UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

HANDYLLY MATHIAS DOS SANTOS MATOS

A EVOLUÇÃO NORMATIVA DA SEGURANÇA CIBERNÉTICA NA UNIÃO EUROPEIA (2013 - 2024)

SÃO CRISTÓVÃO - SE
2025

HANDYLLY MATHIAS DOS SANTOS MATOS

A EVOLUÇÃO NORMATIVA DA SEGURANÇA CIBERNÉTICA NA UNIÃO EUROPEIA (2013 - 2024)

Trabalho de Conclusão de Curso II apresentado ao Departamento de Relações Internacionais como requisito para obtenção do título de Bacharel em Relações Internacionais pela Universidade Federal de Sergipe.

Orientador: Prof. Dr. Rodrigo Barros de Albuquerque.

SÃO CRISTÓVÃO - SE
2025

HANDYLLY MATHIAS DOS SANTOS MATOS

A EVOLUÇÃO NORMATIVA DA SEGURANÇA CIBERNÉTICA NA UNIÃO EUROPEIA (2013 - 2024)

Trabalho de Conclusão de Curso II apresentado ao Departamento de Relações Internacionais como requisito para obtenção do título de Bacharel em Relações Internacionais pela Universidade Federal de Sergipe.

Orientador: Prof. Dr. Rodrigo Barros de Albuquerque.

BANCA EXAMINADORA:

Prof. Dr. Rodrigo Barros de Albuquerque (orientador/UFS)

Prof. Dr. Cairo Gabriel Borges Junqueira (examinador/UFS)

Prof. Dr. David Paulo Succi Junior (examinador/UNESP)

AGRADECIMENTOS

Agradeço a Rodrigo por aceitar me orientar, por compartilhar seu conhecimento e por fazer parte da minha vida acadêmica. Minha admiração vai além destas simples linhas. Também agradeço aos professores Cairo e David, por lerem e deixarem importantes comentários no projeto deste trabalho, foi essencial para concluir esta segunda parte.

Agradeço a minha mãe, Sabrina, pela paciência e pelo apoio incondicional durante todo esse processo. Ela acredita em mim desde sempre. Também agradeço a minha irmã, Helena, principalmente pela companhia em alguns momentos durante o processo de escrita deste trabalho. Tudo fica mais leve com um abraço e um sorriso de quem mais amamos.

Agradeço também aos colegas de turma pelos quase quatro anos juntos e pelo conhecimento compartilhado. Em especial, agradeço Anna Clara e Sabrina, por fazerem com que minha passagem pela UFS fosse mais leve e alegre. O processo seria mais complicado sem Anna para compartilharmos todo nosso conhecimento sobre cinema e sem Sabrina para termos longas conversas sobre a vida. A amizade é essencial, e por isso deixo meu agradecimento aos meus amigos de fora da universidade que acompanharam minha trajetória e me auxiliaram de alguma forma durante o processo.

No curso de Relações Internacionais encontrei o meu lugar, e por isso deixo meu agradecimento ao Departamento de Relações Internacionais e a todos os docentes, pois, de alguma forma, vou levar um pouco de cada um ao decorrer da minha vida. De verdade, meu muito obrigado!

RESUMO

O ciberespaço elevou as preocupações dos Estados e das organizações acerca da soberania, da proteção de dados e da Inteligência Artificial. Dessa forma, emergiu diversos debates acerca da segurança cibernética, principalmente no que diz respeito à criação de regulamento nesse campo. Sendo assim, o presente trabalho analisa a segurança cibernética da Europa sob a ótica da União Europeia, com foco na estrutura normativa adotada para proteger suas instituições e Estados-membros. Para isso, examina os principais marcos regulatórios do bloco, como a criação da Agência Europeia para a Segurança das Redes e da Informação (ENISA), a Diretiva de Redes e Sistemas de Informação (NIS), o Regulamento para a Cibersegurança, e sua aplicação no fortalecimento da resiliência cibernética europeia. Além disso, a pesquisa explora a influência dos ciberataques sofridos pela Estônia em 2007 e pela Geórgia em 2008 na formulação das políticas de defesa digital da UE. Ademais, investiga como a segurança cibernética ganhou ou não aspectos securitizadores ao decorrer da formulação do arcabouço normativo da agenda no âmbito da UE. Ademais, ainda o papel e os impactos do processo de regulamentação da Inteligência Artificial no escopo da União Europeia. Para tal, será feita uma leitura de documentos oficiais da UE, juntamente com o uso da literatura especializada em cibersegurança no escopo da Europa e da União Europeia, bem como da teoria de securitização.

Palavras-chave: Ciberespaço; Segurança Cibernética; Normas; União Europeia; Securitizaçao.

ABSTRACT

Cyberspace has intensified concerns among states and organizations regarding sovereignty, data protection, and Artificial Intelligence. Consequently, numerous debates have emerged around cybersecurity, particularly concerning regulatory developments in this field. This study, therefore, analyzes cybersecurity in Europe from the perspective of the European Union, focusing on the normative framework adopted to protect its institutions and Member States. To this end, it examines the EU's key regulatory milestones, such as the establishment of the European Union Agency for Cybersecurity (ENISA), the Directive on Security of Network and Information Systems (NIS), and the Cybersecurity Act, and assesses their roles in strengthening European cyber resilience. Moreover, the research explores the influence of the cyberattacks against Estonia in 2007 and Georgia in 2008 on the formulation of the EU's digital defense policies. It also investigates whether and how cybersecurity has taken on securitized characteristics throughout the development of the EU's regulatory framework. Finally, the study addresses the role and impact of the regulatory process for Artificial Intelligence within the European Union. To achieve these objectives, the research draws upon an analysis of official EU documents, complemented by specialized literature on cybersecurity in Europe and the European Union, as well as the theory of securitization.

Key-words: Cyberspace; Cybersecurity; Norms; European Union; Securitization.

LISTA DE ABREVIATURAS E SIGLAS

CCDCOE - Centro de Excelência em Defesa Cibernética Cooperativa da OTAN

CERT - Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores

DDoS - Distributed-Denial of Service

DoS - Denial of Service

DIH - Direito Internacional Humanitário

ENISA - Agência Europeia para Segurança das Redes e da Informação

GDPR - Regulamento Geral de Proteção de Dados

GRENA - Georgian Research and Educational Networking Association

IA - Inteligencia Artificia**l**

ICJ - Corte Internacional de Justiça

NIS - Diretiva de Redes e Sistemas de Informação

OECD - Organização para a Cooperação e Desenvolvimento Econômico

ONU - Organização das Nações Unidas

ONGs - Organização não Governamental

OTAN - Organização do Tratado do Atlântico Nort**e**

TIC - Tecnologias da Informação e Comunicação

URSS - União das Repúblicas Socialistas Soviéticas

UE - União Europeia

LISTA DE FIGURAS

Figura 1 - Pirâmide de Riscos do Regulamento da UE sobre Inteligência Artificial

À minha mãe. Meu maior orgulho e minha fortaleza.

SUMÁRIO

1 INTRODUÇÃO..... 11

2 SEGURANÇA CIBERNÉTICA: CONJUNTURAS CRÍTICAS NA EUROPA.....15

2.1 A era digital.....15

2.2 O caso da Estônia.....16

2.3 O caso da Geórgia.....20

2.4 O Manual de Tallinn.....24

3 O ESCUDO CIBERNÉTICO EUROPEU..... 28

3.1 Segurança e a securitização do ciberespaço.....28

3.2 A Coordenação da segurança cibernética na União Europeia.....31

4 REGULAMENTAÇÃO SOBRE INTELIGÊNCIA ARTIFICIAL NA UE.....39

4.1 A Estratégia da UE para a Inteligência Artificial.....39

4.2 O Livro Branco da União Europeia sobre IA.....41

4.3 O Regulamento de Inteligência Artificial..... 42

CONSIDERAÇÕES FINAIS..... 46

REFERÊNCIAS BIBLIOGRÁFICAS..... 48

1 INTRODUÇÃO

Segundo Souza e Freitas (2022, p. 259), o ciberespaço é uma projeção do mundo real para uma realidade de interações virtuais – ou o contrário – marcada por uma espacialidade que permite novas formas de comunicação, sejam elas humanas, sociais ou econômicas para além do espaço físico. Desse modo, essa nova forma de se relacionar também resultou na transformação dos riscos, bem como da criminalidade, com o surgimento dos cibercrimes em suas diversas formas. Em adição, o ciberespaço influencia diretamente nas ações tomadas pelos Estados, visto que, assim como na realidade, as ameaças também estão presentes nos ambientes digitais e também possuem um elevado poder destrutivo (Savaş; Karataş, 2022). Sendo assim, graças a dependência em relação ao uso da internet para armazenar dados dos cidadãos e informações, bem como por ser um ambiente que integra e afeta não apenas o meio digital mas também o físico, o ciberespaço já é considerado o quinto domínio de guerra (Reisdoefer; Alcântara, 2020, p. 164).

