedade às ameaças à segurança (REPÚBLICA TCHECA, 2017, p.15, tradução própria).

Na Estratégia de Defesa de 2017, é explícita a ameaça da Federação Russa e suas ambições imperialistas contra a República Tcheca e o ocidente, já que

> Desde 2012, a situação de segurança na Europa se deteriorou significativamente. No Leste Europeu, a Federação Russa realiza descaradamente suas ambições de poder, inclusive por meio do uso da força militar. Ao fazer isso, a Federação Russa viola as normas do direito internacional, incluindo a integridade territorial de seus estados vizinhos. Executou operações híbridas contra nações da OTAN e Estados-Membros da UE, incluindo atividades de desinformação direcionadas e ataques cibernéticos (REPÚBLICA TCHECA, 2017, p.7, tradução própria).

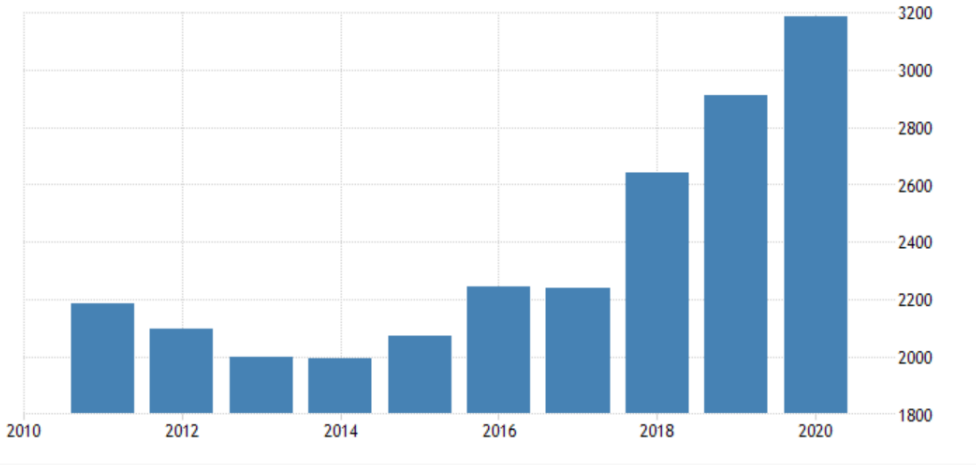
Ambos os documentos desenvolvem continuamente a orientação da política externa e de segurança que a República Tcheca tem seguido desde 1993, ou seja, orientação pró-ocidental e anti-Rússia, laços com a parceria transatlântica de segurança e construção da dimensão de segurança do processo de integração europeia.

Como afirmado no documento de Estratégia de Defesa, a República Tcheca está respondendo com o aumento do orçamento de defesa em detrimento da instabilidade do seu entorno estratégico. Ainda, afirma-se que a

> A tarefa mais urgente é reparar as consequências da queda no nível das capacidades de defesa e do pessoal, tecnologia e negligência material que se acumularam nos anos anteriores, e desenvolver as Forças Armadas Tchecas para que sejam capazes de cumprir suas tarefas (REPÚBLICA TCHECA, 2017, p. 7, tradução própria).

Quando analisamos de forma quantitativa, podemos analisar que após o ano de 2017 o orçamento em defesa aumentou, sendo que no ano de 2021 a estimativa de gastos em defesa em milhões de dólares é 4,013bi. Para os próximos anos, torna-se incerto os gastos em defesa já que o novo governo Tcheco não possui orçamentos precisos para muitas áreas públicas, assim como as Forças Armadas.

Gráfico 1 - Gastos de Defesa por ano pela República Tcheca



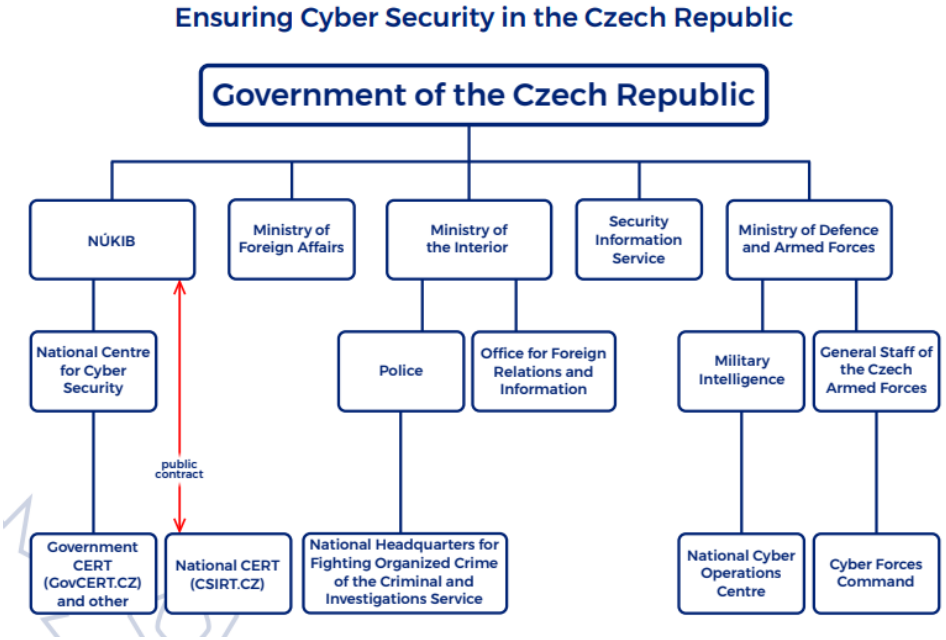
Fonte: World Bank (2021).

O primeiro-ministro Andrej Babis propôs o incremento dos gastos em defesa para 1.46% do PIB, planejado para 2021. Ainda, rejeitou todos os esforços contrários - principalmente pelo Partido Comunista - em reduzir os gastos em defesa. Como dito pelo próprio primeiro-ministro, a prioridade é conseguir chegar nos 2% de investimento em defesa como prometido durante a Cúpula de Bruxelas em 2021 (EURACTIV, 2021).

3.2.1.3 Estratégia Nacional de Segurança Cibernética da República Tcheca 2021-2015

Segundo o documento Estratégia Nacional de Segurança Cibernética da República Tcheca 2021-2015, a República Tcheca possui ambições de ser um líder cibernético regional e mundial. Portanto, o governo Tcheco vem financiando e renovando a sua estratégia de segurança cibernética contra as infinidades de ameaças que a dimensão ciber acaba por produzir. Desta forma, o governo da República Tcheca possui o seguinte esquema para fortalecer a sua segurança cibernética, como analisamos abaixo.

Figura 3 - Esquema de todas as instituições responsáveis pela segurança cibernética



Fonte: República Tcheca (2020, p. 8).

Segundo o documento, cada unidade demonstrada na figura acima possui uma função específica, principalmente especificada no documento que complementa a Estratégia Nacional de Segurança Cibernética da República Tcheca 2021-2015 chamado Plano de ação para a Estratégia Nacional de Segurança Cibernética da República Tcheca 2021-2015. Para fins didáticos, não será analisado o Plano de Ação, pois o resultado mais importante é compreender a complexidade das redes de proteção cibernética e a função primária do governo da República Tcheca em assegurar a segurança cibernética.

A Ciber Estratégia da República Tcheca (2020) pode ser estruturada e resumida em três pontos principais: a) confiança no espaço cibernético, b) alianças fortes e confiáveis e c) Sociedade Resiliente 4.0. Os três pontos correspondem com o futuro da direção estratégica dos próximos anos. A visão geral do "A República Checa terá uma sociedade e infraestrutura resilientes, atuará confiança no ciberespaço e enfrentará ativamente todo o espectro de ameaças enquanto fortalece alianças confiáveis" (REPÚBLICA TCHECA, 2020, p. 21, tradução própria).

Desta forma, pensando no três pontos citados pelo documento, o resumo dos objetivos estratégicos pode ser encontrado no quadro abaixo,

Quadro 1 - Resumo dos objetivos estratégicos da República Tcheca pelo documento Estratégia Nacional de Segurança Cibernética da República Tcheca 2021-2025

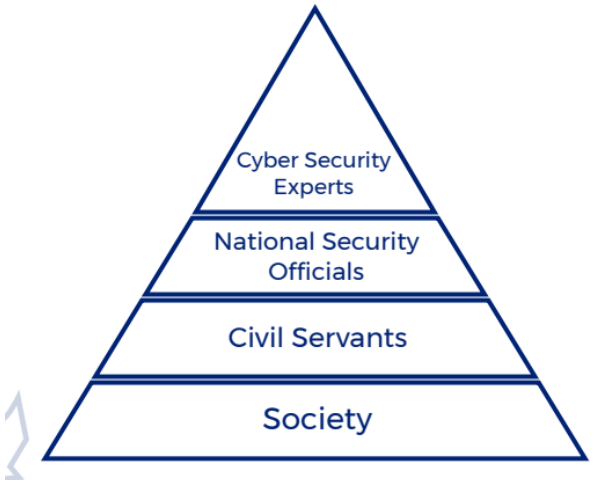
Objetivos Estratégicos		
Confiança do espaço cibernético	Alianças fortes e confiáveis	Sociedade Resiliente 4.0
1. Uma abordagem nacional com ênfase em formação compartilhamento, coordenação e cooperação 2. Desenvolvimento de capacidades e capacidades de segurança cibernética do estado 3. Fortalecimento da segurança e resiliência da infraestrutura 4. Desenvolvimento de previsão, detecção e reações ágeis para ataques cibernéticos • Uma estratégia de comunicação eficaz 5. Prevenção e combate ao cibercrime	1.Cooperação Internacional eficaz 2. Criação de alianças 3. Promovendo os interesses Tchecos interesses no exterior 4. Criação de diálogos em no âmbito internacional 5. Apoiar o comportamento aberto e seguro no ciberespaço 6. Exportação de conhecimento	1. Garantir a segurança da administração estatal/ digitalização do governo eletrônico 2. Alta qualidade do sistema de educação 3. Conscientização 4. Cooperação entre o Estado, o setor privado, e os cidadãos 5. Criação de uma ampla base de especialistas

Fonte: República Tcheca (2020, p. 21, tradução própria).

O documento reitera várias vezes a definição de como os documentos da OTAN e da UE conceituam como resiliência. Portanto, os objetivos estratégicos são focados na resiliência do Estado contra a vulnerabilidade cibernética, tanto na questão do hardware quanto social (REPÚBLICA TCHECA, 2020). Um dos esquemas que o documento demonstra é que a

resiliência faz parte de vários setores do Estado, como especificado abaixo,

Figura 4 - Sistema de Resiliência Cibernética da República Tcheca



Fonte: República Tcheca (2020, p. 19).

Segundo o próprio documento, a sociedade (usuários ordinários da internet) precisa se acostumar a se proteger, reconhecendo possíveis ameaças e compreendendo a dinâmica do ciberespaço. Exatamente por isso o documento afirma que vai investir na educação primária e secundária para modernizar o sistema educacional do país. Além disso, setores específicos da sociedade devem participar de cursos sobre higiene digital e como se proteger online, principalmente posições que demandem o conhecimento e uso de internet com dados sensíveis (REPÚBLICA TCHECA, 2020).

