Alemanha como Líder na Determinação de Ameaças Cibernéticas na União Europeia?

Germany as a Leader in Determining Cyber Threats in the European Union?

DOI: 10.21530/ci.v15n2.2020.1063

Bruna Rohr Reisdoerfer[1]
Bruna Toso de Alcântara[2]

Resumo

A robustez econômica, as relações transatlânticas e a assertividade pragmática conferem à Alemanha legitimidade como Estado central para a tomada de decisão econômica na União Europeia. Todavia, no tocante a questões securitárias e de defesa, o país parece se colocar como líder relutante. Assim, seu papel de líder é contestado na esfera da política externa e de segurança. Todavia, desde o Caso Snowden (2013) a Alemanha destaca-se mundialmente por liderar projetos com ênfase na questão normativa do ciberespaço. Seria a Alemanha um país líder na área da segurança cibernética na Europa? Visa-se, pois, testar a hipótese de que a Alemanha possui papel de liderança na determinação de ameaças cibernéticas na União Europeia. Como o ciberespaço possui aspectos materiais e imateriais, este artigo busca a ótica de duas abordagens teóricas com ontologias distintas para a testagem da hipótese: o realismo neoclássico e o construtivismo convencional. Utiliza-se desenho de pesquisa de caso único, pois ele é propício para o aprofundamento da pesquisa em termos não apenas empíricos, mas também teóricos.

Palavras-Chave: Ameaças Cibernéticas; Alemanha; União Europeia; Realismo Neoclássico; Construtivismo Convencional.

1 Pesquisadora bolsista CAPES em Segurança Internacional e Relações Internacionais. Doutoranda em Estudos Estratégicos Internacionais pela UFRGS. Áreas de concentração: Cooperação em Defesa, Integração Regional e Segurança Internacional. Realizou pesquisa de campo na OTAN, na União Europeia, no governo da Alemanha e em instalações estratégicas do Exército Brasileiro. Currículo Lattes: http://lattes.cnpq.br/6917023951782453; ORCID: https://orcid.org/0000-0001-6180-6663; email: bruna.reisdoerfer@ufrgs.com

2 Pesquisadora bolsista FAPERGS/CAPES em Segurança Internacional e Relações Internacionais. Doutoranda em Estudos Estratégicos Internacionais pela UFRGS. Áreas de concentração: Segurança e Defesa Cibernética, Segurança Internacional, Estudos Estratégicos Internacionais. Atualmente é fellow no Alexander von Humboldt Institute for Internet and Society (HIIG). Currículo Lattes: http://lattes.cnpq.br/7945859311706490; ORCID: https://orcid.org/0000-0002-9091-6578; email: bruna.toso@ufrgs.br

Artigo submetido em 07/04/2020 e aprovado em 17/06/2020.

Abstract

Economic strength, transatlantic relations and pragmatic assertiveness give Germany legitimacy as a central state for economic decision-making in the European Union. However, when it comes to security and defense issues, the country seems to place itself as a reluctant leader. Thus, its role of leader is challenged in the sphere of foreign and security policy. However, since the Snowden Case (2013), Germany stands out worldwide for leading projects with emphasis on the normative issue of cyberspace. Would Germany be a leading country in cybersecurity in Europe? The objective of the present study is to test the hypothesis that Germany has a leading role in determining cyber threats in the European Union. As cyberspace has both material and immaterial aspects, the article seeks the optics of two theoretical approaches with different ontologies for testing the hypothesis: neoclassical realism and conventional constructivism. A single case research design is used, as it is conducive to deepening the research in terms not only empirical, but also theoretical.

Keywords: Cyber Threats; Germany; European Union; Neoclassical Realism; Conventional Constructivism.

Introdução

Aumenta o uso do ciberespaço no dia-a-dia da população mundial. Governos levam cada vez mais em conta este espaço para a tomada de decisão, inclusive em defesa: China, Estados Unidos, Índia, Alemanha, França, Espanha são alguns exemplos de países que criaram uma quarta força em suas estruturas militares: o comando cibernético. Isso porque, atualmente, o ciberespaço é considerado o quinto domínio de guerra, caracterizando-se por ser um ambiente que integra, não apenas o meio digital, mas também o físico, seja através de Sistemas de Controle Industrial ou mais recentemente via Internet das Coisas. Isso gera a necessidade de proteção aos sistemas de funcionamento da sociedade, o que recai sobre os Estados, uma vez que ainda são as entidades que detêm o monopólio legal da força (Lambach 2019).

Debates sobre territorialização e desterritorialização do ciberespaço englobam a persistente tensão entre a visão Westfaliana de Sistema Internacional, no qual há soberania estatal territorialmente delimitada, e o espaço de interação social não territorial criado pelas redes de internet e de computadores. Há, portanto, na literatura de Relações Internacionais, um crescente debate acerca da governança

desse espaço e sua relação com as dinâmicas de poder, especialmente sobre a sua incorporação nas estratégias e políticas dos Estados mais poderosos (Fischerkeller 2017). Esta tensão gera também um questionamento de se as visões teóricas mais tradicionais, como a realista, são capazes de analisar a emergência desse espaço nas Relações Internacionais (Mccarthy 2015; Cavelty 2018). Este questionamento é intensificado quando se acrescenta o nível de análise regional, especialmente na Europa, onde há a União Europeia — um agente além dos Estados centrais produzindo normas, regulamentações, projetos de infraestrutura comum para os seus membros e que adota postura discursiva de exportadora de modelos e regimes internacionais para o ciberespaço (União Europeia 2019). Portanto, o nível de análise regional europeu engloba, além da dicotomia entre materialidade e imaterialidade dos efeitos e ameaças do ciberespaço, também o debate de como se dá essa relação entre Estados soberanos e um ator político supranacional.

Sob este contexto europeu, a Alemanha vem se destacando por liderar, após o Caso Snowden (2013)[3], projetos com ênfase na questão normativa do ciberespaço. O caso alemão chama atenção também, pois o país tem histórico de restrição militar e imagem de poder civil. Todavia, discursos sobre ações retaliadoras no ciberespaço permeiam os círculos domésticos de poder (Reuters 2017). Ou seja, analisar a Alemanha e seu potencial protagonismo na determinação de ameaças cibernéticas no nível regional europeu é um caso importante para contribuir nos debates de quais atores são relevantes para e como se dá a incorporação deste novo domínio de guerra nas agendas políticas dos Estados.

Portanto, é sob esta tensão acerca da (i)materialidade do ciberespaço e como ela se relaciona com a detecção de ameaças pelos Estados que o presente trabalho se insere. Visa-se verificar se existe liderança alemã nos assuntos de cibersegurança a nível europeu. Logo, construiu-se a seguinte hipótese de trabalho: (H) a Alemanha possui papel de liderança na determinação de ameaças cibernéticas dentro da União Europeia. Ela será testada com base em duas abordagens teóricas sobre determinação de ameaças com ontologias diferentes: o realismo neoclássico e o construtivismo convencional. Ressalta-se que a presente pesquisa não exclui que existam outros possíveis líderes[4]. Todavia, optou-se pelo estudo de caso único, pois este desenho de pesquisa possibilita aprofundamento não apenas empírico,

3 No qual houve o vazamento de dados de operações de espionagem conduzidas pela Agência de Segurança Nacional norte-americana, a NSA.

4 Como por exemplo: Estônia, Suécia, Suíça, Finlândia, Polônia, Espanha, França, Reino Unido, Países Baixos, Dinamarca ou República Tcheca — países com algum tipo de representação diplomática para assuntos cibernéticos (Latici 2020).

mas também teórico (Odell 2004) — objetivo deste trabalho. Adotou-se o foco nas abordagens do realismo neoclássico e do construtivismo convencional em detrimento das outras vertentes teóricas do pensamento realista e do pensamento construtivista, por se entender que tais abordagens permitem maior aproximação teórica, uma vez que há operacionalização de variáveis semelhantes, como 'Estado' e 'subjetividade dos atores' (Hopf 1998; Walt 1987). Portanto, há a possibilidade de testagem de hipótese semelhante, apenas com indicadores diferentes (para o realismo neoclássico 'correlação conceitual, ontológica e temporal'; para o construtivismo convencional 'identidade e contexto cultural').

Para o realismo neoclássico, o Estado é ator central nas relações internacionais. Logo, a União Europeia não é um ator securitário *per se* e sim resultado das dinâmicas materiais dos Estados mais poderosos da região. Para que estes países cooperem em defesa, suas percepções de ameaças devem ser convergentes (Dyson 2010; Walt 1987). Por isso, os atores relevantes para a determinação de ameaça cibernética na União Europeia são os Estados membros mais poderosos. O conceito de ameaça cibernética na União Europeia deverá partir de uma ontologia positivista, trazendo materialidade para o ciberespaço. Portanto, como indicador desta relação causal do realismo neoclássico, será verificado empiricamente se a definição de ameaça cibernética da União Europeia tem correlação conceitual, ontológica e temporal com as ameaças elencadas pela Alemanha.