Ademais, já é de amplo entendimento que o ciberespaço dispõe de diversas particularidades, muitas vezes sendo descrito por especialistas como uma "terra de ninguém". Por essa razão, na última década, discussões acerca desse domínio se tornaram mais frequentes entre os atores nacionais e internacionais ao ser identificada a necessidade de se criar instrumentos normativos para lidar com os cibercrimes. Uma das razões para isso é que os ambientes cibernéticos se tornaram uma parte fundamental no cotidiano da humanidade, visto que a grande maioria das pessoas passa a maior parte do dia utilizando ferramentas digitais (Savaş; Karatasş, 2022). Isto posto, a cibersegurança é uma agenda essencial para os países, organizações e também a razão para novas formas de tensão no que diz respeito à proteção de dados, segurança nacional e segurança internacional.

Além disso, devido a rápida transformação tecnológica que o ciberespaço impõe aos Estados e organizações, nos últimos anos houve uma intensificação no discurso acerca dos investimentos necessários para elevar a segurança cibernética. Esse discurso ganhou força graças à crescente regulamentação do ciberespaço por parte de diversos atores do sistema internacional, que estão criando mecanismos normativos com o intuito de estabelecer um espaço cibernético mais seguro para as pessoas, empresas privadas e para o setor público. Logo, os investimentos em segurança cibernética são essenciais, não apenas para a proteção de dados e infraestruturas, mas também para alcançar uma conformidade com as leis de proteção já implementadas em casos específicos (Kianpour; Raza, 2024).

A vista desses fatos, a governança cibernética também ganhou notoriedade na agenda de segurança cibernética. O termo é definido como o funcionamento de processos de tomada

[1]de decisões que visam aumentar a participação, a transparência e a responsabilidade na adoção de medidas relacionadas ao ciberespaço em conjunto com os mecanismos de acordos internacionais, estratégias e normas que se interligam da melhor forma possível observa (Savaş; Karataş, 2022). A governança cibernética se tornou uma das questões mais importantes dos últimos anos, principalmente no âmbito das organizações internacionais, que têm procurado soluções viáveis para os desafios dessa questão. Um dos marcos para essa busca foi a Convenção sobre o Cibercrime do Conselho da Europa (Savaş; Karataş, 2022).

Não obstante, segundo Jaak Aaviksoo (2010), a questão cibernética importa porque as ciberameaças também aumentaram a assimetria entre os atores por serem mais baratas, fáceis de desenvolver, por neutralizam a superioridade militar convencional e deixarem as sociedades conectadas mais vulneráveis. Ainda segundo o pesquisador, essa vulnerabilidade se estende além das ameaças às infraestruturas críticas como estamos acostumados a acompanhar. Graças a essa interconectividade, as sociedades ficaram ainda mais dependentes, e a cibersegurança, bem como a ciberdefesa, passaram a ocupar um lugar proeminente na agenda de segurança, ao lado da segurança energética, das preocupações em torno das mudanças climáticas e dos movimentos sociais.

Ademais, um ponto notório levantado por especialistas é que as ciberameaças não respeitam fronteiras, logo os oceanos não fornecem uma barreira natural contra “zeros e uns” (Jaak Aaviksoo, 2013, p. 15). Dessa forma, as ciberameaças passaram a se empenhar na disseminação do caos através dos meios tecnológicos, principalmente para obter ganhos políticos. Dessa forma, os ciberataques se tornaram uma poderosa ferramenta para desestabilizar governos democráticos e até mesmo para influenciar direta ou indiretamente resultados eleitorais. Em complemento a essa afirmação, o ex-ministro estoniano ainda afirma que:

> O ciberespaço é global e nenhum país é uma “ilha cibernética”. A segurança cibernética hoje está na mesma fase de desenvolvimento que a segurança marítima no século XVIII. Os ciberataques não respeitam nenhuma bandeira ou fronteira nacional. Nessa área, o Estado ainda tem um longo caminho a percorrer antes de alcançar o monopólio do uso da força. Se a capacidade de cruzar fronteiras instantaneamente dá aos cibercriminosos e invasores uma medida de impunidade, temos apenas uma escolha: estender o longo braço da lei e da ordem para além das fronteiras (Aaviksoo, 2013, p. 16).

Na Europa, dois casos de ataques cibernéticos ganharam destaque internacional, não somente pelas questões políticas nas quais tiveram origem, mas também pelos reflexos

[1] O Conselho da Europa é a principal organização de defesa de direitos humanos do continente e não faz parte da UE.

diretos no processo de securitização do ciberespaço. O primeiro ocorreu em 2007, na Estônia, causando impactos significativos na cooperação internacional através da criação do Cooperative Cyber Defense Center of Excellence (CCDCOE), localizado no país e estabelecido em conjunto com a Organização do Tratado do Atlântico Norte (OTAN). A criação do centro ainda deu origem ao Manual de Tallinn, documento que faz uma análise acerca das ações jurídicas que os Estados devem tomar em casos de crimes e conflitos cibernéticos. O segundo caso ocorreu em 2008, na Geórgia, e é notório por causar uma mudança particularmente interessante no sistema jurídico do país através da criação de agências e da implementação de normas para lidar com o ciberespaço, bem como pela alteração na percepção internacional do uso do espaço cibernético em conflitos tradicionais.

Não obstante, a União Europeia vem se destacando nesse campo por empregar maiores esforços na cibersegurança. Em grande medida, esses esforços para proteger o ciberespaço europeu se deram após os ataques à Estônia, caso em que a atuação da Agência Europeia para a Cibersegurança (ENISA) foi de muita importância. Em 2013, o bloco lançou a chamada Estratégia da UE para a Cibersegurança, cujo objetivo é fazer com que a UE alcance a resiliência cibernética, reduzindo cibercrimes, desenvolvendo políticas e métodos que complementem a segurança cibernética com a Política Comum de Segurança e Defesa. Ademais, o Regulamento para a Cibersegurança na União Europeia entrou em vigor em junho de 2019, no qual a ENISA passou a desempenhar um papel ainda mais importante quando se trata do combate às ciberameaças no âmbito da União Europeia (União Europeia).

No centro desse debate, a UE estabeleceu que os ciberataques em que são utilizados programas sequestradores, chamados de ransomware, são uma das maiores ciberameaças ao bloco e suas instituições atualmente. Além disso, ataques envolvendo o programa Distributed-Denial of Service (DDoS) também elevaram as preocupações por conta da sua capacidade de interromper serviços considerados essenciais (União Europeia). Cabe destacar que o DDoS foi a ferramenta utilizada para lançar os ataques em larga escala contra sites governamentais da Estônia em 2007 e, no ano seguinte, contra os sites da Geórgia.

Dito isso, o presente trabalho busca apresentar informações complementares sobre o ciberespaço e sobre a cibersegurança na Europa sob a ótica da União Europeia, fornecendo ainda um mapeamento das normas já implementadas no bloco europeu acerca do tema e suas implicações. Portanto, se questiona quais são as principais normas e regulamentos de segurança cibernética de que a União Europeia dispõe para proteger suas instituições, bem como os Estados-membros?

Assim sendo, é analisada a estrutura normativa de cibersegurança da UE, a exemplo da Diretiva de Redes e Sistemas de Informação, para que dessa forma seja possível mapear de que forma esses mecanismos estão sendo aplicados para elevar a proteção das instituições do bloco e dos seus Estados-membros. Além disso, foi feita uma análise sob a perspectiva da teoria da securitização para compreender como os ciberataques se tornaram uma ameaça existencial para a Europa e para o bloco europeu.

O trabalho consiste ainda em uma pesquisa exploratória. Dessa forma, busca estabelecer bases para estudos futuros referentes à segurança cibernética. Como metodologia, foi aplicada uma abordagem de caráter qualitativo, através da leitura de artigos acadêmicos, documentos oficiais disponibilizados por canais de comunicação oficiais da União Europeia e suas instituições. Além disso, foi feito o uso da leitura especializada em segurança cibernética e securitização.

Ademais, o trabalho está dividido em três capítulos. No primeiro, será feita uma contextualização de diferentes conjunturas críticas que afetam direta ou indiretamente a agenda cibernética da União Europeia, a exemplo do ataque cibernético sofrido pela Estônia em 2007 e do conflito entre Rússia e Geórgia no ano seguinte. Na segunda parte, será examinado todo o aparato de proteção cibernética já implementado na UE, sendo eles as normas e os regulamentos vigentes e de que forma o discurso de securitização influenciou no processo de implementação do mesmo. A terceira parte da pesquisa aborda a questão da Inteligência Artificial e como esse tema vem se tornando uma das prioridades do bloco para a consolidação do chamado escudo cibernético europeu e do protagonismo global.

2 SEGURANÇA CIBERNÉTICA: CONJUNTURAS CRÍTICAS NA EUROPA

2.1 A era digital

O século XXI já é considerado a era digital (Napetvaridze; Chochia, 2018), visto que a internet se tornou uma ferramenta essencial para o cotidiano da maior parte das pessoas ao redor do mudo. Essa dependência tecnológica trouxe inúmeros benefícios para as sociedades e para os Estados, sejam eles econômicos, militares ou sociais. Entretanto, com a criação da internet, surgiu também o ciberespaço, e ele, assim como o mundo real, está suscetível às ameaças, nomeadamente o que ficou conhecido como ataques cibernéticos, nas suas mais variadas formas. Em complemento a essa afirmação, Andrzej Kozlowski diz:

> O rápido desenvolvimento da internet fez com que o ciberespaço se tornasse cada vez mais usado por empresas privadas, chefes de Estado e pessoas comuns. Muitos elementos da vida cotidiana foram transferidos para o mundo virtual, e coisas como serviços bancários online e até mesmo votação online se tornaram comuns em muitos países. Além disso, elementos de infraestruturas críticas do Estado estão conectados à internet e tiram muita vantagem disso. A Revolução da informação também não poderia omitir os militares, permitindo-lhes o acesso à informação em tempo real. A rápida informatização do mundo mudou literalmente todos os aspectos da vida. (Kozlowski, 2013, p. 236).