3.2.1.4 Estratégia Nacional de Combate à Interferência Híbrida

O documento mais importante e recente contra a Guerra Híbrida se chama Estratégia Nacional de Combate à Interferência Híbrida definindo os objetivos e determinando as capacidades de defesa essenciais para a proteção dos interesses nacionais da República Tcheca, que segue os princípios da Estratégia de Segurança contra ameaças híbridas. Tal documento tem um forte apelo para a segurança abrangente proposto pela OTAN e pela UE, já que enfoca todas as áreas vulneráveis que a República Tcheca possui, além da segurança humana (REPÚBLICA TCHECA, 2021).

Assim, o documento afirma que as ameaças híbridas podem incluir a influência aberta ou discreta das estruturas políticas e o processo de tomada de decisão na política, tribunais,

polícia, forças armadas, mídia e opinião pública. Os objetivos dos adversários seriam desestabilizar ou dividir a sociedade Tcheca e diminuir a confiança que os cidadãos possuem nas instituições e na orientação ideológica do país (REPÚBLICA TCHECA, 2021).

Ainda, as ameaças híbridas que podem afetar os interesses econômicos da República Tcheca, e os setores estratégicos que a República Tcheca cita são a dependência de recursos estratégicos de países estrangeiros, como petróleo, gás natural e combustível nuclear. Portanto, a República Tcheca afirma que vai garantir a defesa da abertura da economia e sua orientação para exportação, investimentos estrangeiros e empréstimos que estão em setores estratégicos da economia ou que levam à dependência estratégica de seus fornecedores (REPÚBLICA TCHECA, 2021).

Além da dependência de recursos estratégicos para o desenvolvimento da economia tcheca, também é necessário compreender que as ameaças híbridas podem ser manifestadas por meio do uso de tecnologias, como redes 5G e inteligência artificial utilizadas pelo setor privado, aquelas ameaças citadas de forma direta pela declaração da Cúpula de Bruxelas (REPÚBLICA TCHECA, 2021).

Outros riscos também tangem a corrupção, das ligações entre a diplomacia, o setor privado, a espionagem e o interesse de potências estrangeiras na República Tcheca. As ameaças híbridas podem incluir a mobilização de grupos de interesse (definidos por religião, etnia, nacionalidade ou idioma) ou grupos criminosos agindo contra os interesses de segurança da República Tcheca e violando a ordem pública. A interferência híbrida que busca atrasar ou paralisar os processos de tomada de decisão no domínio da defesa e segurança também apresenta um risco. Isso inclui a defesa coletiva da OTAN e a cooperação política e em defesa da UE (REPÚBLICA TCHECA, 2021).

Para continuarmos com o Estudo de caso da República Tcheca, será analisado se as capacidades e recursos de defesa que a República Tcheca são suficientes para garantir que os documentos estratégicos poderão ser assegurados com sucesso.

3.2.2 Capacidades e estratégias de defesa contra ameaças híbridas

Esta subseção analisa como o setor militar tem passado por um processo de transformação permanente, principalmente após a Revolução de Veludo em 1991, e também como os documentos de defesa influenciam as capacidades e recursos de defesa contra

ameaças híbridas. De acordo com o Ministério da Defesa da República Tcheca em dezembro de 2018, havia 33.084 efetivos, dos quais 25.105 eram soldados profissionais (REPÚBLICA TCHECA, 2019). Nas categorias de tecnologia de armamento pesado limitada pelo Tratado das Forças Armadas Convencionais na Europa, em 1º de janeiro de 2019, a República Tcheca possuía 116 tanques de batalha, 437 veículos blindados de combate, 179 sistemas de artilharia, 36 aeronaves de combate e 17 helicópteros de combate (REPÚBLICA TCHECA, 2019).

A República Tcheca também possui perspectivas futuras da estrutura das forças armadas nacionais e baseando-se no documento denominados *Build-up of the Armed Forces of the Czech Republic 2025 and Long Term Outlook for Defence 2035* (REPÚBLICA TCHECA, 2019). Para as expectativas de garantir a estratégia de defesa e a segurança nacional da República Tcheca, temos que o mínimo "para realizar as tarefas, as forças armadas precisarão aproximadamente 24.000 soldados profissionais, 3.600 funcionários civis e até 5.000 reservas ativas (do número total do departamento, aproximadamente 42.800 funcionários incluindo reservas ativas)" (KRIZ, 2021, p. 47, tradução própria). No que diz respeito às forças armadas tchecas, a questão fundamental no futuro próximo é a modernização das duas brigadas de combate existentes (7ª brigada mecanizada e 4ª brigada de implantação rápida), e a construção do terceiro componente principal, um regimento aerotransportado (REPÚBLICA TCHECA, 2019).

Quando analisamos as ameaças à segurança de aliados podem ser de natureza militar clássica ou podem assumir a forma vaga de guerra híbrida (REPÚBLICA TCHECA, 2019). Embora essas medidas vagas e híbridas possam assumir uma variedade de formas, a maior parte da atenção tem sido dada à sua dimensão informativa, ou às ameaças associadas à guerra de informação e ataques cibernéticos organizados (REPÚBLICA TCHECA, 2019).

Pensando na Guerra Informacional, o documento mais recente contra ameaças híbridas possui uma abordagem de segurança abrangente que vai além da estrutura da segurança militar pura. Portanto, A Estratégia Nacional de Combate à Interferência Híbrida nos mostra como a República Tcheca define objetivos e determina as capacidades de defesa essenciais para a proteção dos interesses nacionais e estratégicos que estão estabelecidos na Estratégia de Segurança da República Tcheca (REPÚBLICA TCHECA, 2021).

As capacidades e recursos de defesa nos documento se baseiam no conceito de resiliência, que é entendido como a capacidade de um Estado e de sua sociedade de lidar com

uma interferência híbrida sustentada e intensiva sem um impacto negativo significativo, e de corrigir imediatamente e restaurar uma funcionalidade completa em caso de dano. Portanto, é necessário que a sociedade, o estado e a infraestrutura crítica sejam resilientes, tornando possível respostas rápidas e eficazes contra ameaças híbridas (REPÚBLICA TCHECA, 2021).

Como parte do sistema de segurança nacional, a República Tcheca tem como objetivo fortalecer a capacidade de detecção de atividades híbridas hostis e a atribuição dos atacantes, para dessa forma reagir de forma adequada aos ataques. A atribuição pública dos perpetradores é uma decisão política tomada pelo Governo Tcheco, e portanto, o trabalho em conjunto dos atores estatais e não-estatais são necessários para fortalecer a soberania nacional (REPÚBLICA TCHECA, 2021).

O conceito de resiliência do Estado e da sociedade possui uma abordagem da segurança abrangente, ou seja, ela tem por si só o fundamento de compreender a segurança do indivíduo, todavia como objetivo também se tem o fortalecimento da infraestrutura crítica para manter sua funcionalidade suficiente para casos de interferência híbrida. Um dos exemplos desse fortalecimento das infraestruturas críticas é o emprego de um sistema de triagem robusto e transparente para investimentos estrangeiros em setores estratégicos da economia e empresas essenciais (REPÚBLICA TCHECA, 2021).

Ainda, tem-se que a República Tcheca pretende reduzir sua dependência estratégica de países com sistemas ideológicos e valores diferentes, pois tal dependência poderia ser usada contra os interesses e valores da República Tcheca. Portanto, um dos pontos é aumentar de forma consistente e coerente a conscientização da sociedade sobre a existência das ameaças híbridas e sua natureza. Assim, o combate à interferência híbrida na República Tcheca também faz parte de programas educacionais relevantes e eventos de divulgação. Para tanto, será intensificada a cooperação entre governo, setor comercial, sistema educacional, setor sem fins lucrativos e sociedade civil (REPÚBLICA TCHECA, 2021).

Tal cooperação entre diferentes atores tem como base a criação de um sistema de comunicação estratégica capaz de compartilhar informações com o público de maneira eficaz, coerente, confiável e oportuna. O governo da República Tcheca compreende que as medidas tomadas devem ser de forma contínua e preventiva, e desta forma tal sistema de comunicação deve ser baseado na coordenação e sincronização das atividades de comunicação entre todos os Ministérios e instituições públicas relevantes contando com uma abordagem sistêmica e

holística da República Tcheca na cooperação interministerial e a coordenação supra-ministerial (REPÚBLICA TCHECA, 2021).

O principal argumento para o aumento da capacidade de coordenação e compartilhamento de informações entre todos os atores nacionais importante é de abranger todo o espectro das possíveis ferramentas que podem ser utilizadas em ataques híbridos, e desta forma promover uma resposta coordenada e adequada. Portanto, com o objetivo de partilhar mais eficientemente informação, a digitalização do governo e da burocracia do país será necessário, como por exemplo a otimização das plataformas do Conselho de Segurança do Estado e a criação do Coordenador de Combate à Interferência Híbrida. Por exemplo, as lições que devem ser aprendidas com ameaças híbridas serão compartilhadas regularmente com um grupo de especialistas (REPÚBLICA TCHECA, 2021).

Na questão da dissuasão, o documento afirma que a adesão da República Tcheca à OTAN e à UE é o principal instrumento para desencorajar interferências híbridas, verificada a prontidão das respostas militares regularmente por meio de exercícios nacionais e internacionais. A solidariedade e o apoio mútuo dos Aliados da OTAN e dos Estados-Membros da UE representam um instrumento eficaz tanto para prevenir a interferência híbrida como para responder às suas manifestações específicas. Nesse quesito, a República Tcheca apoia ativamente a unificação e a solidariedade dos Aliados da OTAN e dos Estados-Membros da UE como por exemplo a possível identificação coletiva de atividades híbridas hostis, que podem dissuadir os perpetradores de continuar a atividade (REPÚBLICA TCHECA, 2021).

Nesse sentido, a República Tcheca contribuirá para as atividades de outras iniciativas internacionais, incluindo o Centro Europeu de Excelência para o Combate a Ameaças Híbridas em Helsinque, na Finlândia. Portanto, tem-se como importante o desenvolvimento da cooperação entre a OTAN e a UE, desenvolvendo capacidades de resposta projetadas para aumentar o custo e reduzir o benefício do emprego de interferência híbrida contra os interesses da República Tcheca (REPÚBLICA TCHECA, 2021).

Com medidas mais drásticas, a República Tcheca está pronta para responder a atividades híbridas hostis com medidas retaliatórias (incluindo sanções) e outros instrumentos, incluindo instrumentos de organizações internacionais das quais a República Tcheca é membro. Uma resposta adequada também envolverá o desenvolvimento de uma

capacidade para avaliar sua eficácia, que fornecerá feedback para informar o futuro curso de ação (REPÚBLICA TCHECA, 2021).