Para o construtivismo convencional — mesmo que seja possível — não há necessidade da centralidade do Estado como ator principal na determinação de ameaças a nível regional (Wendt 1999). Os atores relevantes são relacionais, dependendo do contexto cultural, temporal e do nível de análise. O conceito de ameaça cibernética na União Europeia poderá partir de uma ontologia construtivista, englobando os aspectos imateriais deste domínio. Assim, para a testagem da hipótese de que a Alemanha é líder na determinação de ameaças cibernéticas na União Europeia, tem-se o indicador de que a definição de ameaças nessa região dependerá da identidade da Alemanha, formada e projetada no contexto da União Europeia (relação do 'eu' com o 'outro'). Ou seja, deverá haver autopercepção de liderança na determinação de ameaças por parte da Alemanha, acompanhada de respaldo externo (outros Estados membros ou do próprio bloco). Conforme será retomado na próxima seção, a metodologia de testagem de hipótese no construtivismo convencional é possível dado que ele aceita uma base epistemológica positivista, permitindo e achando necessário certo grau de universalização dos processos estudados (Wendt 1999).

O presente artigo se pautará na testagem de hipótese com base nos preceitos das duas abordagens teóricas escolhidas, observando três esferas de análise para o caso alemão: interna, internacional e institucional. Busca-se elencar a explicação do realismo neoclássico e do construtivismo convencional sobre o que entendem como central para a determinação de ameaças cibernéticas a nível europeu, para depois, com a instrumentalização dos indicadores, verificar se a Alemanha ocupa esta posição. Assim, após o estudo dos argumentos de ambas abordagens, é possível argumentar acerca da capacidade explicativa e de entendimento de cada uma para a análise do caso selecionado.

Convém mencionar que esta pesquisa é um esforço inicial de testagem de hipótese em temática emergente para o campo das Relações Internacionais de modo geral e para o dos Estudos de Segurança de modo específico. Esforços posteriores para o aprofundamento do estudo de caso seriam necessários. A estrutura do artigo divide-se em quatro etapas, além da introdução: i) revisão bibliográfica para debate teórico e epistemológico acerca da definição das teorias selecionadas sobre os atores relevantes na determinação de ameaças cibernéticas; ii) análise documental para levantamento de dados acerca do conceito de ameaça cibernética e os atores relevantes nesta esfera para União Europeia e Alemanha; iii) desenvolvimento da testagem da hipótese, concluindo acerca do papel da Alemanha na determinação de ameaças cibernéticas na União Europeia e iv) conclusão acerca das características, desafios e interconexões entre as duas vertentes teóricas, com futura agenda de pesquisa.

A determinação de ameaças cibernéticas segundo as abordagens realista neoclássica e construtivista convencional

A visão teórica do realismo neoclássico adota abordagem causal estruturalista, mas acrescenta à análise variáveis intervenientes a nível das unidades, como: identidade nacional, vulnerabilidade externa, coesão interna e autonomia executiva (Schweller 2004; Taliaferro 2006; Dyson 2010). Isto é, o comportamento dos Estados é constrangido pela incerteza que a anarquia do Sistema Internacional traz, mas o tempo e a forma de resposta dos países a essa pressão estrutural depende de questões internas tais como: a forma como se dá a tomada de decisão; quem são os grupos políticos no poder e como estão organizados; a autonomia do poder executivo e a coesão interna. Estas variáveis intervêm na capacidade do governo

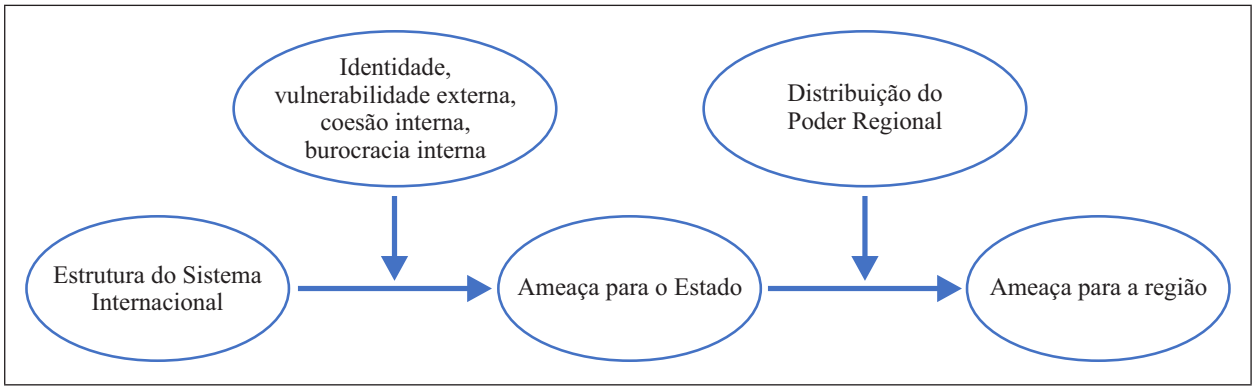
central de utilizar como instrumento a identidade nacional e assim alocar recursos para responder às pressões internacionais (Schweller 2004; Taliaferro 2006; Dyson 2010). Assim, mesmo que acrescente variáveis subjetivas na análise, o foco desta abordagem são os Estados e suas burocracias nacionais sob uma perspectiva materialista e positivista, pois as questões subjetivas não possuem poder de agência para transformar o Sistema Internacional e sua natureza anárquica. Por isso, a percepção de ameaças para esta abordagem teórica, também é vista sob esta ótica. Como partem de uma visão sistêmica a partir da qual entendem os Estados como sendo os principais atores em um sistema ordenado pela anarquia, eles seriam os únicos responsáveis por sua autopreservação. Eles agiriam, portanto, de forma a maximizarem os seus interesses e fazendo frente a possíveis mudanças na relação de poder material entre eles (Mearsheimer 1995). Assim, quando se trata de instituições regionais, elas não produziriam efeitos independentes no comportamento estatal. Isso porque, a cooperação seria uma forma de fortalecer e maximizar os interesses nacionais e seria, pois, criada pelos países mais poderosos (Sperling-Folker 2002). Portanto, a União Europeia não seria um ator securitário *per se,* nem possuiria, na esfera securitária, poder de agência autônomo dos seus Estados membros mais poderosos.

Dessa forma, esta abordagem enxerga a incorporação do ciberespaço como mais uma ferramenta e uma esfera na qual as relações de poder entre os Estados ocorrem (Fischerkeller 2017). O ciberespaço é, pois, incorporado como condicionante sistêmico na atual configuração tecnológica do Sistema Internacional, a Era Digital (Lambach 2019; Shabtai 2016). Partindo desta visão ontológica racionalista e epistemológica positivista das Relações Internacionais, entender a determinação de ameaças a nível da União Europeia requer que o foco seja dado no processo de detecção de ameaças por parte de seus principais Estados membros. Neste sentido, uma das principais abordagens teóricas referente à percepção de ameaça por parte dos Estados que traz, além das variáveis estruturais de distribuição de poder, também variáveis subjetivas, é a da Teoria da Balança de Ameaças, de Stephen Walt 1987. Walt 1987 defende que o padrão de comportamento dos Estados em ambiente de autoajuda se dá visando fazer frente à fonte de maior ameaça e não necessariamente à mais poderosa no Sistema Internacional. Sua visão é, pois, a da Balança de Ameaças e, através dela, o autor acrescenta características das regiões na análise do impacto da polaridade do Sistema Internacional no comportamento estatal — desenvolvendo uma análise subjetiva, mas que confere materialidade à 'percepção' através da análise dos indicadores que, juntos, determinam as ameaças

aos Estados. São eles: i) poder agregado, ii) poder ofensivo, iii) proximidade geográfica e iv) intenções agressivas (Walt 1987).

Para Walt, não é somente a posse estática de elementos de poder que importa para a percepção de ameaça, mas também a capacidade que um Estado tem de transformar esse poderio latente em concreto. Por isso, o autor acrescenta a variável 'poder ofensivo' (Walt 1987. A transformação do poder agregado em capacidade ofensiva se daria, por exemplo, através da infraestrutura estatal e de armamentos militares de projeção — para os quais o ciberespaço é essencial na Era Digital. Por fim, a variável 'intenções agressivas' diz respeito às ambições declaradas e as ações concretas dos países. Portanto, a percepção em relação às intenções dos outros atores seria decisiva para a escolha por alianças (Walt 1987).