Não obstante, os ataques cibernéticos se tornaram mais recorrentes na última década e, em alguns casos específicos, aumentaram significativamente as tensões entre Estados e os investimentos financeiros e políticos na agenda cibernética. Dessa forma, o ciberespaço se tornou também uma preocupação existencial para a comunidade internacional, demonstrando a necessidade de implementar normas para assim criar barreiras de proteção cibernéticas. Uma das razões para isso é a assimetria, característica do ciberespaço, visto que, segundo Carvalho (2019), o domínio possui ferramentas que têm o poder de provocar ações de grande impacto com poucos recursos. Além disso, o espaço cibernético pode potencializar o anonimato de criminosos cibernéticos, dada a dificuldade para se rastrear com precisão a autoria dos ataques.

Em adição, o ciberespaço também é visto como um ambiente propício a um novo tipo de conflito, denominado por especialistas como ciberguerra. A ciberguerra não substitui o conflito em sua forma tradicional, entretanto tem se mostrado como uma ferramenta complementar nos momentos de embates entre os Estados. Em sua essência, a ciberguerra é um conflito travado de forma “invisível”, principalmente nas linhas de comunicações, que hoje estão presentes em praticamente todas as partes do planeta e que permitem o fluxo de informação e comunicação entre as nações em tempo real (Ramos, 2013).

Como será melhor desenvolvido adiante, a primeira vez em que o termo guerra cibernética foi utilizado ocorreu durante os ataques cibernéticos à Estônia em 2007, quando instituições públicas e privadas foram atingidas por uma onda de Ataques de Negação de Serviço (DDoS). Outrossim, no ano seguinte, a disputa entre a Rússia e a Geórgia pelo controle do território separatista Ossétia do Sul voltou a acender do mundo também pelo uso de ataques cibernéticos como método para desestabilizar as forças georgianas. Dessa forma, os acontecimentos na Estônia e Geórgia evidenciam como o ciberespaço transformou as relações entre os Estados, bem como sua capacidade para gerar novas formas de conflitos.

2.2 O caso da Estônia

A Estônia é um dos três países bálticos e fica localizado no nordeste da Europa. Durante a maior parte da sua história, o país foi governado por outras nações, a exemplo da antiga União das Repúblicas Socialistas Soviéticas (URSS), da qual fez parte de 1940 até a dissolução do bloco ao final da Guerra Fria em 1991. Apesar do fim da União Soviética, a presença russa no país ainda é forte, principalmente através da influência dos meios de comunicação russos, da política russa, bem como da cultura. Todavia, apesar dessa forte ligação, desde 1991 a relação entre os dois países já não era das melhores e ganhou um novo capítulo turbulento na primavera de 2007 (Salma, Munabari, 2023).

No dia 27 de abril daquele ano, o governo estoniano decidiu realocar a Estátua do Soldado de Bronze, que homenageia os soldados do Exército Vermelho mortos em combate contra as forças alemãs, para um cemitério militar localizado nos arredores da capital estoniana, Tallinn. O monumento foi construído em 1947 e o governo estoniano nunca deu uma explicação concreta para a mudança da estátua, mas já era possível observar uma insatisfação da população estoniana, visto que para muitos a estátua simboliza a opressão da antiga União Soviética (Kozlowski, 2013).

Contudo, a minoria russa que vivia no país até então, cerca de 26% da população estoniana, enxergou o movimento como uma ofensa grave contra os russos e contra aqueles que morreram durante o conflito que terminou em 1945 (Kozlowski, 2013). Na época, o Kremlin também interpretou a alteração como uma ofensa, o que posteriormente serviu para embasar acusações contra o país acerca da autoria dos ciberataques (Ramos, 2013). Além disso, o cenário piorou por conta de protestos em frente à embaixada da Estônia na Rússia, organizado em sua grande maioria pelo Nashi Youth Group (Zahra, Handayani, Christianti, 2021). Ademais, as relações se deterioram de tal forma, que o governo russo aplicou restrições às exportações da Estônia, companhias russas suspenderam contratos com firmas

estonianas, o trânsito de carga ferroviária e portuária entre os países foi reduzido drasticamente e as conexões ferroviárias foram suspensas (Pernik, 2018, p.55).

A vista desses desdobramentos, a retaliação pela mudança do monumento não demorou muito, e ocorreu já no mesmo dia 27 de abril. Inicialmente, o país foi atingido pelo ataque cibernético conhecido como Denial of Service (DoS) e, em seguida, por uma versão ainda mais destrutiva, o Distributed-Denial of Service (DDoS), que consiste no envio maciço de acessos a um aplicativo ou site, causando congestionamento e impossibilitando o acesso à rede. O DDoS causou danos em sites considerados essenciais para a Estônia, a exemplo do website presidencial, do site do parlamento, da polícia, de alguns partidos políticos e de importantes veículos de imprensa. No dia 30 de abril, o país sofreu ataques mais sofisticados e coordenados, que atingiram as infraestruturas críticas de informações como o Domain Name Servers (DNS) (Pernik, 2018).

Dessa forma, também constatou-se que os ciberataques tiveram impacto nos meios para a distribuição de água e serviços de transporte estonianos. Em adição, no dia 4 de maio de 2007, o ataque cibernético atingiu os setores bancários estonianos e elevou as preocupações por ser uma ação mais sofisticada e coordenada em comparação com os ataques anteriores. Nessa fase, os alvos foram o Hansa Bank e o Eesti Uhisbank, impossibilitando o acesso da população às suas contas e causando um prejuízo de cerca de um milhão de dólares aos bancos. O ataque atingiu seu ápice no dia 09 de maio de 2007, data que coincidiu com o dia da independência russa, que comemora a vitória contra os nazistas (Zahra; Handayani; Christianti, 2021).

Dito isso, no início das investigações constatou-se que os ciberataques começaram de forma espontânea, vindo daqueles que de alguma forma se sentiram ofendidos com a mudança do local do Soldado de Bronze, em sua maioria hackers dispersos. Entretanto, autoridades estonianas desconfiavam de uma possível participação do Estado russo nos ataques. Como citado anteriormente, a Estônia conquistou sua independência em 1991, após a dissolução da União Soviética e as relações com a líder da antiga URSS sempre foram instáveis desde então. Além disso, em 2004, a Estônia aderiu à Organização do Tratado do Atlântico Norte (OTAN), algo que serviu como motivação para deteriorar ainda mais a relação entre os dois países, visto que Moscou não recebeu bem a nova configuração política tão próxima de suas fronteiras (Ramos, 2013). Segundo Kozlowski (2013), após a decisão do governo estoniano de transferir o monumento histórico, o Kremlin ainda acusou as autoridades de Tallinn de violarem direitos humanos, cobrando ainda a renúncia do então

Primeiro-Ministro do país. Dessa forma, o ciberataque é interpretado como o ponto mais alto de uma crise que já durava alguns anos.

Ademais, o ataque é considerado o primeiro conflito cibernético da história e se configura como um evento muito particular não somente por conta da capacidade destrutiva das ciberameaças e da tensão gerada entre o país e a Rússia, mas também pelo envolvimento direto de outros atores internacionais importantes. Apesar da Estônia ser considerado o país mais conectado da Europa, ainda assim não conseguiu lidar sozinha com as consequências dos ataques cibernéticos, recebendo apoio das forças da OTAN e da Agência da União Europeia para a Cibersegurança (Zahra; Handayani; Christianti, 2021, p. 52).

Segundo Salma e Munabari (2023), após os ciberataques, a OTAN, em conjunto com os aliados do Ocidente, consideraram como urgente o monitoramento dos ataques, bem como observar ainda suas ramificações na região. Dessa forma, a aliança ocidental enviou especialistas na área cibernética com o intuito de auxiliar na capacidade de proteção e investigação da Estônia através do fortalecimento da ciberdefesa do país. Logo que a aliança ocidental ficou a par do ataque, oficiais da Estônia apontaram que os autores do cibercrime estavam localizados em território russo e tinham fortes ligações com o serviço de segurança do governo.

Entretanto, a OTAN, bem como as autoridades da União Europeia, optaram por não acusar diretamente autoridades do Kremlin, visto que poderia causar uma escalada nas tensões e também porque era particularmente difícil rastrear com precisão o ponto focal dos ciberataques e apontar uma autoria sem antes realizar uma investigação detalhada. Em adição, Salma e Munabari (2023) ainda enfatizam que:

> O ataque à Estônia poderia inspirar organizações internacionais no futuro, e as circunstâncias da primavera de 2007 deram às nações um conhecimento crucial para o avanço e melhoria de suas capacidades de guerra cibernética. Embora a era da informação tenha muitas vantagens, ela também trouxe muitos perigos, incluindo o ciberterrorismo internacional e a guerra de informação. O ataque também demonstrou que nem mesmo o artigo 5 da OTAN e nem o poder nuclear dos EUA conseguem assegurar a soberania das nações no ciberespaço na era da globalização (Salma; Munabari, 2023, p. 34).