3.3 Conclusões preliminares

Neste capítulo, observou-se as perspectivas político-estratégicas da OTAN e da UE, para posteriormente considerar a influência que tais organizações possuem sobre a estratégia de defesa da República Tcheca e suas devidas capacidades e recursos de defesa. Desta forma, a membresia que a República Tcheca possui tanto com a UE quanto com a OTAN faz com que o país siga certas diretivas que tais instituições propõem, embora aceitando que a defesa da soberania Tcheca é de sua própria responsabilidade.

Quando analisamos as estratégias e planos de defesa da OTAN, analisamos que a principal estratégia é aumentar a capacidade de dissuasão contra quaisquer regiões que possuam poder bélico para desbalancear a posição internacional dos países do hemisfério norte. Todavia, o que pode ser concluído do aumento do poder de dissuasão dos países que fazem parte da OTAN é a natureza da Guerra Híbrida, ou seja, se o poder dissuasório necessita de um ataque formal do inimigo, a natureza da Guerra Híbrida faz com que atores estatais e não-estatais possam utilizar ameaças híbridas que interfiram nos membros da OTAN. Desta forma, observa-se que o *Readiness Action Plan* é um plano que não se defende de ameaças híbridas, mas seria importante na possibilidade de Guerra Híbrida, ou seja, caso algum Estado utilize de métodos regulares e irregulares de Guerra.

Portanto, decidiu-se analisar os documentos dos membros da OTAN e do Conselho do Atlântico-Norte para interpretar as perspectivas político-estratégicas que a OTAN possui da Guerra Híbrida. Desta forma, foi selecionada a Declaração da Cúpula de Bruxelas que possui um discurso securitizador na questão das ameaças híbridas, tais como os países que são possíveis ameaças e os fatores cibernéticos, tecnológicos e políticos que afetam a OTAN.

A outra instituição analisada foi a UE, em dois documentos principais e relativamente recentes que abrangem tanto a descrição das possíveis ameaças híbridas assim como ações que os Estados devem seguir para garantir sua soberania. O documento da Estratégia Global da UE compreende que qualquer ataque híbrido poderia ter consequências transnacionais, já que a interdependência dos países europeus é alta. Ainda, afirma que a cooperação com a

OTAN é necessária para a securitização das ameaças futuras que os países do hemisfério norte.

O segundo documento intitulado Quadro comum em matéria de luta contra as ameaças híbridas é uma proposta que envolve dois objetivos principais: aumentar a conscientização e a resiliência da sociedade em geral sobre possíveis ataques híbridos. Ainda, o documento traz vinte e duas ações para aumentar a conscientização e resiliência para diferentes setores, focando como o avanço tecnológico é um fator que está aumentando a vulnerabilidade dos Estados europeus.

Após a análise dos documentos da OTAN e da UE, iniciou-se a análise da estratégia de defesa da República Tcheca, compreendendo as principais instituições responsáveis por formular os documentos. De uma maneira geral, observa-se que a República Tcheca busca desenvolver seus documentos e sua capacidade de defesa contra ameaças híbridas, principalmente porque o entorno estratégico da República Tcheca está vulnerável a ameaças que compreendem todas as dimensões estratégicas.

Portanto, aqui é necessário pontuar que a Estratégia de Defesa da República Tcheca é afetada pelos desafios estratégicos que fazem parte do avanço tecnológico e da maior dependência da tecnologia. O documento mais pontual nessa questão é a Estratégia Nacional de Combate à Interferência Híbrida, que tenta definir as possíveis ameaças que a República Tcheca está vulnerável, e a especificação da abordagem compreensiva contra ataques híbridos.

Agora que as perspectivas da estratégia de defesa da República Tcheca foram definidas, reconhecendo suas limitações e especificidades, adentraremos no capítulo o qual serão selecionadas ameaças híbridas as quais a República Tcheca está vulnerável. Após a análise das ameaças híbridas selecionadas, será compreendido as respostas estratégicas da República Tcheca que fazem parte da Estratégia de Defesa da República Tcheca.

4 AMEAÇAS HÍBRIDAS RELACIONADAS AO AVANÇO TECNOLÓGICO E AS RESPOSTAS ESTRATÉGICAS DA REPÚBLICA TCHECA

Como descrito no capítulo anterior, é difícil mensurar quais ameaças híbridas os países estão mais vulneráveis, pois países possuem diferentes capacidades de defesa e as ameaças podem ser inúmeras, ou até desconhecidas. Desta forma, existe certa dificuldade em dizer quais setores estão mais vulneráveis e quais necessitam de mais financiamento, e por conseguinte, mais resiliência. Todavia, um dos pontos que o capítulo 1 e 2 nos mostram é o rápido avanço tecnológico e a incapacidade dos Estados seguirem tal velocidade de securitização, defasando respostas estratégicas que possam defender os países.

Pensando no fator *avanço tecnológico*, as ameaças híbridas que serão analisadas nessa seção estão relacionadas com a dependência do Estado e da sociedade estarem de alguma forma ligados com a dimensão cibernética da República Tcheca. Para a análise mais profícua da dependência do Estado e da sociedade em tecnologia, serão analisados três pontos que o relatório anual do NÚKIB de 2020 afirmou ser de extrema importância: os ataques cibernéticos à infraestrutura crítica da informação, a ciberespionagem e o aumento da desinformação (BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA, 2021)

Ademais, ataques cibernéticos à infraestrutura crítica da informação, e a ciberespionagem se tornaram frequentes nos últimos anos, já que concerne foram confirmados pelo *Security Information Service*[2]. A razão pela escolha da desinformação estratégica como ameaça híbrida, é pela recente preocupação que os Estados possuem com a quantidade infinda de informação que necessita ser filtrada. A censura das *fake news* acaba não sendo uma alternativa em democracias, já que um órgão governamental filtrando informações acaba por ir contra os princípios de liberdade de expressão. A análise compreenderá diferentes abordagens para tais ameaças, e se existem respostas estratégicas alternativas para as combater (KADLECOVA; SEMECKA, 2021).

4.1 Infraestrutura Crítica da Informação

A crescente vulnerabilidade cibernética da sociedade moderna é tema de discussões de longo prazo a nível da União Europeia e também da República Tcheca. Portanto, para entendermos mais como a infraestrutura crítica deu a possibilidade de existência para a

[2] Serviço Secreto da República Tcheca

infraestrutura crítica da informação, temos essa evolução dos sistemas de informação modernos e os meios de protegê-los contra ataques cibernéticos é um problema em discussão hoje na República Tcheca.

Para buscarmos uma definição para a infraestrutura crítica da informação, ela inclui os sistemas, serviços, redes e infraestruturas que fazem parte vital da sociedade, providenciando bens e serviços essenciais que são constituídos pela infraestrutura crítica. Alguns dos exemplos são a rede pública de telefone, a internet, e redes *wireless,* ou no caso,

> As infraestruturas críticas da informação sustentam a grande maioria das infraestruturas físicas e está aumentando à medida que essas infraestruturas estão interligadas. A natureza complexa das grandes redes distribuídas torna a camada cibernética extremamente difícil de avaliar e analisar discretamente, mas relativamente fácil de comprometer, dada a superfície de ataque em constante expansão (ou seja, dispositivos conectados) (CLEMENTE, 2013, p.16, tradução própria).

Para exemplificar melhor sobre possíveis infraestruturas críticas da informação, podemos considerar que as instalações as quais utilizam equipamentos especiais para controlar ou gerenciar as telecomunicações, o transporte aéreo, o setor financeiro, a rede elétrica e muitos outros serviços importantes para a economia e a atividade diária estão vulneráveis e tais ataques, além de tudo que envolve tais setores. Portanto, os responsáveis pelos ataques cibernéticos contra a infraestrutura crítica da informação tem como objetivo interromper o funcionamento dessas áreas pelo maior tempo possível (WILSON, 2014).

Além disso, a interrupção do funcionamento pode acarretar em outras atividades maliciosas como a sabotagem e a espionagem cibernética. Exemplos de ataques cibernéticos direcionados a vulnerabilidades de equipamentos de instalações incluem programas de computador maliciosos chamados *Flame* e *Stuxnet*, que teriam sido criados pelos EUA e Israel para vigiar instalações industriais nucleares críticas no Irã. Nos EUA, autoridades expressaram alertas de que ataques cibernéticos de nações, criminosos ou extremistas e terroristas podem em breve ultrapassar os tradicionais ataques terroristas violentos como a principal ameaça à segurança nacional dos EUA (WILSON, 2014).

Como em muitos países Europeus, a proteção da infraestrutura crítica da informação tornou-se a principal prioridade da República Tcheca desde 2011 com o estabelecimento dos blocos de construção para uma melhor segurança cibernética. Desta forma, a infraestrutura crítica da informação inclui os sistemas de comunicação e informação essenciais para o bom funcionamento de uma sociedade da informação (KADLECOVA; SEMECKA, 2021). Para

Kladecová e Semecká (2021) a garantia do funcionamento do Estado, bem como das instituições estatais e privadas, baseia-se em sistemas de informação que representam a chamada infraestrutura crítica, incluindo a infraestrutura crítica de informação.

Por conseguinte, para melhor entendermos como a República Tcheca define no ato nº181/2014, tanto a infraestrutura crítica quanto a infraestrutura crítica da informação, temos que

> Infraestrutura de informação crítica significa um elemento ou sistema de elementos da infraestrutura crítica no setor de sistemas de comunicação e informação no campo da segurança cibernética (REPÚBLICA TCHECA, 2014, s/p, tradução própria).

O próprio ato nº 181/2014 define que a infraestrutura crítica da informação envolve redes de computadores e transferência de dados pela internet que estão abertos e acessíveis sem fronteiras geográficas. Portanto, o ato define que a securitização e a proteção requer não apenas a iniciativa do Estado, mas também a assistência dos cidadãos da República Tcheca (REPÚBLICA TCHECA, 2014).

A próxima subseção versará mais como a securitização da infraestrutura crítica da informação acontece na República Tcheca, qual a autoridade responsável e a abordagem que tal autoridade utiliza no reforço da resiliência dos indivíduos e das instituições públicas e privadas.

4.1.1 Securitização da infraestrutura crítica da informação

Qualquer Estado que deseja securitizar sua infraestrutura crítica da informação, é necessário uma legislação abrangente de proteção da infraestrutura crítica da informação. Na República Tcheca, a principal legislação que dá suporte é o Ato em Segurança Cibernética nº 181/2014 e suas regulações complementares. O ato entrou em vigor em 2015 e foi emendado dois anos depois baseado na nova Diretiva da UE em Segurança da Rede e dos sistemas de informação em 2016 (KADLECOVA; SEMECKA, 2021; REPÚBLICA TCHECA, 2014).