Figura 1. Percepções de Ameaças: visão realista neoclássica

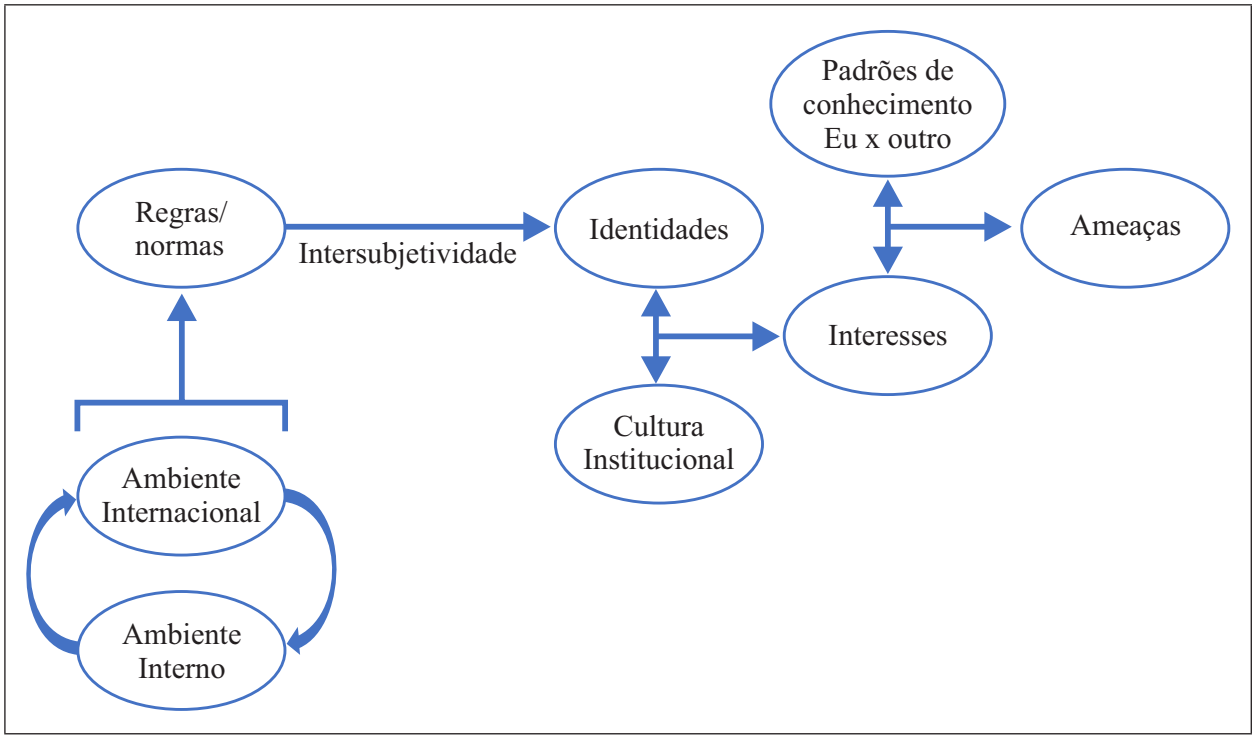


Fonte: Elaboração própria com base em Taliaferro 2006, Dyson 2010 e Walt 1987.

Quanto ao construtivismo, ele parte de base ontológica diferente, para a qual o mundo é socialmente construído. Dessa forma, os fenômenos não se constituem em si mesmos, de forma exógena, mas sim são objetos de conhecimento dentro de práticas discursivas (Guzzini 2000). Isso não significa que não haja objetividade para os construtivistas, mas sim, que eles focam em fatores ideacionais, fazendo com que a estrutura internacional seja percebida de forma tanto material quanto imaterial (contexto cultural do comportamento dos atores) (Kowert and Legro 1996). Dessa forma, o construtivismo explica a variação de comportamentos individuais através das diferenças nas normas sociais que conformam a identidade dos indivíduos (Cornut 2018). Logo, essa abordagem foge ao racionalismo ao entender que os fatores ideacionais não só constituem os interesses e identidades dos atores internacionais, mas também são compartilhados de forma intersubjetiva, não sendo assim reduzíveis a indivíduos particulares (Bertucci, Hayes, and James 2018).

Para o construtivismo, o ciberespaço será, então, uma construção social, para a qual práticas relativamente estáveis tornam-se a chave para a transformação de identidades e interesses, e onde a intersubjetividade ganha relevância. O Sistema Internacional seria composto por regras intersubjetivas reafirmadas pelas práticas humanas (Guzzini 2000). Essa visão é diferente da do realismo neoclássico, pois ela pode considerar como agentes nas Relações Internacionais todos os atores internacionais (e não somente o Estado). Isto é, o ambiente regional, para o construtivismo, serve como base contextual, participando com relações constitutivas na definição de identidades. Dessa forma, definições de identidade que distinguem entre o "eu" e o "outro" implicam definições de ameaça e interesses com efeito nas políticas de segurança (Jepperson, Wendt, and Katzenstein 1996). Logo, a determinação de ameaças no domínio cibernético seguirá a mesma lógica, necessitando que a identidade estatal se 'auto identifique' e identifique o 'outro'. Uma síntese dessa lógica pode ser vislumbrada na Figura 2.

Figura 2. Percepções de Ameaças: visão construtivista convencional

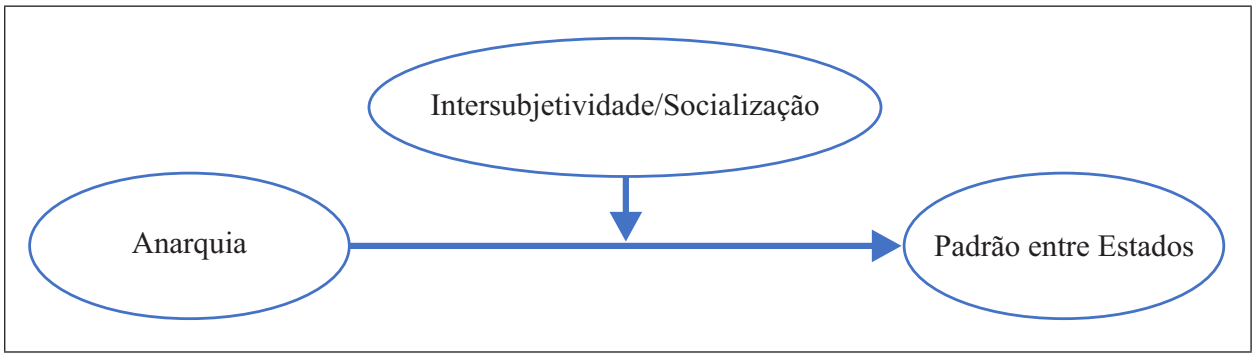


Fonte: Elaboração própria com base em Jepperson, Wendt, and Katzenstein 1996.

A segurança está ligada a culturas nacionais e auto concepções diferentes. Assim, uma visão institucional permite investigar tanto o contexto interno quanto o internacional no qual os Estados e outros atores exercem poder. O construtivismo entende que ambas as esferas, interna e internacional, moldam as identidades

estatais. O ambiente cultural externo teria três efeitos sobre a identidade dos Estados: (1) nas perspectivas de sobrevivência das entidades, (2) no caráter modal do Estado no sistema ao longo do tempo, (3) nas variações de caráter dos Estados dentro de determinado sistema internacional. Já o ambiente cultural interno teria efeitos nas crenças dominantes e [auto]entendimentos dos Estados (Katzenstein 1996). Vê-se, aqui, a diferença com o realismo neoclássico; pois enquanto para ele a ideologia seria apenas uma variável interveniente para o tempo de adequação às pressões sistêmicas, para o construtivismo a ideologia é vista como um sistema de significados que afetam a definição de ameaças (Katzenstein 1996). Para Wendt (1999), a anarquia é vista de maneira social, com não apenas elementos casuísticos, mas constitutivos, dentro de um contexto reflexivo e intersubjetivo, de observação e ação — característica do construtivismo (Figura 3).

Figura 3. Questão Agente e Estrutura no Construtivismo



Fonte: Elaboração própria com base em Wendt 1999

Conforme mostra a representação da Figura 3, o construtivismo convencional aproxima-se da Teoria da Balança de Ameaças, ao pressupor existência ontológica da anarquia. Todavia, diferencia-se por buscar traçar os processos que levam à formação das identidades e interesses. Estes processos levariam a percepção de ameaças e a ações que nem sempre são racionais, uma vez que estão imbuídos em um processo político incessante que envolve normas a nível internacional e interno, gerando entendimentos que se transformam em ações. Logo, se aplicada a visão construtivista para a análise da União Europeia, o bloco teria, tanto quanto suas unidades membros, papel de agente na formação de normas e valores transformativos internacionais. A União Europeia seria um espaço de formação de identidades estatais, permitindo identificar como os Estados, em particular a Alemanha, se auto entendem e entendem os outros na formação de seus interesses e suas políticas securitárias. Haveria, pois, nessa formação, o envolvimento de

dispositivos (principalmente institucionais) que levam-na a maior ou menor papel de liderança dentro do bloco, e mais especificamente nos debates de segurança cibernética. Aspectos desenvolvidos na próxima seção.