Meses após os eventos descritos, Sergei Markov e Konstantin Goloskokov reivindicaram a autoria dos ataques cibernéticos, negando o envolvimento do grupo Nashi, bem como do governo russo. O Nashi, que pode ser traduzido como “nosso”, é um movimento jovem, descrito como anti-fascista, criado em 2005 e considerado por muitos como um grupo pró-Putin. O movimento se tornou alvo de suspeitas por conta da reivindicação de Markov e Goloskokov, bem como por ambos serem comissários do grupo.

(Zahra; Handayani; Christianti, 2021). Além disso, constatou-se também que o Nashi recebia um investimento significativo da Obshestvennaya Palata, uma instituição financeira estatal russa. Entretanto, como citado anteriormente, localizar com precisão a autoria de um ataque cibernético é uma tarefa difícil e não se deve considerar apenas o contexto político em que ocorreu. No caso da Estônia, apesar das confissões de Sergei Markov e Konstantin Goloskokov, a Rússia se negou a cooperar com as autoridades estonianas para elucidar concretamente o que de fato ocorreu naquele período.

Outrossim, a crise do Soldado de Bronze foi importante para revelar toda a dimensão e capacidade destrutiva dos ciberataques, não somente pelos danos financeiros e físicos que podem causar, mas também pelo seu impacto psicológico, visto que podem impactar nas percepções dos indivíduos, induzir emoções, bem como alterar as opiniões e os comportamentos da população. O ministro da defesa da época, Jaak Aaviksoo apontou que o grande objetivo dos ataques era desestabilizar a sociedade estoniana, espalhando medo e ansiedade entre a população. Ademais, visava também ferir a reputação internacional da Estônia no que diz respeito à governança digital (Pernik, 2018). Em adição, internamente, a Estônia entendeu que era preciso recalcular a rota e identificar as principais vulnerabilidades do país para evitar que ataques semelhantes ocorressem novamente:

> Após os nossos ataques cibernéticos em 2007, chegamos a várias conclusões importantes. Percebemos que as velhas linhas divisórias entre conflitos domésticos e internacionais, problemas de defesa e segurança, aplicação da lei e soluções militares, públicas ou privadas, não se sustentam no ciberespaço. Nenhum ministério ou departamento pode lidar com o que é simultaneamente um problema de infraestrutura, defesa, aplicação da lei, comércio e liberdades civis. Além disso, 85% da infraestrutura da web está sob domínio privado. Portanto, 80% dos ataques cibernéticos são lançados contra empresas privadas, ONGs e indivíduos (Aaviksoo, 2013, p. 15)

Dessa forma, a Estônia compreendeu que era importante aplicar uma abordagem multissetorial internamente, desenvolvendo parcerias com o setor privado, isso serviu de arcabouço para o desenvolvimento da Estratégia Nacional de Cibersegurança, adotada ainda em 2008. Ainda segundo Aaviksoo (2013), a estratégia se destaca por adotar uma visão comum entre os principais atores da sociedade no que diz respeito aos meios para reduzir a vulnerabilidade estoniana no ciberespaço. O documento estabeleceu diretrizes para o setor público, setor privado, universidades, bem como para as ONGs e a sociedade em geral, funcionando como um mecanismo para diminuir as inconsistências que podem surgir durante a resposta a um conflito cibernético. Dessa forma, busca também dividir as responsabilidades entre os atores a fim de gerenciar melhor os recursos disponíveis.

2.3 O caso da Geórgia

Assim como ocorreu na Estônia, a Geórgia também foi alvo de ataques cibernéticos que moldaram a conjuntura cibernética a nível nacional, bem como internacional. Localizada no Cáucaso, é um país situado entre a Rússia, ao norte, e a Turquia, ao sul, e também fez parte da antiga União Soviética, da qual se tornou independente também em 1991 após a dissolução do bloco soviético. As similaridades entre os dois países ainda vão além, visto que, assim como os estonianos, a Geórgia também tem um relacionamento historicamente conturbado com o país vizinho. Grande parte das tensões entre Geórgia e Rússia se concentram em torno do domínio da região conhecida como Ossétia do Sul, estopim do conflito de 2008, bem como pela crescente aproximação do país com o Ocidente através das relações com a OTAN e com a União Europeia.

A Ossétia do Sul é uma região separatista da Geórgia localizada no Cáucaso, que durante décadas busca alcançar sua independência mediante referendos e manifestações públicas, nos quais a população já demonstrou de maneira massiva o desejo separatista, porém nunca conquistou reconhecimento em larga escala da comunidade internacional. Apesar da ligação com a Geórgia, desde 1992 a Ossétia do Sul já desenvolve instituições próprias de governo, com seus representantes sendo eleitos pela população local (Mielniczuk, 2013).

Todavia, a região esteve no centro do conflito ocorrido em agosto de 2008 entre a Rússia e a Geórgia. Em ocasiões anteriores ao conflito, a Ossétia do Sul já demonstrava um forte desejo em ser anexada pela Federação Russa, principalmente por conta de questões étnicas, entretanto o governo georgiano sempre manteve uma posição contrária. Segundo um levantamento realizado com a população da Ossétia do Sul e publicado em 2013, cerca de 90% da população tinha sentimentos considerados bons em relação à Rússia (Toal; O' Loughlin, 2013). Dessa forma, segundo Chaves e Schurster (2009) a Rússia passou a acusar o país vizinho de promover uma política nacionalista anti-Russia, enquanto a Geórgia acusava os russos de quererem reacender as aspirações imperialistas que outrora marcou as posições políticas a antiga URSS.

O conflito direto entre os dois países iniciou-se no dia 08 de agosto de 2008, quando a Geórgia promoveu um cerco a Tskhinvali, capital da Ossétia do Sul. Devido aos conflitos históricos preexistentes, bem como pela razão da cidade abrigar uma parcela considerável de russos, além das questões econômicas, o presidente russo à época, Dmitri Medvedev, ordenou um ataque das tropas russas contra as tropas georgianas (Chaves; Schurster, 2009, p.2).

Assim como na Estônia, este conflito ganhou notoriedade pela presença russa e também por conta da sua particularidade envolvendo o ciberespaço, visto que diversos fóruns online, em sua maioria no idioma russo, distribuíram listas de alvos, instruções, bem como ferramentas digitais com o intuito de perpetrar um ataque cibernético contra a Geórgia (Pernik, 2018).

O ataque cibernético entrou em curso em agosto do mesmo ano, tendo como principais alvos os sites do governo georgiano, agências de notícias e os meios de comunicação internos. Na ofensiva, sites do país foram invadidos e suas informações substituídas por imagens de propaganda russa, em alguns casos vinculando a imagem do então presidente do país, Mikheil Saakashvili, a símbolos nazistas. Ademais, cerca de 100 websites da Geórgia foram derrubados, entre eles o site da presidência e o site do parlamento (Napetvaridze; Chochia, 2019, p. 160). Como discutido no caso da Estônia, definir com precisão a autoria de um ataque cibernético beira o impossível, dada a sofisticação dos hackers, entretanto a Rússia logo foi acusada de estar por trás do novo conflito cibernético. O que corrobora essa percepção foi o curto espaço de tempo entre os ataques à Estônia no ano anterior, bem como os métodos semelhantes utilizados, visto que a Geórgia também foi atacada pelo programa conhecido como DDoS.

Especialistas apontaram que a Geórgia vivenciou uma guerra híbrida, pois, ao mesmo tempo em que era atacada no ciberespaço, também sofria ataques de tropas russas no mundo físico. O principal objetivo dos ataques era causar pânico na população e destruir arquivos governamentais, criando assim um vácuo nas informações estatais (Napetvaridze; Chochia, 2019, p. 161). É imprescindível destacar ainda que:

> Essa foi a primeira vez em que ações militares em larga escala foram acompanhadas por ataques cibernéticos massivos. Em 2008, não havia plano de ação coordenado na Geórgia para garantir a política do Estado, consequentemente, não havia agências estatais especiais responsáveis por manter a segurança do ciberespaço e nem mesmo uma lei relevante que qualificasse o ataque cibernético como crime, portanto, a Geórgia não estava preparada (Napetvaridze; Chochia, 2019, p. 162).

Todavia, diferente do que ocorreu na Estônia, os ataques cibernéticos a Geórgia foram mais bem coordenados, pois três anos após os eventos, em 2011, autoridades georgianas descobriram que, enquanto conflito militar ocorria no espaço físico, um sofisticado método de ciberespionagem foi utilizado no domínio cibernético. Segundo especialistas, o malware WIN/32/Geobot conseguiu acessar informações sensíveis e sigilosas relacionadas à segurança nacional do país localizadas em sites das instituições estatais georgianas, bem como informações importantes de organizações não governamentais (Pernik, 2018).

Um contraponto interessante a ser observado no caso da Geórgia em relação ao caso da Estônia é que o país não era altamente conectado, o que ajudou a atenuar de maneira considerável os efeitos do ciberataque e, além disso, é importante destacar que os CERTs da Estônia e da Polônia, em conjunto com a organização georgiana GRENA, conseguiram reduzir os danos causados. Todavia, o governo do país entendeu ser necessário considerar a relevância do ciberespaço e, principalmente, estabelecer mecanismos para proteger o país, para que dessa forma pudesse ter uma capacidade de resposta eficaz caso um evento semelhante ocorresse novamente. Segundo Napetvaridze e Chochia (2019), a percepção governamental é que a cibersegurança não é apenas uma forma de prevenção aos cibercrimes, mas também uma forma imprescindível para manter o bom funcionamento das instituições estatais e privadas através das suas ferramentas tecnológicas.