O *National Cyber and Information Security Agency* é o principal órgão administrativo para securitizar a infraestrutura crítica da informação, incluindo a proteção de dados nos sistemas de informação e comunicação assim como a proteção de criptografia. Tais poderes são determinados também pelo ato nº181/2014 em matéria de segurança cibernética (REPÚBLICA TCHECA, 2014). Desta forma, o ato define as entidades reguladoras e suas

obrigações, além de dar a autoridade ao governo de declarar um Estado de emergência cibernética. Neste caso, uma das estratégias quando se é declarado o Estado de Emergência Cibernética é dar permissão à *National Cyber and Information Security Agency* para regular os provedores de internet, que normalmente não possuem nenhuma regulação. Na prática, essa medida deve ser utilizada apenas em casos específicos, por que a cooperação entre os provedores de internet e o time de resposta do governo (CERT) são normalmente feitas após consultas e recomendações de forma não-coercitiva (REPÚBLICA TCHECA, 2014).

Desta forma, o Estado de Emergência Cibernético nunca foi declarado, todavia ele é utilizado extensivamente em simulações de nível nacional e internacional. É ainda interessante notar que o Estado de Emergência Cibernético é algo único que a República Tcheca possui comparando no contexto do gerenciamento internacional de crises cibernéticas (BOEKE, 2018). Com isso dito, a declaração do Estado de Emergência Cibernética precede qualquer outro Estado de Emergência e dá ao *National Cyber and Information Security Agency* a oportunidade de lidar com a emergência sem a ajuda de outras instituições. Caso o *National Cyber and Information Security Agency* não seja capaz de resolver a situação em 30 dias, o Primeiro-Ministro pode declarar o Estado de Emergência tendo como base o Ato de Crises Act No. 240/2000 Coll., 2000. Tal política é única para a República Tcheca, pois nenhum outro Estado Europeu possui qualquer dispositivo legislativo para declarar um Estado de Emergência Cibernético, assim como nenhuma política da UE. Portanto, entende-se que nenhum outro membro da UE possui a possibilidade do uso do Estado de Emergência que seja específico de uma legislação cibernética (REPÚBLICA TCHECA, 2014).

Todavia, segundo Kadlecová, Bagge, Borovicka e Semecká (2017), como todas as partes interessadas da sociedade civil tiveram a chance de influenciar o Ato em Segurança Cibernética, o Ato é entendido mais como um resultado da cooperação de inúmeras partes tal que um decreto autoritário pelo governo. Portanto, o setor privado foi consultado inúmeras vezes para que a abordagem e a regulação cibernética tivessem boas relações, e consequentemente desenvolvendo uma cooperação mútua entre o governo, o setor público e privado (KADLECOVÁ; SEMECKÁ, 2021).

Um dos pilares que a legislação de segurança cibernética foram criadas e as quais contribuem para uma maior confiança entre as partes é a mínima quantidade de coerção que o Estado aplica. Analisando dessa forma, parece contra intuitivo pensar que a menor quantidade possível de coerção aplicada fornece mais segurança e resiliência para a infraestrutura crítica

da informação, todavia como reiterado por Kadlecová e Semecká (2021), os operadores das infraestruturas críticas da informação possuem liberdade para escolher como será implementado as medidas de segurança da Lei de Segurança Cibernética. Um dos pontos é compreender que a principal responsabilidade da proteção da informação está com os devidos operadores, e como cada operador está familiarizado com sua própria infraestrutura, eles sabem melhor como proteger e fortalecer seus sistemas.

Portanto, a legislação da República Tcheca entende que a Segurança Cibernética é um campo de rápido desenvolvimento e para isso a legislação nacional deve ser flexível para acompanhar as modificações tecnológicas e as possíveis ameaças cibernéticas que podem aparecer (REPÚBLICA TCHECA, 2020).

Desta forma, como analisamos no capítulo 2 o documento chamado Estratégia Nacional de Segurança Cibernética da República Tcheca é o que mais versa sobre a proteção da infraestrutura crítica da informação (REPÚBLICA TCHECA, 2020). Logo, o documento afirma que a República Tcheca vai continuar a atualizar as leis na busca de efetividade, regulações na questão de segurança cibernética para melhor oferecer respostas para diferentes desafios que possam surgir. Ainda, afirma-se que esse processo é direcionado pela implementação da lei da UE na legislação nacional e diferentes padrões legislativos internacionais.

Portanto, a securitização da infraestrutura crítica da informação vai continuar principalmente a aumentar a resiliência de sua infraestrutura de informação estratégica. Tal estratégia é definida e reforçada pela confiança e cooperação mútuas entre todos os órgãos mandatados pelo Ato em Segurança Cibernética. Segundo o documento, tais órgãos são:

> a pedra angular da segurança cibernética e, subsequentemente, nacional. Ataques cibernéticos contra os sistemas de informação e comunicação desses órgãos e indivíduos podem enfraquecer e possivelmente ter resultados devastadores para a economia nacional ou limitar a capacidade de atender às necessidades fundamentais da população. A falha de um componente da infraestrutura pode levar à falha de outras partes, causando um efeito dominó. É por isso que sua defesa e segurança são a mais alta prioridade para o país e é necessário aumentar continuamente a resiliência da infraestrutura (REPÚBLICA TCHECA, 2020, tradução própria).

Segundo o documento, a República Tcheca é o líder europeu na disseminação e uso de tecnologias modernas, resultando na transformação da sociedade Tcheca numa sociedade da informação. Todavia, a insuficiente higiene digital, educação digital e o senso crítico são problemas que estão associados com essa transformação da sociedade. Portanto, a República Tcheca possui a estratégia da sociedade resiliente 4.0, que seria

> um estado em que as ameaças cibernéticas são minimizadas e toda a sociedade pode aproveitar os benefícios das tecnologias modernas e integrá-las em suas vidas diárias. A segurança cibernética deve, portanto, permanecer uma parte intrínseca da vida cotidiana das pessoas (REPÚBLICA TCHECA, 2020, tradução própria).

Para concluirmos a ideia principal de como a República Tcheca defende sua infraestrutura crítica da informação, temos que o espírito de confiança mútuo é um dos pilares de como tal setor é securitizado. Desta forma, o *National Cyber and Information Security Agency* está sempre em contato com os operadores da infraestrutura crítica da informação, tendo seu principal objetivo ajudar os operadores a manter o maior nível possível de segurança (KLADECOVÁ, SEMECKÁ, 2021).

Portanto, o principal ponto do *National Cyber and Information Security Agency* não é utilizar da coerção para encontrar erros e impor penalizações, mas sim garantir a máxima segurança dos sistemas e das redes. Desta forma, um dos pontos interessantes e peculiares da República Tcheca é,

> Esta *auditoria para melhorar* é bastante única na administração estatal Tcheca e aumentou ainda mais a confiança mútua entre a autoridade nacional de segurança cibernética e os operadores das infraestruturas críticas da informação (KADLECOVA; BAGGE; BOROVICKA; SEMECKA, 2017, p.20, tradução própria).

Logo, a confiança entre os operadores da infraestrutura crítica da informação e o Estado é vital. Sem confiança, os operadores têm dificuldades em compartilhar informações e a estratégia de comunicação acaba por fracassar. Desta forma, percebe-se que a criação de um ambiente o qual todas as partes interessadas formulam as regras e a devida legislação, onde o Estado acaba sendo mais um parceiro tal que uma autoridade que vigia e pune, e o qual as soluções dos erros são destacadas, são os pilares da Segurança Cibernética da República Tcheca contra ameaças à infraestrutura crítica da informação que tem funcionado por ora (KLADECOVÁ, SEMECKÁ, 2021).

4.2 Ameaças híbridas relacionadas a ciberespionagem

Para definirmos a ciberespionagem, será utilizada uma abordagem da comunidade internacional, que compreende a ciberespionagem como fruto do progresso tecnológico nas sociedades. Desta forma, uma definição que pode ser compreendida tanto em âmbito global quanto para a República Tcheca é a abaixo,

> A ciberespionagem é definida como o uso intencional de computadores ou atividades de comunicação digital em um esforço para obter acesso a informações confidenciais sobre um adversário ou concorrente com a finalidade de obter uma vantagem ou vender as informações confidenciais por recompensa monetária (COLEMAN, 2008, s/p, tradução própria).

Essa subseção vai compreender a ciberespionagem como componente importante da Guerra Híbrida, principalmente no caso Tcheco. Os relatórios do *Security Information Service* demonstram que a República Tcheca está cada vez mais vulnerável à ciberespionagem, reconhecendo que os dados podem ser utilizados de forma política (nesse caso, utiliza-se de ciberespionagem para prever possíveis políticas domésticas e externas do país) ou simplesmente com fins lucrativos (como para a venda comercial de banco de dados com informações sensíveis) (BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA, 2021)

Segundo Weissbrodt (2013), a ciberespionagem difere da espionagem tradicional por diferenças substanciais e que prejudicam a sua identificação. Nesse caso, Weissbrodt afirma que para os países, utilizar de ações legais ficam mais fáceis caso espiões sejam revelados no território inimigo, já que o Estado não vai extraditar espiões inimigos para que sejam condenados no estrangeiro. A diferença ocorre quando se é muito mais complicado encontrar os ciber espiões que se encontram em território inimigo, reduzindo as oportunidades para que espiões inimigos sejam presos.

Os Estados e a República Tcheca podem utilizar as mesmas leis de espionagem tradicional para a ciberespionagem, todavia os problemas de encontrar os espiões e de acusar pessoas de ciberespionagem acabam por dificultar a ação dos Estados contra esse tipo de ameaça híbrida. Existem duas soluções principais para compreender a ciberespionagem, a primeira compreende que a ciberespionagem deve ser entendida como a mesma ameaça da espionagem, ou seja, as leis internacionais seriam aplicadas tanto para a espionagem quanto para a ciberespionagem. A segunda solução compreende que é a ciberespionagem é mais intrusiva que a espionagem tradicional, passível de roubar bancos de dados (*big data*), sendo que atores estatais ou não estatais podem efetuar o ataque, e dessa forma é necessário a criação de nova legislação que compreenda a ciberespionagem (WEISSBRODT, 2013).

Pensando na segunda solução, Handler (2012) propõe que ao invés de criar um tratado cibernético "[a] melhor opção é focar no desenvolvimento da prática estatal de forma racional que desenvolve arranjos onde o regime legal existente não é o ideal para as operações do ciberespaço" (Handler, 2012, p.237, tradução própria). Em outras palavras, Handler (2012)

propõe que os Estados foquem em práticas que correspondem práticas legais atuais que ajude a desenvolver novas normas de direito internacional consuetudinário contra a ciberespionagem. A República Tcheca pode se beneficiar com a estratégia de utilizar a jurisprudência, pensando que a ciberespionagem deve se transformar à medida que avanços tecnológicos acontecem.

4.2.1 Respostas Estratégicas contra a ciberespionagem

Com a análise dos documentos e dos relatórios do *Security Information Service*, entende-se como responsabilidade primária do *Security Information Service* contra a ciberespionagem. Todavia, há duas outras instituições que compartilham informações sobre ciberespionagem que se chamam *Office for Foreign Relations* e *Information and Military Intelligence*. De acordo com os documentos oficiais, o *Office for Foreign Relations* é responsável por

> [...] principalmente na inteligência relacionada às ameaças impostas pelo terrorismo internacional, proliferação de armas de destruição em massa e seus componentes, crime econômico, migração ilegal, várias formas de extremismo político (VNĚJŠÍ ZPRAVODAJSKÁ SLUŽBA ČESKÉ REPUBLIKY, 2021, tradução própria).