Quadro 1. Diferenças nas Abordagens Teóricas

	Realismo Neoclássico	Construtivismo Convencional
Definição de Ameaça	Material, pois a subjetividade acrescentada à análise não possui papel de agente constitutivo ou transformador	Imaterial, baseada na intersubjetividade
Ator Relevante	Estado e sua burocracia central	Intersubjetividade entre Estado (eu) + ambiente externo (outro)

Fonte: Elaboração própria.

Arcabouço Institucional e Definição de Ameaça Cibernética: União Europeia e Alemanha

O objetivo desta seção é demonstrar o que é ameaça cibernética e que atores são importantes para essa determinação para a União Europeia e para a Alemanha, a fim de verificar se os indicadores e argumentos de cada vertente teórica são encontrados na análise da liderança alemã no contexto europeu.

União Europeia

Pela análise de documentos oficiais da União Europeia, especialmente da regulamentação da Agência da União Europeia para a Cibersegurança (da sigla em inglês ENISA), pode-se concluir que o bloco possui um conceito amplo e vago de ameaça cibernética, que se concretiza quando seus efeitos impactam o mundo físico. Ressalta-se também que o bloco reafirma a centralidade estatal no controle delas. Tem-se a visão de que ameaças cibernéticas são todos os perigos impostos a todas as redes de informação de todas as esferas da vida em coletividade, gerando impactos materiais (União Europeia 2019). Devido à imaterialidade do ciberespaço, esses riscos não possuiriam fronteiras e, por isso, um esforço conjunto a nível europeu seria a melhor resposta para a insegurança cibernética dos países da região. Destaca-se que a esfera imaterial das ameaças das redes ganha materialidade, através da consideração dos impactos tangíveis que os ataques cibernéticos podem ter na economia, na política, na sociedade, na segurança e na defesa dos países da União Europeia.

> Os ciberataques aumentam e as economias e sociedades conectadas, mais vulneráveis a ciberameaças e ciberataques, requerem defesas mais robustas. No entanto, apesar de os ciberataques terem amiúde uma natureza transfronteiriça, a competência das autoridades responsáveis pela cibersegurança e pelo controle da aplicação da lei é predominantemente nacional, bem como as ações por estas adotadas. Os incidentes em grande escala são suscetíveis de perturbar a prestação de serviços essenciais na União. Esta realidade implica uma atuação e gestão de crises efetiva e coordenada a nível da União, com base em políticas específicas e instrumentos mais abrangentes para a solidariedade e a assistência mútua a nível europeu. Além disso, é importante para os decisores políticos, para a indústria e os utilizadores que se proceda a uma avaliação regular da situação em matéria de cibersegurança e de resiliência na União, com base em dados fiáveis da União, bem como a previsões sistemáticas da evolução, dos desafios e das ameaças futuras, tanto a nível da União como a nível mundial (União Europeia 2019, 2).

Ou seja, cada país continua central no controle e determinação de suas ameaças cibernéticas. Todavia, a União seria uma esfera de negociação e trabalho conjunto para o objetivo coletivo de fortalecer a resiliência em matéria cibernética.

A União Europeia possui uma estrutura ampla, com quatro esferas de atuação que têm sua natureza e posterior aprofundamento guiados por suas cinco prioridades estratégicas: i) alcançar resiliência cibernética; ii) reduzir drasticamente o crime cibernético; iii) desenvolver políticas e capacidades de defesa cibernética relacionadas à Política de Segurança e Defesa Comum (da sigla em inglês, CSDP); iv) desenvolver recursos industriais e tecnológicos para segurança cibernética e v) estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia, promovendo os valores fundamentais do bloco (European Comission 2013). Estas prioridades estratégicas são amplas e não determinam metas ou indicadores para a sua avaliação, o que pode reafirmar a característica da União como apenas uma arena de conformação política entre seus membros soberanos. A estrutura institucional de cibersegurança da União Europeia é composta por instituições europeias e dos Estados membros. Ela pode ser resumida em quatro áreas de responsabilidade, conforme demonstrado no quadro 2.

Quadro 2. Arcabouço Institucional da Segurança Cibernética da União Europeia

	Paz, Segurança e Justiça	Mercado Único Digital	Defesa Cibernética	Diplomacia Cibernética		
União Europeia	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM Célula de Fusão Híbrida da UE ERCC	⇐ ⇒	**Indústria** **Academia**
Estados Membros	Autoridades executivas e de proteção de dados	Autoridades encarregadas da segurança da informação	Agências de segurança e de defesa	Ministérios das Relações Exteriores	⇒ ⇐	

Fonte: adaptado de Bendiek 2018, 4, European Comission 2013, 18.[5]

Além dessa estrutura institucional, o bloco possui legislação visando alcançar um nível comum mínimo entre os países membros no que tange aos procedimentos para segurança cibernética. As duas mais importantes e recentes são: o Ato Europeu para Cibersegurança 2019 e a Diretiva 2016/1148. O Ato Europeu para Cibersegurança é uma lei do Parlamento Europeu em acordo com o Conselho Europeu e a Comissão Europeia, vinculante aos Estados membros, sobre o mandato, funcionamento, objetivos e atribuições da ENISA[6]. A lei também estabelece uma estrutura do bloco para conferir certificação de segurança cibernética, aumentando a segurança dos serviços on-line e dispositivos de consumo, criando, assim, um Mercado Digital Único europeu[7] (European Commission 2018). O Ato Europeu

5 Legenda: EUROPOL (EC3): Centro Europeu de Crime Cibernético da Polícia Europeia; Eurojust: Unidade de Cooperação Judicial da União Europeia; EU-LISA: Agência Europeia para a Gestão Operacional de Sistemas de TI de Grande Escala na Área de Liberdade, Segurança e Justiça; CSIRT: Equipe de Resposta a Incidentes de Segurança Computacional; CERT-EU: Equipe de Resposta a Emergências em Computadores; EDA: Agência Europeia de Defesa; GSA: Agência Europeia Global de Sistemas de Navegação por Satélite; EEAS: Serviço Europeu de Ação Externa; SIAC (EU INTCEN, EUMS INT): Capacidade Única de Análise de Inteligência (EU INTCEN: Centro Situacional e de Inteligência da União Europeia, EUMS INT: Missão da Diretoria de Inteligência do Estado-Maior da União Europeia; EU SITROOM: Sala de Situação da União Europeia; ERCC: Centro de Coordenação de Resposta a Emergências.

6 A função da ENISA é servir de ponto de referência para suporte técnico para as instituições, agências, Estados membros da União e todos os seus respectivos tomadores de decisão (European Union Agency for Cybersecurity 2019).

7 O Mercado Digital Único visa remover as diferenças entre as esferas online e offline, diminuindo as barreiras à atividade online transfronteiriça. A estratégia de um mercado único digital foi adotada em 6 de maio de 2015 como uma das ações para alcançar as estratégias elencadas pela Comissão Europeia no documento 'Estratégia Europeia para Cibersegurança de 2013' (European Commission 2019).

para Cibersegurança, acordado em dezembro de 2018 e que entrou em vigor em 17 de abril de 2019, após ratificação pelos parlamentos nacionais, estendeu e tornou permanente a estrutura da ENISA em substituição à Regulamentação No 526/2013 que, por sua vez, também foi fundada para substituir a Regulamentação provisória de 2004 que criou temporariamente a Agência (União Europeia 2019; European Union Agency for Cybersecurity 2019). A Diretiva 2016/1148 do Parlamento e do Conselho Europeu visa produzir um nível comum mínimo de segurança das redes e da informação (União Europeia 2016). Para tanto, ela institui que os Estados membros da União produzam estratégia nacional de segurança das redes e dos sistemas de informação e elenca os seus requisitos técnicos mínimos. Por isso, ela é vinculante, mas não superior aos procedimentos já existentes nacionalmente. Além disso, ela estrutura as instituições citadas no Quadro 2 (União Europeia 2016).

Chama atenção que a estruturação e consolidação do Ato, da Diretiva e de suas instituições, resultaram de uma série de aproximações anteriores — intensificadas nos anos 2010 — entre os líderes dos países europeus e as autoridades europeias que resultaram, entre outros, na estruturação, por parte da Comissão Europeia e da Alta Representante da União para Assuntos Externos, da já mencionada Estratégia Europeia para Cibersegurança de 2013 e no comunicado intitulado 'Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE' em 2017 (Comissão Europeia 2017). Como ato mais recente desenvolvido pela União Europeia, dias antes das eleições para o Parlamento Europeu, está a aprovação, pelo Conselho (reunido na forma de Ministros das Finanças), em 17 de maio de 2019, da possibilidade de aplicação de regime de sanções através de congelamentos de ativos e proibições de viagens a indivíduos, empresas e órgãos de Estado envolvidos em ataques cibernéticos com impactos significativos aos alvos (Jozwiak 2019). Ou seja, traz-se materialidade para o ciberespaço e suas ameaças.