Além disso, é importante destacar que os ataques de 2007 contra a Estônia culminaram em uma mudança de paradigma, visto que expandiu os investimentos em segurança e defesa nacional no espaço cibernético, isso fez o país alcançar o status de modelo global em segurança digital. Um dos produtos dessa expansão foi a fundação do Cooperative Cyber Defense Center of Excellence (CCDCOE), patrocinado principalmente pela OTAN. Em contrapartida, os ataques sofridos pela Geórgia marcaram o uso de ataques cibernéticos em conflitos militares, facilitando, em grande medida, uma mudança radical na percepção militar do ciberespaço. Em agosto de 2008, Kenneth Geers, especialista em cibersegurança, afirmou que a partir daquele momento todos os conflitos políticos e militares passariam a ter uma dimensão cibernética (Napetvaridze; Chochia).

Dessa maneira, para expandir a segurança cibernética da Geórgia, em 2010, o governo adotou o Documento de Avaliação de Ameaças da Geórgia, nele a proteção do ciberespaço passou a ser considerada uma questão de segurança nacional (Napetvaridze; Chochia, 2019, p. 164). É notório destacar que esse passo da Geórgia é um fato interessante, visto que, como citado anteriormente, na época dos ataques cibernéticos o país não possuía nenhuma legislação ou órgão estatal relevante que pudesse lidar com as questões do ciberespaço, demonstrando como as ciberameaças podem transformar de maneira significativa a agenda de segurança dos Estados e das organizações. Em adição, o documento ainda faz a seguinte afirmação:

> Durante a guerra de 2008, a Federação Russa usou ataques cibernéticos concentrados e massivos contra a Geórgia, em paralelo com o uso das forças terrestres, aéreas e navais. Esses ataques cibernéticos demonstraram que a defesa do ciberespaço é tão importante para a segurança quanto à defesa dos espaços terrestres, marítimos e aéreos. A experiência de 2008 mostra que ataques

> empregando tecnologias da informação representam uma ameaça real no mundo globalizado moderno (National Threat Assessment Document of Georgia).

Ademais, após a compreensão de que a cibersegurança é uma questão de segurança nacional, ainda em 2010 a Geórgia implementou a Lei de Crime Cibernético como parte do Código Penal. Dessa forma, o país constatou que também era necessário criar agências que pudessem lidar especificamente com os assuntos de cibersegurança e ciberdefesa. Em janeiro de 2011, foi criada uma equipe capacitada para responder a emergências tecnológicas, estando sob a jurisdição da Agência de Intercâmbio de Dados do Ministério da Justiça. A agência está equipada para lidar com incidentes cibernéticos que eventualmente possam afetar as redes governamentais e as infraestruturas críticas da Geórgia (Napetvaridze; Chochia, 2019).

Ademais, em janeiro de 2014, foi criado o Departamento de Segurança Cibernética, sob a responsabilidade do Ministério da Defesa e tendo como principal função o desenvolvimento de sistemas de tecnologia de informação estáveis, eficazes e seguros (Napetvaridze; Chochia, 2019). É importante destacar que nada disso garante a segurança cibernética e que também é importante analisar a eficácia dos novos sistemas, mas a drástica mudança de postura do país foi notória por conta do interesse estatal em investir recursos para elevar a segurança e a soberania digital do país.

Cabe destacar ainda que, em 2012, após a ratificação do Conselho Europeu sobre segurança cibernética, a Geórgia foi incluída na lista oficial de países que declararam guerra ao crime cibernético. Além disso, o crescente número de ataques cibernéticos massivos influenciaram diretamente países, principalmente do Ocidente, a criarem políticas de Estado na área de cibersegurança. A Geórgia pode se enquadrar como um desses países, visto que antes do conflito em 2008 o país não desenvolvia políticas públicas no âmbito do ciberespaço e nem enxergava o crime cibernético como uma questão de segurança nacional. Como citado anteriormente na pesquisa, esse entendimento mudou consideravelmente através da criação de agências e da aprovação de leis específicas para lidar com questões acerca do ciberespaço. A mudança de postura também aproximou ainda mais o país de grandes potências, a exemplo da OTAN, bem como da União Europeia.

Não obstante, os ataques à Geórgia, bem como à Estônia, marcaram o início de uma nova era quando se fala de espaço cibernético, visto que demonstraram como ataques digitais podem ser utilizados como ferramentas de pressão política e guerra híbrida. Concomitantemente, ainda evidenciaram a vulnerabilidade das infraestruturas digitais e a

dependência da população em relação às ferramentas disponibilizadas pelo espaço cibernético, fato que resultou na necessidade de estudos mais detalhados acerca da importância desse domínio. Dessa forma, considerando os fatos debatidos, constatou-se a importância de se estabelecer diretrizes jurídicas sobre a aplicação do Direito Internacional no âmbito dos conflitos cibernéticos, e um dos primeiros passos para isso foi dado através do que ficou conhecido como Manual de Tallinn. Apesar de não ser normativamente vinculante, o documento tornou-se uma referência importante para governos e especialistas no que diz respeito à interpretação das normas internacionais sob a ótica do ciberespaço.

2.4 O Manual de Tallinn

No dia 14 de março de 2008, foi criado o Cooperative Cyber Defense Center of Excellence (CCDCOE), cujo objetivo principal é apoiar os países membros da OTAN no que diz respeito aos assuntos cibernéticos. As atividades do centro incluem pesquisa, treinamento, exercícios de defesa cibernética, bem como visa auxiliar os membros com tecnologia, estratégia e operações. O CCDCOE foi criado por iniciativa da Estônia, algo que o país já vinha tentando estabelecer desde 2004, sem sucesso. Entretanto, os ataques cibernéticos sofridos pelo país em 2007 representaram um fator crucial para a criação do centro, servindo como um alerta político para os Estados-membros da organização sobre a importância e os perigos provenientes do ciberespaço (CCDCOE).

Outrossim, ainda em 2008, o Conselho do Atlântico Norte concedeu ao centro a classificação de Organização Militar Internacional. Além disso, ganhou mais relevância internacionalmente ao conduzir conferências internacionais em 2009, com foco nos aspectos legais e tecnológicos, bem como ao promover pesquisas acerca dos conflitos cibernéticos. Em complemento, o centro realiza anualmente, desde 2010, o que é considerado o maior e mais complexo exercício internacional de defesa cibernética do mundo, nomeado de Locked Shields (CCDCOE).

Inicialmente, o centro de excelência foi criado em conjunto com outras seis nações, sendo elas Alemanha, Itália, Letônia, Lituânia, Eslováquia e Espanha, atualmente, cerca de 32 países são membros do centro e outros sete são parceiros, a exemplo da Coreia do Sul e da Suíça. Dessa forma, o CCDCOE se tornou um “efeito colateral” particularmente interessante no pós-ataques de 2007, principalmente por conta da sua relevância enquanto ferramenta para auxiliar em questões técnicas acerca do ciberespaço. Por iniciativa do CCDCOE, em 2009, foi implementado o processo que daria origem ao Manual de Tallinn, documento elaborado por acadêmicos e militares publicado em 2013 pela Cambridge University Press (CCDCOE).

Sua criação foi impulsionada pelos ataques cibernéticos contra a Estônia, bem como pelo conflito entre Rússia e Geórgia, casos descritos anteriormente. Schmitt aponta que:

> O Manual de Tallinn examina as leis internacionais que regem a “guerra cibernética". Em geral, abarca tanto o jus ad bellum, lei internacional que rege o uso da força pelos Estados como instrumento de política nacional, quanto o jus in bello, lei internacional que regula a conduta em casos de conflitos armados. Questões relacionadas ao direito internacional, como a responsabilidade do Estado e a leis do mar, também são tratados no contexto desses tópicos (Schmitt, 2013, p. 18).

Em adição, Michael Schmitt (2013, p. 18) enfatiza que os pontos levantados no manual dizem respeito a legalidade das atividades de inteligência cibernética e como elas estão relacionadas com as noções de *jus ad bellum* de uso da força e ataque armado, ou no contexto de conflito armado sob a noção de *jus in bello,* promovendo uma análise da Carta da ONU, das Convenções de Genebra e do Direito Internacional Humanitário (DIH). Ressalta-se ainda que, apesar de sua importância, o Manual de Tallinn não tem valor legal no âmbito do direito internacional, consoante o Artigo 38 da Corte Internacional de Justiça (ICJ). Porém, segundo pesquisadores da área, a regra 30 do manual tem capacidade de se tornar pelo menos um costume internacional no futuro (Zahra; Handayani; Christianti, 2021, p. 61).