O *Military Intelligence*, por outro lado, tem sua responsabilidade na ciberespionagem, todavia focada na ciberespionagem de dados e instituições militares. “O Centro é responsável por minimizar o impacto de ataques como, por exemplo, ataques cibernéticos usados como parte de operações militares ou híbridas, espionagem cibernética direcionada à aquisição de informações de militares” (KADLECOVA; BAGGE; BOROVICKA; SEMECKA, 2017, p. 28).

Portanto, segundo os documentos analisados, por mais que as instituições responsáveis pelas respostas estratégicas da ciberespionagem são variadas, a instituição de mais importância é o *Security Information Service*. É essa mesma instituição que produz relatórios anuais sobre inteligência em geral, incluindo ciberespionagem. Portanto, o *Security Information Service* é o serviço de contrainteligência que identifica atividades de outros países estrangeiros e por pessoas físicas agindo contra os interesses da República Tcheca. O *Security Information Service* rastreia essas atividades e coleta informações, além de ter como

o objetivo de proteger informações sensíveis e secretas para outras nações (SECURITY INFORMATION SERVICE, 2021).

As respostas estratégicas do *Security Information Service* acabam por ser de difícil análise, já que quando analisamos o documento que legitima todas as ações do *Security Information Service*, não existe nenhuma seção dos poderes e permissões que possui contra a ciberespionagem. Ainda, o próprio website afirma que uma parte significante das atividades de inteligência, especialmente a preparação para operações, não podem ser resumidas ou abordadas por nenhuma norma legal ou por estritas definições válidas indefinidamente (SECURITY INFORMATION SERVICE, 2021).

Como respostas estratégicas contra a ciberespionagem, pode-se inferir que o processamento e a análise da contrainteligência do *Security Information Service* tem duas funções principais:

> a) a função informativa – os destinatários legalmente estipulados são informados sobre as atividades, interesses e intenções das potências estrangeiras na República Tcheca
>
> b) função preventiva – os serviços de contra-inteligência sugerem ou adotam medidas destinadas a dificultar ou interromper as operações de inteligência estrangeira na República Tcheca (SECURITY INFORMATION SERVICE, 2021, s/p, tradução própria).

Além disso, por mais que as funções informativas e preventivas sejam discretas, no dia 28 de janeiro de 2022, o *National Cyber and Information Security Agency* publicou no seu website um relatório chamado *aviso sobre o risco aumentado de ciberespionagem ou ataques de ransomware contra a República Tcheca*. Segundo o documento, devido à atual situação geopolítica do leste europeu, em especial a Ucrânia, há um aumento dos riscos de ciberespionagem e ataques spyware (NÚKIB, 2022). O documento afirma que as instituições nacionais e estratégicas sofrem mais riscos, mas quaisquer entidades podem estar em perigo, já que os atores dos ataques buscam vulnerabilidades dos sistemas para conseguir acesso às informações. Assim, o documento recomenda a identificação de 19 tipos de técnicas de ataques cibernéticos relacionados à ciberespionagem e 14 das vulnerabilidades mais comuns de sistemas de informação. Abaixo estão descritas todas as técnicas de ciberespionagem mais utilizadas no leste europeu, e desta forma, para cada uma das opções há diferentes formas de proteção e defesa. A recomendação do *National Cyber and Information Security Agency* é a

vigilância desse tipo de ciberespionagem pela frequência e vulnerabilidade que a maioria dos sistemas possuem (NÚKIB, 2022).

Quadro 2 - Técnicas de ciberespionagem descritos pela *National Cyber and Information Security Agency*

Técnica	Definição
T1059 (Command and Scripting Interpreter)	Utilização de linha de comando para executar código malicioso.
T1218 (Signed Binary Proxy Execution)	Utilização de binários legítimos para executar proxies de código malicioso.
T1543 (Create or Modify System Process)	Utilização da capacidade de criar ou modificar processos de nível sistema operacional para executar novamente o código malicioso.
T1053 (Scheduled Task/Job)	Utilização de agendamento de tarefas para execução inicial ou recorrente de código malicioso.
T1003 (OS Credential Dumping)	Tentativa de imprimir as informações de login para obter as informações da conta do SO e software.
T1055 (Process Injection)	Inserção de código malicioso em um processo legítimo, em particular para evitar a detecção.
T1027 (Obfuscated Files or Information)	Dificultar a detecção ou análise de um arquivo malicioso criptografando-o ou por senha
T1105 (Ingress Tool Transfer)	Movimentação de ferramentas ou outros arquivos por um invasor externo para sistema comprometido.
T1569 (System Services)	Utilização de serviços de sistema legítimos para executar código ou programa

	malicioso.
T1036 (Masquerading)	Modificar códigos e arquivos maliciosos para mantê-los seguros considerando os instrumentos legítimos ou inofensivos.
T1486 (Data Encrypted for Impact)	Criptografia de dados no sistema de destino usando ransomware
T1082 (System Information Discovery)	Uma tentativa de obter informações detalhadas sobre o sistema operacional e o hardware
T1497 (Virtualization/Sandbox Evasion)	Meios usados para detectar e evitar a virtualização ou ambiente analítico.
T1566 (Phishing)	E-mails de phishing que podem conter um anexo malicioso na forma de link ou documento anexo.
T1078 (Valid Accounts)	Utilização de contas de usuário legítimas que um invasor comprometeu (por exemplo, conhecimento ou roubo de dados de login).
T1190 (Exploit Public-Facing Application)	Explorar vulnerabilidades em aplicativos ou programas abertos à rede Internet.
T1133 (External Remote Services)	Uso indevido de serviços remotos (por exemplo, VPN) para obter a principal aproximação.
T1595 (Active Scanning)	Verificação ativa de intervalos de IP e sistemas vulneráveis.
T1110 (Brute Force)	Usando força bruta para obter acesso a contas quando senhas não são conhecidas ou seus hashes são obtidos.

Fonte: NÚKIB (2022, s/p, tradução própria)

Portanto, observa-se a preocupação do *Security Information Service* e do *National Cyber and Information Security Agency* em informar a sociedade sobre as possíveis modalidades de ciberespionagem que podem ocorrer nos sistemas. Além disso, é explicado como cada técnica é utilizada e como se defender, garantindo assim a resiliência da sociedade, já que é uma nota pública à sociedade tcheca.

4.3 A ameaça híbrida da guerra informacional e da (des)informação

Desde que o conceito de guerra existiu nas sociedades humanas, sempre foi conectado com a informação. Portanto, decisões e ações de quaisquer naturezas podem ser compreendidas em termos informacionais. Desta forma, controlar o fluxo da informação e suas características podem representar um fator importante em influenciar as condutas de certos alvos, e logo pode ser utilizada como uma arma para alcançar objetivos políticos (FILIPEC, 2019).

Para clarificar, essa sub-seção terá como objetivo compreender o principal ambiente o qual a guerra informacional acontece e as táticas de desinformação que ocorrem na República Tcheca. Portanto, será definido como uma ameaça principal à República Tcheca pelo fato dos documentos citarem a desinformação como um grande problema não somente na sociedade Tcheca, mas também no mundo. Os termos são abrangentes e podem também ser nomeados como *disseminação de informações falsas* ou nas mídias de massa também conhecido como *fake news*, todavia esse trabalho toma como principal termo a desinformação, já que para os documentos tchecos o uso de *fake news* está dentro da categoria de desinformação.

A desinformação possui várias definições e conceitos sobrepostos que podem variar de país para país, todavia para este trabalho será utilizada a definição utilizada pelo ministério do interior da República Tcheca:

> disseminação sistemática e intencional de informações falsas principalmente por atores estatais ou suas afiliadas contra o estado estrangeiro ou a mídia com o objetivo de influenciar o processo decisório ou a opinião daqueles que tomam decisões (REPÚBLICA TCHECA, 2019, s/p, tradução própria).

Desta forma, quando analisamos essa definição pelo Ministério do Interior, o primeiro problema que analisamos é como as notícias podem ser tendenciosas na forma como é apresentada ou fraseada, dependendo da intenção do escritor ou jornalista. O segundo problema que encontramos são outros sites que relatam notícias que não possuem evidências

na realidade, normalmente também pode ser considerado como *clickbaits*, já que tal conteúdo online atrai a atenção para que os visitantes cliquem no link para gerar renda de publicidade. Ainda, temos outras possibilidades como Estados espalhando propaganda como parte da estratégia de informação para desestabilizar seus adversários, mas também indivíduos motivados por vinganças pessoais ou crenças em teorias da conspiração (FILIPEC, 2019).

Seja qual for a motivação ou vetor da desinformação, a velocidade com que as notícias falsas podem se espalhar é multiplicada pelas mídias sociais e algoritmos computacionais que aumentam as suas visualizações. Para compreendermos mais como esses algoritmos funcionam, esses softwares mostram ao usuário apenas conteúdos semelhantes aos quais ele gostava antes, criando bolhas de filtro ou repetições destes conteúdos e influenciando ao usuário apenas ler e compartilhar informações nas quais já acredita (FILIPEC, 2019).

Desta forma, o usuário acaba por confirmar suas visões através dos conteúdos que encontra repetidamente por causa dos algoritmos, e desta forma, cria visões de mundo equivocadas mesmo quando tais conteúdos são refutados por fontes externas. Esse fenômeno também pode ser chamado de viés de confirmação nos usuários, já que "é a tendência de se lembrar, interpretar ou pesquisar por informações de maneira a confirmar crenças ou hipóteses iniciais" (PLOUS, 1993, p.223).

Contra essa possibilidade de viés de confirmação, redes sociais como o Facebook e o Google introduziram processos e softwares capazes de identificar e verificar a veracidade de cada notícia. Todavia, como vamos ver com os limites entre democracia e censura na próxima sub-seção, temos que tal solução possui limitações. Desta forma, podemos verificar que até a inteligência artificial e a tecnologia possuem dificuldades para verificar a veracidade das possíveis *fake news* (RYCHNOVSKA; KOHUT, 2018).

Portanto, partindo da ideia de que as empresas de tecnologia não podem resolver tal problema sozinhas, os Estados estão cada vez mais envolvidos na securitização das *fake news*, tendo como principal base o estabelecimento de agências estatais e instituições financiadas pelo Estado para verificar as *fake news.* Um dos exemplos que vamos explorar será como a República Tcheca criou em 2017 uma unidade dentro do Ministério do Interior para esse fim, enquanto a Alemanha e a Indonésia estão considerando o exemplo Tcheco e o estabelecimento de unidades semelhantes para combater quaisquer notícias que são caluniosas, falsas, enganosas, e que espalham o ódio (FILIPEC, 2019).