Por fim, da análise dos documentos e das instituições da União Europeia, pode-se verificar que o bloco apresenta estrutura própria que serve de instrumento para facilitar e regulamentar o trabalho entre os Estados membros. Visa-se assim, fortalecer a segurança cibernética do bloco, sem se sobrepor às competências, responsabilidades e soberania de cada ator. Portanto, a União Europeia nos assuntos de segurança cibernética configura-se como uma espécie de agência técnica dos Estados membros (European Union Agency for Cybersecurity 2019; União Europeia 2019). A concepção de ameaças cibernéticas, como demonstrado, é ampla e engloba todas as esferas e atores dos sistemas de informação dos Estados membros e da União Europeia: seus cidadãos, suas burocracias nacionais, suas empresas, a área acadêmica e suas forças policiais e armadas (União Europeia 2019).

Alemanha

Levando em consideração que tanto a abordagem realista neoclássica quanto a construtivista convencional concentram-se em Estados e no nível sistêmico, para que ambas as abordagens teóricas possam ser testadas no caso alemão são necessários três ambientes de análise em relação à construção e percepção de ameaças: *a)* o *interno* (relevante para relações constitutivas do 'eu' e do 'outro' no construtivismo, e no que tange a temporalidade das ações do país para o realismo neoclássico), b) o *internacional* (relevante como nível de análise e fonte dos constrangimentos a ações estatais para o realismo neoclássico e como segunda base constitutiva do 'eu' e do 'outro' para o construtivismo) e c) o *institucional* (como forma relacional de interação entre os outros dois ambientes).

No que tange ao ambiente interno, a Alemanha mostra-se um país conectado, coma penetrabilidade de Internet atingindo 96% da população do país (Internet World Stats 2019) e o setor de comércio eletrônico entre empresas e consumidores avaliado em 53,3 bilhões de Euros, em 2018, e com previsão de crescimento (Handelsverband Deutschland 2019). Contudo, seu grau de digitalização ainda encontra dificuldades. A velocidade de internet importa quando tecnologias como o 5G estão sendo usadas e a indústria 4.0 necessita de conexão rápida para prosseguir com suas atividades. Em 2017, apenas 23,5% das pequenas e médias empresas venderam on-line, enquanto 11,3% venderam bens ou serviços a clientes em outros países (European Commission 2019). Segundo reportagem do Deutsch Welle, os executivos de negócios estão insatisfeitos com a hesitação dos políticos em relação à digitalização da economia (Wenkel 2017). Para além desta questão, a falta de pessoal capacitado para trabalhar nas áreas que envolvem tecnologia também tem um peso para o desenvolvimento digital alemão. De acordo com a estratégia Digital 2025 (Bundesministerium für Wirtschaft und Energie 2016) maior necessidade foi percebida em habilidades de análise de dados (45%), competência em mídias sociais (35%) e programação (35%), mas a proteção e a segurança dos dados (25%) também desempenham papel importante. Em 2017 se constatou que 67% das pequenas e médias empresas relatam escassez de habilidades em Tecnologias de Informação e Comunicação (TIC) entre seus funcionários (European Commission 2019). Dados que são relevantes para a atual corrida em relação ao desenvolvimento de computadores quânticos e inteligência artificial.

De fato, nos últimos dois anos, 68% das empresas alemãs foram vítimas de ataques cibernéticos, sabotagem, roubo de dados ou espionagem (Simsek 2018),

sendo que 96% das pequenas e médias empresas alemãs já tiveram experiências desagradáveis envolvendo incidentes de segurança de Tecnologia da Informação (TI) (Bundesministerium für Bildung und Forschung 2019). Além disso, o governo alemão não apenas passou por uma série de invasões cibernéticas internas, como também sofreu influência de acontecimentos internacionais ante a percepção de ameaças cibernéticas.

Em relação ao ambiente internacional, segundo Robin2018, quatro eventos internacionais e cinco eventos nacionais impactaram a percepção alemã no âmbito da segurança cibernética. A nível internacional tem-se: os ataques *DDoS*[8] na Estônia, em 2007; a descoberta do Stuxnet, em 2010[9]; as revelações de espionagem feitas por Snowden em relação a agência norte americana de segurança nacional e a Alemanha, em 2013, e a quebra de dados do Escritório de Gestão de Pessoas dos Estados Unidos, a qual expôs dados de aproximadamente 18 milhões de empregados, caracterizando ataques direcionados a Estados. Já a nível nacional, o primeiro evento foi o *defacement*[10] no website do exército alemão, em 2003; seguido de uma invasão de um *Trojan*[11] em vários ministérios alemães, incluindo a chancelaria, em 2007. Poucos anos depois o grupo "No Name Crew", entre 2010/2011, invadiu servidores de várias agências investigativas alemãs (BKA, ZKA, BUPOL). Em seguida, houve uma Ameaça Avançada Persistente (sigla em inglês, APT)[12] a uma siderúrgica, em 2014, que provocou falhas em vários sistemas de controle causando não apenas prejuízos físicos, mas econômicos e em 2015, ocorreu o evento que ficou conhecido como *Bundestaghack* (envolvendo descoberta de um *malware* nos servidores do governo alemão). Acrescenta-se a essa lista o recente vazamento de dados, por um hacker que se intitulava "God", tido como o maior vazamento de dados de políticos e personalidades da mídia na Alemanha (Bershidsky 2019).

8 Ataque de Negação de Serviço se baseia na sobrecarga de sistemas devido a cargas extras de informação (Greathouse 2014).

9 O *worm* chamado Stuxnet, teve como objetivo atingir um programa de controle presente nas usinas de enriquecimento de urânio iranianas. Por sua especificidade e por ser o primeiro malware a ter efeito físico comprovado, ele passou a ser considerado a primeira arma cibernética do mundo. Dada sua complexidade constatou-se que apenas Estados poderiam ter desenvolvido o código malicioso, sendo apontados como desenvolvedores do malware Israel e Estados Unidos (Macková 2013).

10 *Defacement* é a desconfiguração do conteúdo original de páginas da web (Maggi et al. 2018).

11 *Trojan* é um programa com características benignas, mas que serve a objetivos maliciosos (Hansman and Hun 2005).

12 APT é um inimigo com altos recursos e nível de experiência que utiliza vários vetores de ataque (cibernético, físico e enganoso) (National Institute of Technology and Standards 2013).

Assim, tanto o ambiente interno quanto o externo contribuem para maior preocupação alemã em relação às ameaças advindas do ciberespaço. De fato, relatório do Conselho Europeu de Relações Internacionais de 2018 atesta que Estados membros grandes e ricos, entre eles a Alemanha, parecem estar mais preocupados com ataques cibernéticos, em termos de probabilidade, impacto ou administração dos mesmos do que os demais países. Ainda, segundo esse relatório, tal preocupação advém da consciência de que as sociedades destes países são dependentes de sistemas digitalizados (Dennison, Franke, and Zerka 2018).

Quanto ao ambiente institucional — diante dos acontecimentos internacionais e do panorama doméstico — a Alemanha vem, com sua Estratégia Nacional de Segurança Cibernética, mudando o tom de sua narrativa em relação à projeção de liderança internacional, em especial no âmbito da União Europeia. A estratégia de 2016 indica que a segurança interna e externa do ciberespaço não pode ser claramente distinguida e que a segurança e defesa cibernética se tornaram uma questão nacional que deve ser tratada em conjunto (Bundesministerium des Innern 2016). Ademais, uma das diretrizes é o posicionamento ativo da Alemanha no mercado europeu e internacional, com objetivo de criar um sistema europeu eficaz e moldar ativamente a política de segurança cibernética como um tópico da Política Externa e de Segurança Comum da União Europeia (Bundesministerium des Innern 2016). Não apenas isso, a nova estratégia, ainda que reforce uma perspectiva holística, indica a necessidade de centralização institucional e maior interligação entre as agências. Isso porque há uma separação forte entre segurança e defesa cibernética a nível institucional. A primeira a cargo do Ministério Federal do Interior (sigla em alemão, BMI), Ministério das Relações Exteriores (sigla em alemão, AA) e o Gabinete do Chanceler (sigla em alemão, BKAmt) já a segunda fica a cargo do Ministério da Defesa (sigla em alemão, BMVg).

Especificamente, o BKAmt coordena os aspectos internacionais da política de cibersegurança através do AA e a coleta de informações através do Serviço de Inteligência Federal (sigla em alemão, BND). Já o BMI é o responsável pela formulação da estratégia geral de segurança cibernética e tem suas competências cibernéticas delegadas em escritórios específicos, a exemplo do Escritório Federal de Segurança em Tecnologia da Informação (sigla em alemão, BSI). Esse Escritório tem a tarefa de fortalecer a segurança em tecnologia da informação do governo federal, como autoridade com o mais alto conhecimento técnico, abrigando entre outros, o Centro Nacional de Defesa Cibernética (sigla em alemão, Cyber-AZ), a Aliança para Segurança Cibernética (sigla em alemão, AfCS), o Centro Nacional

de Situação de TI do Escritório Federal de Segurança da Informação (sigla em alemão, LZ), Grupo de Resposta a Incidentes de Segurança para a Internet (CERT) do governo federal (sigla em alemão, CERT-Bund) e CERT- Cidadão (sigla em alemão, Bürger-CERT). Por fim, a nível militar, o BMVg é responsável pela coordenação da defesa cibernética, centralizando aspectos militares no Comando do Domínio Cibernético e da Informação (sigla em alemão, KdoCIR), criado em 2017, equipado com recursos cibernéticos defensivos e ofensivos (Robin 2018; Herpig and Messing 2019).