A Regra 30 do manual define o que é um ataque cibernético. Segundo o documento, um ataque cibernético é uma operação, seja ela ofensiva ou defensiva, em que se espera que cause ferimentos ou morte às pessoas, bem como danos e destruição a objetos (Manual de Tallinn 1.0, 2009). Os autores do manual destacam que a noção de ataque no direito internacional serve de base para diversas limitações e proibições em que, de maneira geral, se entende que civis e objetos civis não devem ser atacados. Dessa forma, os autores ainda pontuam:

> A palavra “causa” desta regra não se limita aos efeitos no sistema cibernético alvo. Na verdade, abrange qualquer dano consequente, destruição, ferimento ou morte razoavelmente previsível. Ataques cibernéticos envolvem raramente o uso da força física direta contra um sistema cibernético alvo; no entanto, eles podem resultar em grandes danos a indivíduos ou objetos. Por exemplo, liberação de águas de barragens pela manipulação de um sistema SCADA pode causar destruição em massa sem necessariamente danificar o sistema. Se essa operação fosse conduzida pelos meios comuns, como por exemplo o bombardeio da barragem, não restaria dúvidas de que seria considerado um ataque. Não existe nenhuma justificativa para chegar a uma conclusão diferente no contexto cibernético (Manual de Tallinn 1.0, 2009).

Ademais, o manual de Tallinn 1.0 sofreu algumas alterações desde o seu processo de escrita, entre 2009 e 2012, e seu lançamento em 2013. Em 2017, foi publicado o Manual de Tallinn 2.0 e, enquanto na versão anterior o manual aborda questões mais severas envolvendo operações cibernéticas, a exemplo das violações do uso da força, a versão 2.0 considera em

seu texto as regras do direito internacional que regem os incidentes cibernéticos que os Estados precisam lidar no dia a dia. Além disso, para acompanhar as constantes mudanças do ciberespaço, o CCDCOE já está trabalhando desde 2021 na versão 3.0 do Manual. O processo terá uma duração de cinco anos e irá revisar os capítulos já existentes do Manual, bem como irá explorar novas questões que afetam o interesse dos Estados no âmbito do direito cibernético (CCDCOE).

Dessa maneira, a importância do Manual de Tallinn pode ser medida através da sua influência direta nos países da OTAN, visto que o documento se tornou uma ferramenta auxiliar no desenvolvimento de estratégias cibernéticas em que esses Estados se baseiam nos princípios apresentados pelo Manual. Ademais, graças a contribuição do manual acerca das interpretações do Direito Internacional no âmbito do ciberespaço, em 2021, durante a cúpula de Bruxelas, a Aliança Militar do Ocidente reafirmou o impacto das atividades, das transformações e dos riscos cibernéticos, reconhecendo que atividades maliciosas significativas podem, em certas circunstâncias, ser consideradas um ataque armado que levando o Conselho do Atlântico Norte a invocar o Artigo 5 da organização sobre o princípio da defesa coletiva (OTAN, 2021).

Ademais, esse reconhecimento do Artigo 5, apesar de muito vago em sua definição, pode ser interpretado como um dos reflexos do ataque cibernético a Estônia em 2007, visto que CCDCOE define o acontecimento como o "ataque que mudou o jogo" e utiliza a crise do Soldado de Bronze como marco para definir ataques cibernéticos generalizados (OTAN, 2021). É válido relembrar que, ainda em 2007, nos dias que se seguiram ao ataque, o então Ministro da Defesa, Jaak Aaviksoo foi uma das primeiras figuras políticas a levantar a discussão sobre o tema, enfatizando que na época a Aliança não definia ataques cibernéticos como ação militar clara, o que impedia o uso do artigo 5. Todavia, o ministro enfatizou que o tema iria precisar ser resolvido em um futuro próximo (The Guardian, 2007).

Outrossim, os ataques à Estônia, o conflito híbrido na Geórgia e a criação do Manual de Tallinn foram responsáveis por dar início de maneira mais concisa ao debate sobre a securitização do espaço cibernético. Como discutido nos casos anteriores, os ataques a Estônia demonstraram para o mundo e, mais especificamente para a Europa, o potencial destrutivo de um ataque cibernético, fato esse que resultou em uma mudança radical de percepção dos Estados, bem como das grandes organizações, a exemplo da Organização do Tratado do Atlântico Norte e da União Europeia. Além disso, o fato influenciou diretamente na criação do Cooperative Cyber Defense Centre of Excellence, que por sua vez se tornou um espaço propício para a cooperação entre os Estados-membros da OTAN, bem como

proporcionou a cooperação com países que não fazem parte da organização, a exemplo dos parceiros externos (OTAN). Da mesma forma, o conflito entre Rússia e Geórgia serviu como um alerta para o uso de ferramentas cibernéticas durante conflitos convencionais e ainda influenciou os debates sobre o uso militar dos instrumentos tecnológicos.

Ademais, o Manual de Tallinn, mesmo não tendo força de lei, estabelece diretrizes para uma eventual resposta do Estado a ataques cibernéticos, foi essencial para esclarecer questões acerca da soberania dos Estados no espaço cibernético e ainda influenciou na formulação de políticas cibernéticas nacionais e internacionais. Dessa forma, a seguir será feita uma análise das normas de cibersegurança no âmbito da União Europeia, visto que, ao decorrer dos últimos anos, o bloco se tornou um modelo no que se refere ao desenvolvimento e aplicação de normas cibernéticas.

3 O ESCUDO CIBERNÉTICO EUROPEU

3.1 Segurança e a securitização do ciberespaço

Segundo Buzan et al (1998), o termo segurança se aplica ao movimento que leva a política para além das regras estabelecidas do jogo, elevando a questão a um tipo especial de política ou até mesmo a um nível acima disso. Em contrapartida, segundo os autores, a securitização localiza-se em um aspecto mais extremo da politização. Dessa maneira, qualquer matéria pública pode ser incluída neste espectro, porém com algumas variações, sendo elas não politizadas, politizadas e securitizadas, essa última acontece quando a questão é apresentada como uma ameaça existencial, exigindo medidas de emergência e justificando ações fora dos limites normais do procedimento político (Buzan et al. 1998, p. 23). Dada a complexidade do sistema internacional, as pautas politizadas muitas vezes podem variar entre os Estados:

> Alguns Estados podem politizar a religião (Irã, Arabia Saudita, Birmânia) e alguns não (França, Estados Unidos). Alguns podem securitizar a cultura (ex-União Soviética) e outros não (Reino Unido, Países Baixos). No caso de algumas questões que sairam dramaticamente da categoria nao politizada nota-se a dupla questão de saber se eles apenas foram politizados ou também foram securitizados (Buzan et al, 1998)

A vista disso, a definição exata e os critérios de securitização são constituídos pelo estabelecimento intersubjetivo de uma ameaça existencial com relevância suficiente para causar efeitos políticos substanciais (Buzan et al. 1998, p. 25). Dito isso, no caso da segurança cibernética, segundo as acadêmicas Lene Hansen e Helen Nissenbaum (2009), inicialmente a Escola de Copenhague tratou os desdobramentos acerca desse tema como uma mera tentativa de securitização, visto que o entendimento era de que a cibersegurança não causava nenhum efeito sobre outras questões de segurança (Buzan et al. 1998 apud Hansen, Nissenbaum, 2009). Todavia, segundo Hansen e Nissenbaum (2009) essa compreensão mudou ao longo dos anos, principalmente pela influência das transformações tecnológicas e políticas significativas, a exemplo da formulação da Estratégia de Segurança Nacional Cibernética implementada por George W. Bush em 2003 nos Estados Unidos e da criação do Cooperative Cyber Defence Center of Excellence na capital da Estônia em 2008.

Ademais, os estudos acerca da cibersegurança enquanto conceito securitizador tiveram início fora dos debates das relações internacionais, notadamente nas disciplinas de informática e ciências da computação, no qual a primeira menção a segurança cibernética

ocorreu no Conselho de Informática e Telecomunicações. Na ocasião, o órgão definiu segurança como a proteção contra a divulgação, modificação ou destruição de dados de um sistema e também a proteção dos próprios (Hansen, Nissenbaum, 2009).

Entretanto, para a Escola de Copenhague, essa ótica se encaixa mais no campo da segurança da informática e, por essa razão, não se encaixaria como uma pauta de securitização. Isso se dá porque, segundo Helen Nissenbaum, a segurança da informática não se qualificaria, na maioria dos casos, como um conceito de segurança, visto que a maioria dos cientistas da computação geralmente adotam um discurso mais técnicos, a exemplo do desenvolvimento de programas eficientes capazes de impedir o acesso de invasores externos. Todavia, houve uma mudança significativa nesse entendimento visto que a segurança da informática passou a ser conhecida como cibersegurança e, dessa forma, o discurso técnico tornou-se um elemento complementar ligado diretamente ao discurso securitizador, visto que, em alguns casos, pode ser desenvolvido no âmbito da segurança nacional (Hansen, Nissenbaum, 2009).

Em adição, no relatório publicado em 1991, o Conselho de Informática e Telecomunicações enfatiza que a população estão em risco quando se trata das ameaças cibernéticas, e Nissenbaum (2009) utiliza o uso dessas palavras para dizer que essa afirmação torna sim cibersegurança uma pauta securitizadora, visto que o perigo existencial é um dos maiores argumentos utilizados pelos agentes durante o processo de securitização. Dessa maneira, ao longo dos últimos anos, mais especificamente nas últimas duas décadas, a cibersegurança passou a transitar com muita facilidade nos mais diversos setores considerados essenciais para os Estudos de Segurança.