Historicamente, a intervenção do Estado no controle e censura de determinados meios de comunicação sempre foi existente, todavia normalmente confinada apenas a Estados autoritários. Nos dias atuais, com o desenvolvimento tecnológico que exploramos nos capítulos passados, os Estados democráticos estão tentando afirmar quais são as fontes de informação mais verdadeiras. Como o perigo em todo Estado que possui censura, um temor é que essas medidas possam levar a supressão futura de pontos de vista divergentes e comprometer a liberdade de expressão nas democracias estabelecidas (RYCHNOVSKA; KOHUT, 2018).

Portanto, quando analisamos a República Tcheca, podemos perceber que quando a instituição responsável pela análise de ameaças híbridas e *fake news* se diz como única fonte de verdade, isso pode levar a uma erosão da confiança no Estado. De forma irônica não somente os indivíduos podem desconfiar mais do Estado, mas também a própria classe política pode duvidar das análises e relatórios feitos pelo governo Tcheco (RYCHNOVSKA; KOHUT, 2018).

Além disso, para Filipec (2019), se o Estado tem poder limitado para lidar com as *fake news* e a influência de potências estrangeiras, a literatura acadêmica atual sugere que os cidadãos sejam mais críticos em relação às informações que consomem online. Isso exige que o Estado financie habilidades de alfabetização digital para avaliar criticamente se as notícias que lêem são autênticas ou não. Todavia, alguns estudos mostram que mesmo pessoas com certo nível de educação possuem dificuldades para distinguir *fake news*. A incapacidade cada vez maior dos indivíduos de não conseguirem verificar notícias falsas faz com que um esforço do Estado seja necessário.

Desta forma, cidadãos podem ser manipulados para fazer decisões que são contra seus próprios interesses e de sua nacionalidade, proporcionando danos. Alguns dos exemplos são o referendo do Brexit no Reino Unido e as eleições presidenciais nos Estados Unidos da América em 2016, os quais transformou a situação geopolítica desses países. Nos dois casos fake news e desinformação foram cruciais para os resultados das votações, no caso do Brexit, bots russos entregaram mais de 10 milhões de impressões no twitter durante o referendo (89UP, 2021). Por conseguinte, para Cizik (2017) a guerra informacional baseada na desinformação tem um efeito individual, pois acaba por fazer os indivíduos desconfiarem mais dos conhecimentos dos indivíduos e das instituições.

Assim como apontado por Cizik (2017), a desinformação é conduzida principalmente na área social, pois os principais alvos são cidadãos e suas capacidades de distinguir o que é correto ou incorreto com a intenção de os confundir. Desta forma, acadêmicos, jornalistas e políticos tendem a relacionar a poluição informacional que acontece atualmente com o surgimento da chamada política pós-verdade, sugerindo que explicações científicas perdem relevância aos olhos do públicos em comparação com as narrativas falsas espalhadas por fontes de mídia alternativas (BERLING; BUERGER, 2017).

4.3.1 A securitização da guerra informacional e da (des)informação pela República Tcheca

A desinformação está presente em todas as sociedades, e desta forma muitos países securitizam o campo da informação para garantir proteção aos indivíduos e a devida punição aos infratores. Todavia, os países democráticos possuem mais barreiras à medida que tentam encontrar o equilíbrio entre a liberdade de expressão e a proteção dos direitos básicos de cada um, já que a censura não é aceitável em democracias liberais.

Para adentrarmos mais na perspectiva da República Tcheca, as campanhas de desinformação estrangeiras foram avaliadas como uma séria ameaça à segurança interna e uma das recomendações para combater essas formas de guerra híbrida era “estabelecer departamentos dentro das instituições governamentais relevantes para a avaliação de campanhas de desinformação e outras manifestações de influência de poder estrangeiro” (REPÚBLICA TCHECA, 2016, p. 61).

Segundo o serviço de inteligência Tcheco, a República Tcheca se tornou um laboratório para a Guerra Híbrida Russa (BEZPECNOSTNÍ INFORMACNI SLUZBA, 2020). Importante lembrar que pela situação geográfica da República Tcheca e seu passado, ‘menos Europa’ automaticamente significa ‘mais Rússia’. Desta forma, podemos analisar que a política da Rússia de infringir medo é de interesse nacional, e desta forma um dos objetivos que a Rússia tem é ganhar mais suporte da sua política externa pela utilização da estratégia de desinformação (RYCHNOVSKA; KOHUT, 2018).

Desta forma, uma resposta para esse problema foi o estabelecimento do Centro contra terrorismo e ameaças híbridas (*Centrum proti terorismu a hybridním hrozbám*) em 2017, como descrito no capítulo 2. Portanto, como explicitado acima, um dos pontos e dificuldades

que os Estados possuem é combater a desinformação à custa de direitos básicos, como o direito de expressão, e desta forma o atual presidente da República Tcheca, Milos Zeman, sugeriu que o Centro infringiria a liberdade de expressão (REUTERS, 2021).

É exatamente por isso que a República Tcheca encontra barreiras para penalizar a desinformação, já que tal termo não existe no sistema legislativo tcheco. Por não existir um termo específico para a desinformação, a República Tcheca possui diferentes crimes que podem ser tipificados como desinformação, como no Código Penal, Capítulo II ofensas criminais contra a liberdade, direitos de privacidade e pessoais e confidencialidade apenas no caso de § 181 violação de direitos alheios, § 184 difamação, § 345 falsas acusações, § 355 difamação da nação, raça, etnias ou outros grupos de pessoas, § 356 instigação de ódio contra grupos de pessoas ou da supressão de direitos e liberdades, § 357 divulgação de notícias alarmantes, §364 incitação a ofensas criminais, § 365 aprovação de ofensas criminais, § 404 expressar simpatias por movimentos que procuram suprimir os direitos humanos e liberdades de acordo com o ato nº 40/2009 (FILIPEC, 2019).

O código penal não é apenas a única ferramenta contra a desinformação, já que é mais uma finalidade que um meio. Quando analisamos outros países, podemos encontrar diferentes respostas ao problema, como por exemplo promover contra-narrativas no contexto doméstico, promover contra-narrativas internacionalmente, ou fornecer uma história da perspectiva do próprio Estado para ir contra campanhas de desinformação (HELLMAN; WAGNSSON, 2017).

Com os obstáculos que foram explicitados acima, a securitização da guerra informacional ou da desinformação acontece primariamente com a emergência de uma nova rede de profissionais composta por *think tanks* e jornalistas que conseguem atingir o público e influenciar *policy-makers*. Desta forma, esta rede é formada por profissionais de diversos campos, e logo elas fazem conexões entre diferentes instituições. Um dos exemplos é o *European Values* e o Ministério do Interior da República Tcheca, que possuem boas conexões e desenvolvem políticas em conjunto (RYCHNOVSKA; KOHUT, 2018).

Desta forma, o *European Values* iniciou a f, e consequentemente, foi publicado o endosso especialista para legitimar as políticas agressivas do governo Russo. Outro ponto é analisar como o Ministério do Interior foi influenciado, legitimando as atividades do *European Values* e trazer toda a problemática da desinformação para o primeiro plano da atenção da mídia (RYCHNOVSKA; KOHUT, 2018).

Ainda, segundo Rychnovska e Kohut (2018), existem diferentes redes que possuem distintas audiências nos debates da guerra informacional. Por exemplo, enquanto a *think tank PSSI* se comunica principalmente com a sociedade civil doméstica e internacional e atores privados, a *European Values* tem uma relação muito mais próxima com o aparato da Segurança da República Tcheca.

Ainda, a relação da politização e securitização da desinformação acaba por complicar as possibilidades de respostas pelo governo tcheco, todavia a adição de instituições independentes acabam por criar novas medidas que podem ser adotadas em diferentes contextos contando com a potencial mobilização social, além de apenas estar criando *blacklists* de mídias não confiáveis, selecionando indivíduos que compartilham propaganda pró-Rússia, ferramentas de verificação de fatos ou educação digital (RYCHNOVSKA; KOHUT, 2018).

Portanto, um dos pontos principais é compreender a limitação do governo Tcheco em combater a desinformação, e como essa limitação deu espaço para organizações não-governamentais entrarem como agentes combatentes da desinformação. Desta forma, a desestatização do combate à desinformação pode ser uma das soluções para a República Tcheca continuar com sua narrativa democrática e transparente dando espaço para organizações não-governamentais filtrarem informações que condizem com a realidade.

4.4 Conclusões preliminares

Para o capítulo três, há três conclusões e lições que podem ser analisadas. Podemos começar com ameaças híbridas que estão relacionadas com a infraestrutura crítica da informação, e analisar que o fator *avanço tecnológico* está ligado com o aumento da vulnerabilidade dos sistemas que são essenciais na vida das sociedades contemporâneas. Para tanto, a República Tcheca parece reconhecer a importância da resiliência no âmbito da infraestrutura crítica da informação, e dessa forma, possui dispositivos legais e específicos para garantir a segurança cibernética da sociedade tcheca. O ponto principal é compreender que vários setores da sociedade são importantes para proteger a dimensão da infraestrutura crítica da informação, tanto empresas privadas quanto instituições públicas. Além disso, apenas com a confiança entre cidadãos e instituições é possível atingir os resultados esperados

pelos dispositivos legais, e por conseguinte, construir o plano da sociedade 4.0 que o Estratégia Nacional de Segurança Cibernética da República Tcheca procura.

Outra ameaça híbrida que a República Tcheca está vulnerável é a ciberespionagem, principalmente segundo os relatórios de inteligência tchecos. Portanto, a dependência da República Tcheca em tecnologia pode atrair atores (estatais ou não) a conseguir informações que sabotem a posição de negociação da República Tcheca em âmbito internacional. Infelizmente não foi possível entrar em detalhes de como o serviço secreto da República Tcheca se defende de ciberespiões, pois o método de abordagem não pode ser divulgado publicamente. O interessante, todavia, é analisar que não apenas o serviço secreto da República Tcheca, mas outras instituições fazem esse trabalho conjunto, principalmente operando com a função informativa e a função preventiva.

Por último, foi analisada a estratégia da desinformação como ameaça híbrida na República Tcheca. Portanto, foi compreendido como a desinformação vem aumentando em diferentes sociedades, não sendo diferente na República Tcheca. Todavia, a conclusão e lição é compreender a natureza ambivalente do Estado contra a desinformação, já que democracias operam de forma diferente. Um desses pontos é compreender que respostas não-estatais surgiram em reação à desinformação, dando espaço para *think tanks* e organizações na análise e defesa contra a desinformação. Observa-se que esse ponto ainda pode ser estudado mais profundamente, ou seja, vê-se uma tendência da utilização de *think tanks* e organizações independentes no futuro da estratégia contra a desinformação.

5 CONCLUSÃO

Essa monografia buscou abordar quais são as respostas estratégias da República Tcheca contra as ameaças híbridas. Portanto, a hipótese considerada para responder à proposta de pesquisa foi que as respostas estratégicas de defesa contra a Guerra Híbrida da República Tcheca são influenciadas pela percepção de ameaça no seu entorno estratégico, seguindo diretrizes provenientes de organizações internacionais. Para isso, foi-se analisado como o entorno estratégico da República Tcheca possui uma identidade nacional e supranacional, já que a percepção de ameaça da República Tcheca é afetada pela membresia de diferentes instituições, principalmente a UE e a OTAN.