O arcabouço institucional alemão não se restringe a essas instituições, e desenrola-se atualmente em 56 agências. Todavia, conforme mostra o Quadro 3, apenas algumas dessas agências comunicam-se diretamente com o arcabouço cibernético institucional europeu. Essas agências são: AA, BMI, BMVg, BSI, o Ministério Federal de Justiça e Defesa do Consumidor (sigla em alemão, BMJv) o Ministério Federal de Educação e Pesquisa (sigla em alemão, BMBF), o Departamento Federal de Polícia Criminal (sigla em alemão, BKA) e o BND.

Quadro 3. Relação Institucional Alemã e Europeia no Âmbito da Segurança Cibernética

Instituição ALE/UE	**Conselho Europeu**	**Comissão Europeia** (HORIZON 2020, GD HOME, CERT-EU)	**Serviço Europeu para Ação Externa** (EUMS INT, INTCEN GD Home),	**Agência Europeia de Defesa** (ENISA, Eurojust)
AA			X	
BMI	X		X	
BMJv	X			
BMVg	X		X	
BMBF		X		
BKA		X	X	
BND			X	
BSI (AfCS,CERT)				X

Fonte: Elaboração própria com base em Herpig and Messing 2019.

Percebe-se, com essa relação, que as instituições alemãs participam de todas as quatro áreas de responsabilidade cibernética da União Europeia, convergindo no que tange à percepção ampla de ameaças no ciberespaço. Em específico, a partir da leitura dos documentos oficiais (Bundesministerium der Verteidigung 2016; Bundesministerium des Innern 2005; 2009; 2011; 2016; Federal Republic of Germany 2014; 2018) e dos problemas estruturais internos apontados, pode-se

dizer que a visão alemã de maiores ameaças no ciberespaço engloba invasão/ataque às infraestruturas críticas, crime, terrorismo, espionagem no ciberespaço, além da possibilidade de guerra híbrida (i.e., envolvendo meio digital e domínios convencionais de guerra). Ou seja, o país reconhece como ameaça questões materiais e imateriais do ciberespaço.

Ademais, interessa ressaltar que as áreas de responsabilidade europeia são citadas em documentos nacionais, a fim de criar convergência no âmbito europeu. Dessa forma, a Alemanha cria uma narrativa com participação da sociedade (civil/academia) voltada à proteção de dados, resguardando a liberdade da internet e a privacidade dos usuários, através de enfoque no desenvolvimento legal e aproximações multilaterais (especialmente com União Europeia e OTAN). Discursivamente, o país resguardava um papel de poder civil, e não militar. Entretanto, nos últimos documentos oficiais o país tem envolvido sua parte militar nesse setor (Bundesministerium der Verteidigung 2016; Bundesministerium des Innern 2011; 2016; Federal Republic of Germany 2014; 2018; Robin 2018).

A Agenda Digital do país já colocava como objetivo para um ciberespaço mais seguro reforçar a cooperação internacional nesta área, por exemplo com o Centro Europeu de Cibercrime da Europol (Federal Republic of Germany 2014). O Livro Branco de 2016 menciona como uma das prioridades iniciais na União Europeia a proteção e defesa cibernética, colocando a Alemanha como nação-quadro e fomentadora de projetos multilaterais (Bundesministerium der Verteidigung 2016). Mas é a Estratégia Nacional de Segurança Cibernética que melhor descreve a autopercepção alemã em relação a seu papel na segurança cibernética internacional:

> O governo federal é percebido mundialmente como **um ator confiável**. Ele também pode usar suas habilidades existentes para apoiar Estados e regiões parceiras no futuro por meio da capacitação cibernética. Isso inclui o **desenvolvimento de estratégias de segurança cibernética, legislação, instituições, certificação, pesquisa, educação e treinamento e iniciativas regionais**. Especialmente quando as pessoas têm acesso ao ciberespaço graças a políticas de desenvolvimento, as condições e conhecimentos básicos para seu uso seguro e confiável devem ser apoiados (Bundesministerium des Innern 2016, 42, tradução nossa, grifo nosso)[13].

13 Do original em alemão: "Die Bundesregierung wird weltweit als vertrauenswürdiger Akteur wahrgenommen. Auch bestehende Kompetenzen kann sie nutzen, um Partnerstaaten und regionen zukünftig verstärkt durch Cyber Capacity Building zu unterstützen. Dies umfasst unter anderem die Entwicklung eigener Cyber-Sicherheitsstrategien, Gesetzgebungen, Institutionen, Zertifizierung, Forschung, Aus- und Weiterbildungsmaßnahmen sowie regionale Initiativen. Insbesondere dort, wo Menschen der Erstzugang zum Cyber-Raum dank entwicklungspolitischer

Análise de Dados: o papel da Alemanha na determinação de ameaças a nível regional

Levando em consideração as abordagens teóricas e o caso analisado, busca-se, nesta seção, comparar o conceito de ameaça cibernética e os atores relevantes para essa conceituação na União Europeia com os da Alemanha. Busca-se, assim, uma conclusão acerca do papel do país na determinação de ameaças a nível regional.

Retomando a visão da União Europeia, constata-se que o seu conceito de ameaça cibernética é amplo, envolvendo todas as esferas estatais (política, econômica, jurídica, social e científica) e configurando-a como ameaça que transcende as fronteiras nacionais. Todavia, o seu controle e combate continuam sendo prerrogativa dos governos nacionais. As ameaças cibernéticas recebem territorialidade no discurso de que o ciberespaço tem impacto material nas trocas econômicas e na infraestrutura de armamentos, por exemplo (União Europeia 2019).

Observando a Alemanha, constata-se que sua percepção de ameaças cibernéticas também é ampla, com foco em ataques às infraestruturas críticas, crime, terrorismo, espionagem no ciberespaço, além da possibilidade de guerra híbrida (Bundesministerium des Innern 2016). Há, portanto, uma visão tanto material quanto imaterial do ciberespaço. Sua estrutura institucional e seus conceitos de ameaça cibernética têm forte correlação com as instituições europeias e há precedência temporal de suas políticas e discursos em relação aos desenvolvimentos formais no bloco.

Quadro 4. Semelhanças e Diferenças entre União Europeia e Alemanha

	União Europeia	**Alemanha**
Definição de Ameaça Cibernética	Ampla (além das fronteiras nacionais e em todas as esferas estatais). Material.	Ampla (em todas as esferas estatais). Material e imaterial.
Atores Relevantes para a Determinação de Ameaça	Estados nacionais e instituições regionais	Estados nacionais e instituições regionais. Agências internas, relação do 'eu' com o 'outro'

Fonte: Elaboração Própria.

Maßnahmen ermöglicht wird, müssen die Rahmenbedingungen und Kenntnisse für seine sichere und verlässliche Nutzung unterstützt werden" (Bundesministerium des Innern 2016, 42).

Quadro 5. Correlação Temporal de Eventos — Alemanha e União Europeia

2003	*Defeacement* no website do exército alemão
2004	Regulamentação provisória que criou temporariamente a ENISA
abril 2007	Ataques *DDoS* na Estônia em 2007 (cunhado pela mídia como primeira guerra cibernética do mundo)
2007	Invasão de um *Trojan* em vários ministérios alemães
2010	Descoberta do Stuxnet (primeira arma cibernética do mundo)
2011	Invasão de servidores de várias agências investigativas alemãs (BKA, ZKA, BUPOL) pelo grupo "No Name Crew"
fev 2013	Estratégia de Cibersegurança da União Europeia
maio 2013	Revelações de espionagem feitas por Snowden em relação a Agência de Segurança Nacional norte americana (NSA) e a Alemanha
2014	Ataque APT a uma siderúrgica alemã, causando falhas em vários sistemas de controle (prejuízos físicos e econômicos)
2015	Bundestaghack (envolvendo descoberta de um *malware* nos servidores do governo alemão)
julho 2016	Assinatura da Diretiva Europeia 2016/1148
nov 2016	Lançamento da Estratégia Nacional de Segurança Cibernética da Alemanha
2017	Comunicado 'Resiliência, dissuasão e defesa: reforçar a cibersegurança na União Europeia'
2018	Ato Europeu para Cibersegurança
janeiro 2019	Vazamento de dados, por um hacker que se intitulava "God", tido como o maior vazamento de dados de políticos e personalidades da mídia na Alemanha.
abril 2019	Ratificação do Ato Europeu para Cibersegurança 2019
maio 2019	União Europeia acorda possibilidade de aplicação de regime de sanções através de congelamentos de ativos e proibições de viagens a indivíduos, empresas e órgãos de Estado envolvidos em ataques cibernéticos, com impactos significativos aos alvos.