O tema ganhou alcance significativo nos estudos de segurança individual e segurança coletiva, entre as instituições públicas e instituições privadas, bem como entre a segurança econômica e a segurança político-militar (Hansen, Nissenbaum, 2009). Essa relevância crescente é motivada pelo receio do setor econômico, bem como do setor público e privado, de uma perda financeira acentuada e de que ataques cibernéticos elevem as preocupações na segurança pública nacional dos Estados.

Em complemento, segundo Hansen e Nissenbaum (2009), o sistema econômico moderno e, assim como a rede cibernética, é constituído por redes transfronteiriças, e a autoridade e a soberania estão localizados de forma mais ambígua do que na segurança nacional-militar tradicional. As autoras também reforçam argumentos discutidos no capítulo anterior, dessa vez com a adição do setor econômico, ao afirmarem que, em ambos os setores, em diversas ocasiões é difícil identificar a origem de um ataque cibernético. Isso ocorre

porque, com o alcance da internet, bem como da economia mundial, questões acerca das responsabilidades na aplicação de medidas normativas ainda são fontes contínuas de problemas transfronteiriços (Hansen, Nissenbaum, 2009).

Em suma, a segurança cibernética hoje se concentra em dois níveis. O primeiro engloba as tecnologias digitais, especificamente o bom ou mau uso por parte dos atores humanos em contextos econômicos, sociais e políticos. Já a segunda dimensão é caracterizada por processos de negociação duradouros e, muitas vezes, altamente conflituosos em contextos formais e informais o Estado e suas burocracias, a sociedade e o setor privado, principalmente em pautas que possam definir os papéis, as responsabilidades, os limites legais e as regras aceitáveis em se tratando de cibersegurança (Cavelty, Wenger, 2019, p. 4).

Não obstante, Hansen e Nissenbaum (2009) apresentam três conceitos fundamentais que auxiliam na identificação do grau de securitização da segurança cibernética, fazendo mediante os argumentos elaborados por Buzan. O primeiro conceito apresentado pelas autoras é a hiper securitização que possibilita observar a expansão da securitização para além do nível considerado normal de ameaças e perigos, ação que leva a um exagero do que é considerado ameaça, recorrendo a contramedidas consideradas excessivas. Um exemplo disso é a comparação entre os discursos de segurança cibernética e ambiental, visto que, segundo as autoras, nas argumentações mais drásticas se costuma afirmar que o destino do planeta está em jogo.

Em ambos os discursos, o fator da irreversibilidade da situação é crucial. No caso da segurança ambiental, coloca-se em foco a questão da extinção humana, enquanto no caso cibernético, o desaparecimento de um sistema digital e seu efeito cascata que pode gerar caos generalizado. É claro que ambos os exemplos diferem muito um do outro, visto que no caso ambiental o processo é mais lento e as chances de reversão são bem menores, já no caso cibernético é instantâneo, porém as chances de reversão são maiores. Dessa forma, os discursos securitizadores muitas vezes recorrem à urgência para alcançar a legitimidade (Hansen; Nissenbaum, 2009).

O segundo conceito é chamado de práticas diárias de segurança, e consiste na forma como os atores securitizadores transformam as atividades consideradas normais em cenários críticos para influenciar o cotidiano dos indivíduos. Cabe observar que esses atores em geral podem ser organizações e empresas privadas, bem como políticos e figuras de grande relevância social. Essa transformação nas atividades consideradas corriqueiras tem como principal objetivo criar um ambiente para inflar e respaldar as ações da hiper securitização. Todavia, a securitização cibernética da vida cotidiana apresenta algumas distinções, visto que

nela o indivíduo pode ser um parceiro no combate à insegurança, mas também pode ser visto como uma responsabilidade que recai sobre os atores ou até mesmo uma ameaça (Hansen, Nissenbaum, 2009).

Em adição, o terceiro conceito é o da tecnificação e diz respeito ao papel que os especialistas de determinada área desempenham no processo de securitização. No caso da segurança cibernética, segundo Hansen e Nissenbaum (2009) os especialistas em cibersegurança alcançaram um papel ainda maior do que se constata em outras áreas, visto que eles transcenderam suas localizações científicas específicas e já estabeleceram um contato direto com o público de forma ampla em um movimento facilitado que funciona para apoiar as securitizaçoes cibernéticas reivindicadas por políticos, bem como pela mídia (Hansen, Nissenbaum, 2009, p. 1167).

> O papel privilegiado atribuído aos cientistas da computação e da informação no discurso da segurança cibernética é, em parte, um produto da própria lógica da securitização: se a segurança cibernética é tão crucial, não deve ser deixada para amadores. No entanto, cientistas e engenheiros da computação não são apenas especialistas, mas técnicos e constituir a segurança cibernética como seu domínio é tecnificar a segurança cibernética. As tecnificações são, como securitizações, atos de fala que "fazem algo" em vez de apenas descrever, e constroem uma questão como dependente de conhecimento técnico e especializado, mas também pressupõe simultaneamente uma política e normativamente à qual a tecnologia serve (Hansen, Nissenbaum, 2009, p. 1167).

Dessa forma, segundo Lene Hansen e Helen Nissenbaum (2009, p. 1167) essa busca por tecnificação tem como principal objetivo alcançar uma legitimidade por meio de uma autoridade epistêmica, na qual o técnico demonstra ter um domínio na no qual nem a maioria da população e nem os políticos envolvidos no processo são detentores. A vista disso, os especialistas se tornam atores securitizadores ao mesmo tempo em que se distinguem da “politicagem” dos políticos e outros atores do mesmo nicho. Em adição, é importante enfatizar que o técnico e o objeto securitizado precisam ser vistos como partes que se complementam de maneiras complexas (Hansen, Nissenbaum, 2009, p.1168).

Não obstante, o intuito desta seção da pesquisa foi trazer os principais conceitos sobre segurança, securitização e os elementos que caracterizam a teoria. Dessa forma, na seção seguinte será feita uma análise do aparato cibernético da União Europeia sob a ótica das normas já implementadas desde 2013, buscando identificar se houve um processo de securitização da agenda cibernética do bloco europeu, com base nos três conceitos discutidos. Além disso, será debatido se houve ou não alguma influência direta indireta dos eventos ocorridos na Estônia e na Geórgia na agenda cibernética da UE.

3.2 A Coordenação da segurança cibernética na União Europeia

Segundo Bederna e Rajnai (2023), durante a campanha de ciberataque contra a Estônia, a União Europeia reconheceu a importância da cibersegurança e enfatizou a necessidade de tomar medidas para elevar o nível das capacidades de ciberdefesa, o que, nos anos seguintes, resultou em diversas mudanças no quadro normativo do bloco europeu. Em 2013, como consequência da ascensão do ciberespaço, a União Europeia lançou a Estratégia da UE para a Cibersegurança, cujo objetivo é fazer com que a União Europeia alcance a resiliência cibernética, reduzindo cibercrimes, desenvolvendo políticas e instrumentos normativos que complementem a segurança cibernética com a Política Comum de Segurança e Defesa (Comissão Europeia). Segundo Fuster e Jasmontaite (2020), a publicação da estratégia é um marco importante até hoje, visto que estabeleceu a segurança cibernética como uma nova política no âmbito do bloco europeu. Em adição, enfatiza-se ainda que:

> A Estratégia de 2013 forneceu uma definição segundo a qual "[c]ibersegurança geralmente se refere às salvaguardas e ações que podem ser usadas para proteger o domínio cibernético, tanto no campo civil quanto militar, das ameaças que estão associadas ou podem prejudicar suas redes interdependentes e infraestrutura de informação" (Comissão Europeia e Alto Representante 2013). Nesse contexto, os objetivos primários da cibersegurança foram considerados a preservação da disponibilidade e integridade das redes e infraestrutura e a confidencialidade das informações nelas contidas (Fuster, Jasmontaite, 2020).

Outrossim, reafirmando o que Hansen e Nissenbaum (2009) já haviam discutido anteriormente, Fuster e Jasmontaite (2020) observam que a segurança cibernética hoje em dia é considerada uma agenda altamente complexa e requer o envolvimento ativo de uma série de partes interessadas nessa questão, incluindo os legisladores. Além disso, os autores afirmam que essa ótica normativa representa uma mudança expressiva, visto que a área era entendida como uma questão puramente técnica relacionada a medidas que buscavam garantir a disponibilidade, integridade e confidencialidade de informações e sistemas de informação (Fuster, Jasmontaite, 2020). De fato, esse ainda é o objetivo central da segurança cibernética em sua última instância, porém não é mais possível ignorar a crescente influência dos discursos políticos neste processo.

Ademais, ao longo dos anos, constatou-se que a segurança cibernética na escala da União Europeia é um exemplo claro de como os diferentes campos de políticas do bloco precisam ser combinados. Além disso, as medidas de cibersegurança, como a maioria das políticas do bloco, precisam ser tomadas tanto no nível da UE como também nos Estados-membros. Nesse último ponto, pesquisadores enfatizam que fragmentação, inerente à estrutura do bloco, podem dificultar as ambições de resiliência cibernética que a UE destaca

em sua estratégia, visto que a necessidade de competências externas depende frequentemente da existência de competências internas, limitando os poderes legais da União como interveniente global no domínio cibernético (Fuster, Jasmontaite, 2020).