Para responder de forma satisfatória a ambição do problema de pesquisa, o Capítulo 1 tem como principal objetivo definir o conceito de Guerra Híbrida. Portanto, utiliza-se a teoria que a Guerra Híbrida é composta pelas diferentes gerações de guerra, principalmente pensando em como o fator *avanço tecnológico* é vital para as gerações de guerra. Após conceitualizar a Guerra Híbrida, é analisado como o entorno estratégico vem sendo transformado pelo fator *avanço tecnológico,* e posteriormente é analisado o entorno estratégico Tcheco pelos documentos oficiais de defesa.

Após a análise dos documentos oficiais de defesa, observou-se a direta conexão entre o entorno estratégico da República Tcheca e como tais instituições internacionais influenciam as perspectivas político-estratégicas da República Tcheca. Logo, para analisar as respostas estratégicas da República Tcheca, encontrou-se a necessidade de também compreender os documentos mais importantes que limitam ou guiam a compreensão Tcheca sobre a Guerra Híbrida. Portanto, foi selecionado os documentos mais importantes da UE e da OTAN que versam sobre perspectivas político-estratégicas para posteriormente entender como tais documentos podem influenciar os documentos oficiais da República Tcheca. Um ponto importante para se considerar aqui é que os documentos das duas instituições versam sobre como uma resposta coordenada da OTAN e da UE e de seus membros correspondentes são necessárias para combater o futuro das ameaças (aqui, chamadas de Ameaças Híbridas).

Após a análise dos documentos da OTAN e da UE no capítulo, seguiu-se para a segunda parte do capítulo que analisa os documentos mais importantes da República Tcheca, e posteriormente as capacidades de defesa definidas pelo documento. No capítulo 1 foi verificado que o fator *avanço tecnológico* é essencial para a conceitualização da Guerra Híbrida, e no capítulo dois é considerado que o avanço tecnológico será fundamental para a

diferente gama de ameaças que podem vulnerabilizar os Estados. Portanto, pensando no fator *avanço tecnológico*, nesse trabalho foi selecionada a dimensão cibernética para ser analisada, já que as ameaças híbridas aumentam proporcionalmente com o aumento da dependência da tecnologia pelos setores dos Estados.

Ainda, para compreender as ameaças que a República Tcheca está vulnerável, buscou-se analisar os relatórios oficiais cibernéticos e de inteligência da República Tcheca que são pilares para o processo de transparência em matéria de defesa. As ameaças selecionadas foram: ataques cibernéticos à infraestrutura crítica da informação, a ciberespionagem e a desinformação.

Com isso, essa monografia buscou compreender uma especificação das possíveis respostas estratégicas da República Tcheca contra as ameaças híbridas que se encontram na dimensão cibernética. Ameaças híbridas são apenas parte de um conceito mais abrangente chamado Guerra Híbrida, mas que são essenciais na defesa da soberania de um país.

No terceiro capítulo, as ameaças híbridas à infraestrutura crítica da informação, a ciberespionagem e a desinformação foram escolhidas por dois motivos principais. O primeiro motivo foi o alerta que o Serviço de Inteligência Tcheco fez nos relatórios de 2020 contra essas três ameaças, além das recentes notícias relacionadas com a interferência estrangeira. Para isso, foram selecionadas essas três ameaças híbridas para serem melhor compreendidas e posteriormente analisadas as respostas estratégicas da República Tcheca se enquadram em cada uma das ameaças híbridas.

A análise das respostas estratégicas tiveram resultados diversos, compreendendo que cada uma das dimensões possui especificidades. Verifica-se, portanto, a eficiência das respostas estratégicas unicamente centradas no Estado. Para a ameaça híbrida referente à informação crítica da informação, analisado que o Estado possui a maior responsabilidade referente à criação de uma sociedade digital resiliente, todavia para o funcionamento dessa sociedade digital é necessário a colaboração de diferentes setores, como por exemplo a confiança entre empresas privadas e o setor público.

Além disso, quando analisamos a desinformação na sociedade tcheca, inferimos que democracias podem possuir obstáculos para censurar e filtrar as informações que vão passar pelos meios digitais. Desta forma, é analisado que para a desinformação, a descentralização

da estratégia contra a desinformação pode ser uma resposta eficiente, tais como o trabalho conjunto entre organizações independentes como *think tanks* e o governo Tcheco.

Para concluirmos, essa monografia demonstrou quais as respostas estratégicas e a capacidade que a República Tcheca possui contra ameaças híbridas que estão relacionadas com o seu entorno estratégico (que vem mudando desde 1993). Em outras palavras, a incapacidade que o Estado possui em securitizar todos os avanços tecnológicos acaba por criar diferentes respostas e estratégias contra ameaças híbridas, como por exemplo o fortalecimento do conceito de resiliência entre todas as partes da sociedade, além do uso de organizações independentes que possam ser usadas estrategicamente contra a desinformação.

Além disso, o conceito de Guerra Híbrida e as ameaças híbridas subjacentes ainda estão em constante mudança, e portanto, compreende-se a natureza metamórfica dos resultados desse trabalho. Infere-se então que os campos ainda carecem de respostas específicas e completamente efetivas contra as ameaças híbridas analisadas nesse trabalho, e que posteriormente podem ser desenvolvidas em estudos de caso para a análise mais profícua.

REFERÊNCIAS

89UP. **Brexit**. Disponível em: https://www.89up.org/category/brexit. Acesso em: 21 dez. 2021.

AARONSON, M., DIESSEN, S., DE KERMABON, Y., LONG, M. B., & MIKLAUCIC, M. NATO Countering the Hybrid Threat. **PRISM**, v. 2, n. 4, p. 111–124, 2011. http://www.jstor.org/stable/26469152

ALMÄNG, J. War, vagueness and hybrid war, **Defence Studies**, v. 19, n. 2, 189-204, 2013. DOI: 10.1080/14702436.2019.1597631 Acesso em: 10 dez. 2021

ARNOLD, J. M. NATO's Readiness Action Plan: Strategic Benefits and Outstanding Challenges. **Strategic Studies Quarterly**. v. 10, n. 1, p. 74–105, 2016. http://www.jstor.org/stable/26271088

BACHMANN S.D., MUNOZ MOSQUERA A.B. Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach. In: Cusumano E., Corbe M. (eds) A Civil-Military Response to Hybrid Threats. **Palgrave Macmillan**, Cham, 2018. https://doi.org/10.1007/978-3-319-60798-6_4 Acesso em: 21 dez. 2021

BAYLIS, John; WIRTZ, James; GRAY; Colin S. **Strategy in the Contemporary World: An Introduction to Strategic Studies.** Oxford University Press. 2019

BERZINS, J. Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy. **Policy Paper**, 2, p. 2002-2014, 2014.

BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. **Annual Report of the Security Information Service for 2020**. Praga: Bezpečnostní Informační Služba, 2021. Disponível em: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/ar2020en-2.pdf. Acesso em: 21 dez. 2021.

BOEKE, S. "National Cyber Crisis Management: Different European Approaches" **Governance: An International Journal of Policy, Administration, and Institutions**, v. 31, n.3, 449–464, jul. 2018.

BROOKS, Rosa. **How everything became war and the military became everything: Tales from the Pentagon**. Simon & Schuster. 2016.

BUEGER, C; BERLING, T. V. **Security Expertise: An Introduction**. Security Expertise: Practice, Power, Responsibility. Routledge, 2015.

BULL, H. **The anarchical society.** A study of order in world politics. New York: Columbia University Press. 1977.

CADIER, D. The Geopoliticisation of the EU's Eastern Partnership. **Geopolitics**, v. 24, n.1, p. 71-99, DOI: 10.1080/14650045.2018.1477754 Acesso em: 11 dez. 2021.

CAMPBELL, D. Poststructuralism. In T. Dunne, M. Kurki, & S. Smith (Eds.), **International relations Theories**. Discipline and Diversity. Oxford: Oxford University Press. p. 223–246, 2013.

ČIŽIK, T. Information warfare as a geopolitical tool. **CENAA Analysis**. Centre for European and North Atlantic Affairs. p. 1339-7168, 2017.

COLEMAN, K. G. Cyber Espionage Targets Sensitive Data. 2008. http://sip-trunking.tmcnet.com/topics/security/articles/47927-cyber-espionage-targets-sensitive-data.htm. Acesso em: 08 dez. 2021.

COMMISSION, European (org.). **A Europe that protects: EU works to build resilience and better counter hybrid threats**. Brussels: Online Document, 2018. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4123. Acesso em: 20 out. 2021.

CORBETT, Julian. Part I. In: CORBETT, Julian. **Some Principles of Maritime Strategy**. Uckfield: The Naval And Military Press Ltd, p. 1-292, 2009.

CLARKE, A. R; KNAKE, K. R. **Cyber war: the next threat to national security and what to do about it**. Ecco. 2010.

CLAUSEWITZ, Carl. **On war**. Princeton: Princeton University Press. 1984.

CLEMENTE, D. Cyber security and global interdependence: what is critical?. Chatham House, **Royal Institute of International Affairs**. 2013.

DELLA SALA, V. Narrating Europe: The EU's Ontological Security Dilemma. **European Security**, v.27 n.3, p. 266–279, 2018.

EBERLE, Jakub; DANIEL, Jan. Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. **Political Geography**, Prague, v. 92, n. 102502, p. 1-9, set. 2021.

EURACTIV. **CZECH PM BABIS REJECTS CUTS IN DEFENCE SPENDING**. Disponível em: https://www.euractiv.com/section/politics/short_news/czech-pm-babis-rejects-cuts-in-defence-spending/. Acesso em: 21 dez. 2021.

EWALD, F., The return of descartes's malicious demon: an outline of a philosophy of precaution. In: T. Baker and J. Simon, eds. Embracing risk. Chicago, IL: **Chicago University Press**. p. 273–302, 2002.

FILIPEC, O. Towards a Disinformation Resilient Society? The Experience of the Czech Republic. **Cosmopolitan Civil Societies: an Interdisciplinary Journal**. v. 11, n.1, p. 1-26. 2019. https://doi.org/10.5130/ccs.v11.i1.6065

GRAY, Colin. **Another Bloody Century: Future Warfare**. Phoenix Press. 2017.

HAMMES, X. Thomas. **The Sling and The Stone: on War in the 21st Century**. Zenith Press. 2004.

HANDLER, S. G. New cyber face of battle: developing a legal approach to accommodate emerging trends in warfare. **Stan. J. Int'l L**., v.48, n. 209, 2012.

HOFFMAN, F. G. *Hybrid warfare and challenges*. NATIONAL DEFENSE UNIV WASHINGTON DC INST FOR NATIONAL STRATEGIC STUDIES. 2009.