Fonte: Elaboração própria.

Os dados elencados sob a ótica dos indicadores de cada vertente teórica permite argumentar que o indicador da explicação do realismo neoclássico para o caso alemão sob contexto europeu (a saber: existência de correlação conceitual, ontológica e temporal da definição de ameaça cibernética e de atores relevantes para União Europeia e Alemanha) foi encontrado. Assim, poder-se-ia afirmar que, de uma visão realista neoclássica, o primeiro teste essencial da hipótese de que Alemanha é líder para a determinação de ameaças cibernéticas na União Europeia

foi concluído com resposta positiva. Do ponto de vista construtivista convencional, poder-se-ia afirmar que a União Europeia possui poder de agência, na medida em que ela se coloca como ator coordenador e em certa medida padronizador de ações estatais via legislação comum. Isso se dá, pois, ela estaria partindo das demandas expressas pelos Estados membros; mas construiria a partir disso, suas próprias percepções através de processos burocráticos em formato reflexivo (eu x eles). Assim, a Alemanha não necessariamente ganharia uma posição de liderança e, sim, faria parte de um processo de co-constituição a nível regional. Ademais, uma visão construtivista advogaria que ainda que a Alemanha busque a construção de um papel protagonista em seus discursos sobre o ciberespaço (Bundesministerium des Innern 2016; Federal Republic of Germany 2014), esse papel não se concretiza efetivamente. Isso porque, dentro de sua própria narrativa, há quebra de hierarquia entre o interno e o externo. Fato que fortalece o argumento sobre a existência de uma relação de co-constituição com a União Europeia, já que defende que o fortalecimento europeu também significa o fortalecimento alemão e coloca iniciativas europeias como fonte de embasamento para a sua tomada de decisão (Bundesministerium des Innern 2016).

> A nível da União Europeia (EU), apoiamos medidas adequadas baseadas no plano de ação para a proteção de infraestruturas críticas da informação. Também apoiamos a extensão e a expansão moderada do mandato da Agência da União Europeia para a Cibersegurança (ENISA), tendo em vista a mudança da situação das ameaças nas TIC e nas partilhas de competências em TI nas instituições da UE. A estratégia de segurança interna da UE e a agenda digital fornecem orientações para outras atividades (Bundesministerium des Innern 2011, 11, tradução nossa)[14].

Conclusão

O estudo permite concluir que é possível encontrar a argumentação e as explicações de ambas as vertentes teóricas para a análise de que a Alemanha é um país necessário para a determinação de ameaças cibernéticas na União

14 Do original em alemão: "Auf Ebene der Europäischen Union (EU) unterstützen wir geeignete Maßnahmen, die sich insbesondere aus dem Aktionsplan für den Schutz der kritischen Informationsinfrastrukturen ergeben. Außerdem unterstützen wir die Verlängerung und maßvolle Erweiterung des Mandats der Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) in Hinblick auf die geänderten Bedrohungslagen im IKT-Bereich sowie die Bündelung von IT-Zuständigkeiten in EU-Institutionen. Die EU-Strategie der Inneren Sicherheit und die Digitale Agenda sind Wegweiser für weitere Aktivitäten." (Bundesministerium des Innern 2011, 11).

Europeia. Todavia, as conclusões das duas abordagens teóricas, através da operacionalização das variáveis e dos indicadores elencados, são que os dados obtidos são insuficientes para confirmar a liderança da Alemanha a nível regional. Isto é, o indicador realista — 'a definição de ameaça cibernética da União Europeia possui correlação conceitual, ontológica e temporal com as ameaças elencadas por Alemanha' — e o indicador construtivista — 'a definição de ameaça na União Europeia dependerá da identidade da Alemanha formada e projetada dentro do contexto da União Europeia' — não são suficientes para comprovar se a Alemanha, além de necessária, é também o país líder na determinação de ameaças cibernéticas.

Do ponto de vista realista neoclássico, para poder afirmar se a Alemanha é também uma variável suficiente (isto é, além de país necessário, também país líder) para determinar as ameaças cibernéticas a nível regional, seria necessário acrescentar uma análise sobre a centralidade e a correlação de França e Reino Unido (países com grande poderio material e iniciativas cibernéticas) nas aproximações da União Europeia; bem como, analisar a tomada de decisão nas instituições da União Europeia para verificar se houve protagonismo das burocracias alemãs no desenvolvimento das iniciativas que resultaram nos documentos e nas instituições formais do bloco. Da mesma forma, uma argumentação construtivista coloca que a pesquisa até aqui não consegue determinar se a narrativa alemã é predominante ou se entra em uma hierarquia de narrativas na União Europeia, pois seria necessária a comparação de outras narrativas fortes nas discussões sobre o ciberespaço. Propõe-se, pois, a incorporação destas variáveis e dos casos elencados como futura agenda de pesquisa para expansão do esforço científico iniciado com este trabalho.

Por fim, dado que resultados semelhantes foram alcançados partindo-se de investigação inicial de um mesmo caso de análise, há indícios de que haveria possibilidade de interconexão entre as duas abordagens teóricas. Obviamente, os resultados encontrados partiram de pressupostos ontológicos diferentes, analisados sobre lentes próprias em relação à determinação de ameaças, e não se tem certeza se uma pesquisa comparativa, com maior número de casos, manteria essa aproximação. Independentemente disso, o que se percebe é uma complementaridade passível de ser atingida no que se refere à construção do conceito de ameaças no ciberespaço já que, substancialmente, a incorporação do ciberespaço nas políticas e nos atores analisados deu-se em uma relação tanto de materialidade quanto de imaterialidade. Já que o realismo neoclássico considera variáveis internas e comportamento racional dos atores estatais, o construtivismo

convencional permite abrir a caixa preta da racionalidade, incluindo questões contextuais a um nível mais profundo. Portanto, os esforços desta pesquisa para a incorporação do ciberespaço nos debates teóricos sobre percepção de ameaça, incorporando o nível regional, visam contribuir para a consolidação de importante agenda de pesquisa empírica e teórica nos Estudos de Segurança.

Referências

Bendiek. Annegret. 2018. "The EU as a Force for Peace in International Cyber Diplomacy". *German Institute For International And Security Affairs*, Berlin, 19 (19): 1-8.

Bershidsky, Leonid. 2019. "Why Germany's Worst Data Leak Isn't Such a Scandal: Hackers worked for months but seem to have found little incriminating data". *Blomberg Opinion*. Acessado em: 23 de novembro de 2019 < https://www.bloomberg.com/opinion/articles/2019-01-07/why-germany-s-god-hack-wasn-t-such-a-scandal > .

Bertucci, Mariano E, Jarrod Hayes and Patrick James. 2018. "A New Look at Constructivism" In *Constructivism Reconsidered: Past, Present and Future* edited by Mariano E. Bertucci, Jarrod Hayes, Patrick James, 1-14. Ann Arbor: University of Michigan Press

Bundesministerium der Verteidigung. 2016. *Weissbuch*: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. Berlin: Bundesministerium der Verteidigung.

Bundesministerium des Innern. 2005. *Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)*. Berlin: Bundesministerium des Innern.

Bundesministerium des Innern. 2009. *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. Berlin: Bundesministerium des Inner.

Bundesministerium des Innern. 2011. *Cyber-Sicherheitsstrategie für Deutschland*. Berlin: Bundesministerium des Inner.

Bundesministerium des Innern. 2016. *Cyber-Sicherheitsstrategie für Deutschland* 2016. Berlin: Bundesministerium des Inner.

Bundesministerium für Bildung und Forschung. 2019. "Cybersecurity research to boost Germany's competitiveness". Acessado em: 23 de novembro de 2019 < https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html > .

Bundesministerium für Wirtschaft und Energie. 2016. *Digital Strategie 2025*. Berlin: Bundesministerium für Wirtschaft und Energie.

Cavelty, Myriam Dunn. 2018. "Europe's cyber-power". *European Politics and Society*, 19 (3): 304-320. Acessado em 07 de abril de 2020 < https://www.tandfonline.com/doi/abs/10.1080/23745118.2018.1430718 > .

Comissão Europeia. Comunicado Conjunto nº JOIN (2017) 450. Bruxelas, 13 de setembro de 2017. *Comunicação Conjunta ao Parlamento Europeu ao Conselho:* Resiliência, dissuasão e defesa reforçar a cibersegurança na UE. Bruxelas. Acessado em 03 de julho de 2019. < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri = CELEX:52017JC0450&from = EN > .