JAMES HACKETT (org.). **Editor's Introduction.** In: THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES (IISS) (org.). **The Military Balance 2015**. Oxfordshire: The International Institute For Strategic Studies (Iiss), 2015. p. 1-504.

KADLECOVÁ, L; SEMECKÁ, M. CZECH REPUBLIC: a new cyber security leader in central europe. In: ROMANIUK, Scott N.; MANJIKIAN, Mary. **ROUTLEDGE COMPANION TO GLOBAL CYBER-SECURITY STRATEGY.** New York: Routledge, 2021. p. 1-657.

KADLECOVÁ, L., BAGGE, D. P., BOROVIČKA, V. & SEMECKÁ, M. The Czech Republic: A Case of a Comprehensive Approach toward Cyberspace. **NATO CCDCoE**, Tallinn, Estonia. 2017.

KEOHANE, R. O., & NYE JR, J. S. Power and interdependence in the information age. **Foreign Aff.**, v. 77, n. 81, 1998.

KOŘAN, M. Coloring it Europe? the Europeanization of Czech foreign policy. In **The New Member States and the European Union.** Routledge. p. 75-89, 2013.

KŘÍŽ, Zdeněk. The security perception and security policy of the Czech Republic, 1993–2018. **Defense & Security Analysis**. v. 37, n. 1, p. 38-52, 2021. DOI: 10.1080/14751798.2020.1831231

LIANG, Q; Xiangsui, W. **Unrestricted Warfare**. People´s Liberation Army Literature and Arts Publishing House. Pequim, China. Fev. 1999.

LIBICKI, Martin. **CYBERDETERRENCE AND CYBERWAR.** Santa Monica: Rand. p. 1-214, 2009.

LIND et al. The Changing Face of War: Into the Fourth Generation. **Marine Corps Gazette**. 1989. Disponível em: https://globalguerrillas.typepad.com/lind/the-changingface-of-war-into-the-fourth-generation.html. Acesso em: 02 de dezembro de 2021.

MACKINDER, H. **Geography, an Art and a Philosophy.** Geography 27. pp.129-30. 1962.

MANNERS, I. European [security] Union: from existential threat to ontological security. Copenhagen: **Copenhagen Peace Research Institute**. 2002.

MÄLKSOO, M. Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. **European Security**. v. 27, n. 3, p. 374-392, 2018 DOI: 10.1080/09662839.2018.1497984 Acesso em: 06 dez. 2021.

MEIJER, Hugo; WYSS, Marco. The Handbook of European Defence Policies and Armed Forces. In: SPERLING, James; WEBBER, Mark. **NATO Operations**. Oxford: Oxford Scholarship Online, 2018. Cap. 51. p. 888-914.

METZ, S. In Ukraine, Russia Reveals Its Mastery of Unrestricted Warfare. **World Politics Review**, v. 16, Apr, 2014.

NORTH ATLANTIC COUNCIL. **Brussels Summit Communiqué**. 2021. Disponível em: https://www.nato.int/cps/en/natohq/news_185000.htm. Acesso em: 21 dez. 2021.

NORTH ATLANTIC TREATY ORGANIZATION. **Relations with the European Union**. Disponível em: https://www.nato.int/cps/en/natohq/topics_49217.htm. Acesso em: 21 dez. 2021.

NORTH ATLANTIC TREATY ORGANIZATION. **The North Atlantic Treaty**. Washington D.C., 4 abr. 1949. Disponível em: https://www.nato.int/cps/en/natolive/official_texts_17120.htm. Acesso em: 20 set. 2021.

NORTH ATLANTIC TREATY ORGANIZATION. **NATO's Readiness Action Plan**. Brussels: Public Diplomacy Division (Pdd) – Press & Media Section, 2016. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf. Acesso em: 25 nov. 2022.

NORTH ATLANTIC TREATY ORGANIZATION. **Strategic Concept**: for the defence and security of the members of the north atlantic treaty organization. Lisbon: Nato Graphics & Printing, 2010. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf. Acesso em: 25 set. 2021.

NÚKIB. UPOZORNĚNÍ NA ZVÝŠENÉ RIZIKO KYBERŠPIONÁŽNÍCH ČI RANSOMWAROVÝCH ÚTOKŮ PROTI ČESKÉ REPUBLICE. 2022. Disponível em: https://www.nukib.cz/download/publikace/analyzy/Upozorneni_na_zvysene_riziko_proti_CR.pdf. Acesso em: 29 jan. 2022.

NYE, Joseph S. Jr. Cyber Power. Harvard Kennedy School: **Belfer Center for Science and International Affairs**. Cambridge, p. 1-24. maio 2010. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf>. Acesso em: 21 nov. 2019.

PEREIRA, J. AS AMEAÇAS HÍBRIDAS–UMA ABORDAGEM CONCEPTUAL NO QUADRO DA OTAN E DA UE. **Direito, Segurança e Democracia**. Out, 2018.

PIFER, S. NATO looks divided and its eastern members look exposed. **Financial Times**, v. 19. 2014.

PLOUS, Scott. **The psychology of judgment and decision making**. Mcgraw-Hill Book Company. 1993.

POLYAKOVA, A. – BOYER, S. The future of political warfare: Russia, the West, and the coming age of digital competition. Washington DC: Brookings Institution. 2018.

PROCHÁZKA, J., & CHALUPOVÁ, I. The Czech Republic Defence Strategies: a Comparative Analysis and Qualitative Assessment. In ***International Scientific Conference" Strategies XXI"*** (pp. 242-252). " Carol I" National Defence University. 2017.

REED, J. Donald. Beyond the War on Terror: Into the Fifth Generation of War and Conflict. **Studies in Conflict & Terrorism**, v. 31. n.8, 684-722, Aug, 2008. DOI: 10.1080/10576100802206533.

REPÚBLICA TCHECA. Ato nº 181, de 23 de julho de 2014. **No 181/2014 Coll**: The Act on Cyber Security. Praga, Disponível em: https://nukib.cz/download/publications_en/legislation/Act_181_2014_EN_v1.0_final.pdf. Acesso em: 21 nov. 2021.

REPÚBLICA TCHECA. MINISTÉRIO DAS RELAÇÕES EXTERIORES. **Security Strategy of the Czech Republic.** Prague, 2015. Disponível em: https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf Acesso em: 21 dez. 2021.

REPÚBLICA TCHECA. MINISTÉRIO DA DEFESA DA REPÚBLICA TCHECA. **THE DEFENCE STRATEGY OF THE CZECH REPUBLIC.** Prague, 2017. Disponível em: https://www.army.cz/assets/en/ministry-of-defence/strategy-and-doctrine/defencestrategy2017.pdf Acesso em: 21 dez. 2021.

REPÚBLICA TCHECA. MINISTÉRIO DA DEFESA DA REPÚBLICA TCHECA. **THE LONG TERM PERSPECTIVE FOR DEFENCE 2035.** Prague, 2019. Disponível em: https://www.army.cz/assets/en/ministry-of-defence/basic-documents/dv-2035-aj.pdf Acesso em: 21 dez. 2021.

REPÚBLICA TCHECA. National Cyber and Information Security Agency. **National Cyber Security Strategy of the Czech Republic.** Prague, 2020. Disponível em: https://www.nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf Acesso em: 21 dez. 2021.

REPÚBLICA TCHECA. MINISTÉRIO DA DEFESA DA REPÚBLICA TCHECA. **NATIONAL STRATEGY FOR COUNTERING HYBRID INTERFERENCE.** Prague, 2021. Disponível em: https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf Acesso em: 21 dez. 2021.

REPÚBLICA TCHECA. MINISTÉRIO DO INTERIOR. **Definice dezinformací a propagandy.** 2019. Disponível em:

https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx. Acesso em: 21 dez. 2021.

REUTERS. **Czech "hybrid threats" centre under fire from country's own president**. Disponível em: https://news.trust.org/item/20170104185631-56r53. Acesso em: 21 dez. 2021.

RYCHNOVSKÁ, D., & KOHÚT, M. The battle for truth: mapping the network of information war experts in the czech republic. **New Perspectives**, v. 26 n. 3, p. 57-87, 2018.

SECURITY INFORMATION SERVICE. **Homepage**. Disponível em: https://www.bis.cz/en/. Acesso em: 21 dez. 2021.

SNYDER, G. Deterrence by Denial and Punishment, Woodrow Wilson School of Public and International Affairs. **Center of International Studies Research Monograph**, no.1. Princeton, NJ: Woodrow Wilson School of Public and International Affairs, Center of International Studies, Princeton University. 1959.

SPERLING, James; WEBBER, Mark. NATO Operations. In: MEIJER, Hugo; WYSS, Marco. **The Handbook of European Defence Policies and Armed Forces**. Oxford: Oxford Scholarship Online. p. 1-915, 2018.

USA, Department Defense Of The. **Quadrennial Defense Review Report**. Washington: Secretary Of Defense, 2010. Disponível em: https://history.defense.gov/Portals/70/Documents/quadrennial/QDR2010.pdf?ver=vVJYRVwNdnGb_00ixF0UfQ%3d%3d. Acesso em: 29 set. 2021.

UNIÃO EUROPÉIA. **A Global Strategy for the European Union's Foreign And Security Policy**. Bruxelas: European External Action Service (Eeas), 2016a. Disponível em: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf. Acesso em: 25 nov. 2021.

UNIÃO EUROPÉIA. **Joint Framework on countering hybrid threats**. Bruxelas: Eur-Lex, 2016b. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. Acesso em: 25 nov. 2021.

UNITED NATIONS. **United Nations Charter**. San Francisco, Disponível em: https://www.un.org/en/about-us/un-charter/full-text. Acesso em: 20 set. 2021.

VNĚJŠÍ ZPRAVODAJSKÁ SLUŽBA ČESKÉ REPUBLIKY. **WHAT IS YOUR MAIN MISSION?** Disponível em: https://www.uzsi.cz/en/what-is-your-main-mission. Acesso em: 21 dez. 2021.

WAGNSSON, Charlotte; HELLMAN, Maria. Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare. **JCMS: Journal of Common Market**. 2017. Studies. 56. 10.1111/jcms.12726.

WEISSBRODT, D. Cyber-conflict, cyber-crime, and cyber-espionage. **Minn. J. Int'l L**., v. 22, n. 347, 2013.

WILLIAMSON, S. C. (2009). **From fourth Generation Warfare to hybrid war**. ARMY WAR COLL CARLISLE BARRACKS PA.

WILSON, C. (2014) Cyber Threats to Critical Information Infrastructure. In: Chen T., Jarvis L., Macdonald S. (eds) Cyberterrorism. Springer, New York, NY. https://doi.org/10.1007/978-1-4939-0962-9_7

WITHER, J. K. Making Sense of Hybrid Warfare. **Connections**, v. 15, n. 2, 73–87, 2016. http://www.jstor.org/stable/26326441.

WORLD BANK. **World Bank Open Data**. 2021. Disponível em: https://data.worldbank.org/. Acesso em: 05 de dezembro de 2021.