Cornut, Jérémie. 2018. "New Wine into a (Not So) Old Bottle? Constructivism and the Practice Turn". In *Constructivism Reconsidered: Past, Present and Future*, edited by Mariano E. Bertucci, Jarrod Hayes and Patrick James. Ann Arbor: University of Michigan Press

Dennison, Susi, Ulrike Esther Franke and Pawel Zerka. 2018. "The nightmare of the dark: the security fears that keep Europeans awake at night". *European Council on Foreign Relations.* Acessado em 23 de novembro de 2019 < https://www.ecfr.eu/specials/scorecard/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n > .

Dyson, Tom. 2010. *Neoclassical Realism and Defence Reform in Post-Cold War Europe***.** London: Palgrave Macmillan. Kindle edition.

European Commission. Joint Communication nº JOIN (2013) 1. Brussels, February 7th, 2013. *Joint Communication to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions:* Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace. Brussel. Acessado em 03 de julho de 2019 < http://register.consilium.europa.eu/doc/srv?l = EN&f = ST%206225%202013%20INIT > .

European Commission. Joint Communication nº JOIN. 2018. "Cybersecurity Act"**.** Acessado em 03 de julho de 2019 < https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en > .

European Commission. Joint Communication nº JOIN. 2019. "What is the Digital Single Market about". 2019. Acessado em 03 de julho de 2019 < https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html > .

European Union Agency for Cybersecurity 2019. "About ENISA". Acessado em 02 de julho de 2019 < https://www.enisa.europa.eu/about-enisa > .

Federal Republic of Germany. 2014. *Digital Agenda 2014-2017*. Berlin: Federal Ministry for Economic Affairs and Energy, Federal Ministry of the Interior and Federal Ministry of Transport and Digital Infrastructure.

Federal Republic of Germany. 2018. *Artificial Intelligence Strategy*. Berlin: Federal Ministry of Education and Research, the Federal Ministry for Economic Affairs and Energy, and the Federal Ministry of Labour and Social Affairs

Fischerkeller, Michael. 2017. "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies", *Survival,* 59 (1): 103–134.

Greathouse, Craig B. 2014. "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" In: *Cyberspace and International Relations: Theory, Prospects and Challenges*, edited by Jan Frederik Kremer and Benedikt Müller, 21-40. Heidelberg: Springer.

Guzzini, Stefano. 2000. "A reconstruction of Constructivism in International Relations". *European Journal of International Relations*, 6.(2): 147–182.

Handelsverband Deutschland. 2019. *Frühjahrspressekonferenz Handelsverband Deutschland*. Powepoint Presentation, Düsseldorf, 24 April 2019 Acessado em 23 de novembro de 2019 < https://einzelhandel.de/images/presse/Pressekonferenz/2019/Fruehjahrs-PK/PK_Charts.pdf > .

Hansman, Simon and Ray Hunt. 2005. "A taxonomy of network and computer attacks". *Computers & Security*, 24 (1):31-43.

Herpig, Sven and Kira Messing. 2019. "Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik". *Stigung Neue Verantwortung*. Acessado em 23 de novembro de 2019 < https://www.stiftung-nv.de/de/publikation/akteure-und-zustandigkeiten-der-deutschen-cybersicherheitspolitik-3-auflage > .

Hopf, Ted. 1998 "The Promise of Constructivism in International Relations Theory". *International Security*, 23 (1): 171-200

Internet World Stats. 2019. "TOP 25 countries with the highest internet penetration rates (users divided by population"). Acessado em 23 de novembro de 2019 em < https://www.internetworldstats.com/top25.htm > .

Jepperson, Ronald L, Alexander Wendt and Peter J. Katzenstein, 1996. "Norms, Identity, and Culture in National Security" In: *The Culture of National Security Norms and Identity in World Politics*, edited by Peter J. Katzenstein, 33-78. New York: Columbia University Press.

Jozwiak, Rikard. 2019. "EU Approves New Cyber-Sanctions Regime ahead of Parliament Elections. *Radio Free Europe*. Acessado em 03 de julho de 2019 < https://www.rferl.org/a/eu-approves-new-cyber-sanctions-regime-ahead-of-parliament-elections/29947704.html > .

Katzenstein, Peter J. 1996. "Introduction: Alternative Perspectives on National Security" In: *The Culture of National Security Norms and Identity in World Politics*, edited by Peter J. Katzenstein, 1-32. New York: Columbia University Press.

Kowert, Paul and Jeffrey Legro. 1996. "Norms, Identity, and Their Limits: A Theoretical Reprise" In: *The Culture of National Security Norms and Identity in World Politics*, edited by Peter J. Katzenstein, 451-497. New York: Columbia University Press, 1996.

Lambach, Daniel. 2019. "The Territorialization of Cyberspace". *International Studies Review*, Oxford University Press < https://doi.org/10.1093/isr/viz022 > .

Latici, Tania. 2020. "Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence". *European Parliamentary Research Blog (EPRS*). Acessado em 01 de julho de 2019: < https://epthinktank.eu/2020/05/29/understanding-the-eus-approach-to-cyber-diplomacy-and-cyber-defence/https://epthinktank.eu/2020/05/29/understanding-the-eus-approach-to-cyber-diplomacy-and-cyber-defence > .

Macková, Veronika. 2013. "*Cyber War of the States: Stuxnet and Flame virus opens new era of war*". Policy Papers in Cyber Security. CENAA, 2: 1–10. Acessado em 01 julho de 2019 < http://cenaa.org/wp-content/uploads/2014/05/Veronika-Mackova-PP-No.-15-2013-Vol.-2.pdf > .

Maggi, Frederico, Marco Balduzzi, Ryan Flores; Lion Gu, and Vincenzo Ciancaglini. 2018. "Investigating Web Defacement Campaigns at Large". In: *ASIA CCS '18*, June 4–8, 2018, Incheon, Republic of Korea. Acessado em 09 de dezembro de 2019 < http://www.madlab.it/papers/hacktivism_asiaccs18.pdf > .

Mccarthy, Daniel R. 2015. *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and Internet*. New York: Palgrave Macmillan.

Mearsheimer, John J. 1995. "The False Promise of International Institutions". *International Security*, Harvard, 19 (3): 5-49. Acessado em 23 de setembro de 2015 < http://mearsheimer.uchicago.edu/pdfs/A0021.pdf > .

National Institute of Technology and Standards. 2013. "Security and Privacy Controls for Federal Information Systems and Organizations". NIST Special Publication. Acessado em 09 de dezembro de 2019 < https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf > .

Odell, John, S. 2004. "Case Study Methods in International Political Economy". In: *Model, Numbers and cases: Methods for Studying International Relations, edited by* Detlef F Sprinz and Yael Wollinsky.56-80. Ann Arbor: The University of Michigan Press.

Reuters. 2017. "German cyber agency calls for authority to hack back: Spiegel". Acessado em 04 de dezembro de 2019 < https://www.reuters.com/article/us-germany-cyber/german-cyber-agency-calls-for-authority-to-hack-back-spiegel-idUSKBN1DM1XU > .

Robin, Patrice. 2018. "Germany" In: *National Cybersecurity and Cyberdefense Policy Snapshots* edited by Robert S. Dewar, Collection 1, 43-62. Center for Security Studies (CSS), ETH Zürich.

Schweller, Randall L. 2004. "Unanswered Threats". *International Security,* 29 (2): 159-201.

Shabtai, Shay. 2016. "The War After Next Is Here — What Does the Elephant Look Like?" *Defense & Security Analysis,* 32(4):312–320.

Simsek, Ayhan. 2018. "*German companies lost billions to cyber-attacks: Report*". Anadolu Agency. Acessado em 23 de novembro de 2019 < https://www.aa.com.tr/en/economy/german-companies-lost-billions-to-cyber-attacks-report/1253827 > .

Sterling-Folker, Jennifer. 2002. *Theories of International Cooperation and the Primacy of Anarchy: Explaining U.S. International Policy Making After Bretton Woods*. New York: State University of New York Press.

Taliaferro, Jeffrey W. 2006. "State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State." *Security Studies*, 15 (3): 464-495.

União Europeia. Diretiva nº 2016/1148, de 06 de julho de 2016. *Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 Relativa a Medidas Destinadas a Garantir um Elevado Nível Comum de Segurança das Redes e da Informação em Toda a União.* Bruxelas, Acessado em 02 de julho de 2019 < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri = CELEX:32016L1148&from = EN > .

União Europeia. Regulamento nº 2019/881, de 17 de abril de 2019. *Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019 Relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à Certificação da Cibersegurança das Tecnologias da Informação e Comunicação e que Revoga o Regulamento (UE) No. 526/2013 (Regulamento Cibersegurança)*. Bruxelas. Acessado em 02 de julho de 2019. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri = CELEX:32019R0881&from = EN.

Walt, Stephen. 1987. *The Origins of Alliances.* London: Cornell University Press.

Wendt, Alexander. 1999. *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Wenkel, Rolf. 2017. "Germany in the digital slow lane". *Deutsch Welle (online)*. Acessado em 23 de novembro de 2019: < https://www.dw.com/en/germany-in-the-digital-slow-lane/a-39187166 > .