Outrossim, na Estratégia, Bruxelas destaca que a tecnologia é a pedra angular do desenvolvimento do ciberespaço, sendo um importante instrumento para a adaptação permanente no processo de evolução tecnológica. Em adição, o documento também aponta que um elevado nível de segurança das redes e da informação não somente são cruciais para a manutenção de serviços essenciais que mantêm o bom funcionamento da economia europeia, mas para garantir a integridade física dos cidadãos europeus (Parlamento Europeu, 2013). Durante o processo de pesquisa não foi possível identificar uma ligação direta entre a regra número 30 do Manual de Tallin e este ultimo ponto da Estrategia de 2013 da UE, mas é interessante notar a menção a integridade física das pessoas ao mencionar os riscos dos ciberataques, ponto que foi discutido durante os ataques a Estônia, bem como durante o processo de formulação do Manual iniciado em 2009.

Em complemento, Bruxelas salienta que as atividades criminosas no ciberespaço são tão prejudiciais para o bem-estar das sociedades quanto as infrações cometidas no mundo físico. Dessa maneira, muitas vezes essas formas de crime se reforçam mutuamente, a exemplo da exploração sexual de crianças e do crime organizado. Além disso, o documento destaca a necessidade de elevar o apoio e os recursos financeiros para a Eurojust, para o Centro Europeu de Criminalidade da Europol, para os CERT, bem como para as universidades e centros de investigação, visto que também são vitais para o combate à cibercriminalidade (Parlamento Europeu, 2013).

Ademais, na atualização de 2020 da estratégia, a União Europeia ainda reforça a necessidade da cooperação internacional, visto que no ciberespaço global os ciberataques e as ciberameaças frequentemente tem sua origem de fora da União. Sendo assim, o documento salienta a necessidade de que o bloco e os Estados-membros cooperem para promover o comportamento responsável do Estado para dessa forma aumentar a resiliência global e a sensibilização no que tange às ciberameaças (Comissão Europeia, 2020).

Em paralelo com a estratégia, a UE também já trabalhava na chamada Diretiva de Redes e Sistemas de Informação (NIS ou UE 2016/1148). Segundo autoridades da UE, essa diretiva, em conjunto com a Estratégia de 2013, representam um passo significativo para o bloco enquanto modelo de cibersegurança na Europa, visto que foram as primeiras medidas juridicamente vinculativas sobre a agenda no escopo normativo, no qual o objetivo da NIS é garantir a segurança das redes e dos sistemas de informação (Bederna; Rajnai, 2022). Foi a

partir dessas duas diretrizes que a UE, juntamente com os Estados-membros, passou a lidar com as questões que consideram urgentes na escala da cibersegurança e do ciberespaço.

A NIS é vista como um instrumento importante para a resiliência cibernética da UE, principalmente a segurança cibernética das infraestruturas críticas, porque graças a ela foram estabelecidas obrigações para os Estados-membros, a exemplo da adoção de uma estratégia nacional voltada para a cibersegurança e a indicação de autoridades especializadas na área. Todavia, a diretiva apresentava algumas lacunas em sua estrutura, principalmente nas formas de aplicação das normas. A NIS 1 era considerada limitada, uma vez que se aplicava somente a provedores de alguns serviços, com essa restrição englobando provedores de serviços essenciais que se restringiam ao setor de energia, transporte, bancos infraestruturas do mercado financeiro, saúde, bem como a distribuição de água potável e infraestrutura digital. O que se observou é que a diretiva não considerava a interconexão e a interdependência com outros setores como, por exemplo, o setor de empresas menores na escala da UE (Schmitz-Berndt, 2022).

Outrossim, é possível notar que Bruxelas, ao longo dos anos pós-adoção da Estratégia e da NIS, buscou ampliar a agenda de cibersegurança para além da área de segurança cibernética enquanto campo técnico, incluindo na pauta as esferas sociais e econômicas para elaborar normas mais abrangentes e que alcançassem alguma eficácia (Bederna; Rajnai, 2022). Inicialmente, a questão da cibersegurança na União Europeia tinha um viés puramente econômico, com o intuito de fortalecer o Mercado Único Europeu no âmbito tecnológico, impulsionando o desenvolvimento das economias europeias.

Todavia, a partir do final dos anos 1990, aspectos da securitização passaram a ter uma certa relevância no âmbito da cibersegurança da UE, principalmente por conta da influência de fatores internacionais, a exemplo de iniciativas cibernéticas implementadas pelos Estados Unidos, aliado histórico de Bruxelas (Geraldes, 2019). Dessa forma, a segurança cibernética passou a ser tratada como um campo de política próprio, abordar a insegurança das infraestruturas digitais se tornou mais do que somente uma questão de mercado, estendendo-se até a defesa e a política externa (Cavelty, Smeets, 2023).

Em dezembro de 2022 foi publicada a NIS2, atualização da diretiva anterior, que tem como um dos objetivos estabelecer uma cultura de segurança em todos os setores vitais para a economia e sociedade que dependem das TIC, como energia, transportes, saúde e infraestruturas digitais (Conselho Europeu). Além disso, adicionou ao escopo das infraestruturas críticas atividades ligadas ao espaço, gestão de resíduos, serviços postais, bem como a produção e distribuição de produtos químicos.

Em adição, o Regulamento Geral de Proteção de Dados (GDPR), que entrou em vigor em maio de 2016 e é aplicável desde maio de 2018, é visto como uma das estratégias mais importantes no quadro de instrumentos de segurança cibernética da União Europeia (Bederna, Rajnai, 2022). O regulamento reforça os direitos fundamentais das pessoas no âmbito digital e facilita a atividade comercial, estabelecendo normas aplicáveis às empresas e aos organismos públicos no mercado único digital (União Europeia). Todavia, apesar da sua importância, o regulamento enfrenta algumas barreiras no seu processo de aplicação, nomeadamente a heterogeneidade das leis em torno da segurança cibernética do bloco europeu.

Ademais, após a adoção da Diretiva NIS para a Cibersegurança e com a implementação da Lei Europeia sobre Cibersegurança em 2019, também de chamada de Regulamento (UE) 2019/881, a Agência Europeia para a Segurança das Redes e da Informação (ENISA) ganhou mais espaço na pauta cibernética. Criada em 2004, o órgão tem a função de auxiliar na orientação técnica ao nível da União, mas passou a acumular algumas funções adicionais. Ao órgão, foi delegado a auxiliar os Estados-membros na implementação da diretiva, uma mudança significativa de função, visto que antes limitava-se a segurança cibernética das instituições do bloco. Além disso, a agência também se tornou integrante do Grupo de Cooperação da NIS, no qual fornece consultoria, bem como desempenha o papel de facilitar o compartilhamento de informações entre os Estados-membros (Cavelty, Smeets, 2023).

A ENISA exerce a função de promover a conscientização sobre segurança cibernética, auxiliando no desenvolvimento de expertise através da criação do mês de segurança cibernética e do apoio em exercícios de incidentes cibernéticos (Cavelty, Smeets, 2023). Em adição, a iniciativa de segurança cibernética fornece diversos materiais de cibersegurança para professores, crianças, adolescentes e pais, como por exemplo os primeiros socorros em caso de ataques cibernéticos. A ferramenta está disponível para todos os Estados-membros da UE e oferece medidas práticas para a população em geral reportar os ataques e buscar ajuda nas proximidades (ENISA).

Dessa forma, de acordo com o Regulamento (UE) 2019/881, a cibersegurança não é somente uma questão relacionada à tecnologia, mas também está conectada ao comportamento humano, logo é preciso promover ativamente o processo chamado de ciber higiene. Esse método consiste na adoção de medidas rotineiras que, quando implementadas e aplicadas com regularidade pelos cidadãos, organizações e empresas, minimizam a exposição

de ambos aos riscos provenientes das ciberameaças (Parlamento Europeu; Conselho da União Europeia, 2019).

Todavia, é importante destacar que a agência ainda enfrenta muitos desafios para desenvolver suas atividades e a principal delas é a falta de padronização das políticas cibernéticas entre os Estados-membros, visto que ainda existem diferentes compreensões acerca da agenda cibernética nos principais setores dos países, a exemplo dos ministérios, da inteligência, da ala militar, do setor econômico e do setor digital (Cavelty, Smeets, 2023).

Ademais, a União Europeia também dispõe do Serviço de Cibersegurança para as Instituições, Órgãos e Organismos da União (CERT-UE). Estabelecido em 2011, sua principal função é colaborar com a segurança das infraestruturas de TIC de todas as instituições, órgãos e agências da União. Além disso, representa um procedimento importante na condução da coordenação da troca de informações sobre segurança cibernética, bem como tem a função de responder a incidentes cibernéticos contra organizações protegidas (Bederna, Rajnai, 2022, p. 41).

Apesar dos modelos já adotados pela UE, alguns pesquisadores acreditam que ainda existe uma certa ambiguidade na definição do que se enquadra como uma ameaça cibernética, pois segundo Reisdoefer e Alcântara (2020, p. 172), o bloco possui um conceito amplo e vago de ameaça cibernética, que se concretiza quando seus efeitos impactam o mundo físico. De fato, as normas adotadas até o momento são vistas pela UE como fundamentais para o alcance da resiliência cibernética, entretanto a fragmentação da aplicação dessas diretrizes na escala dos Estados-membros representa um dos maiores desafios dos modelos de segurança cibernética adotados por Bruxelas até o momento. Essa assimetria das políticas entre os países já foi citada por Sliwinski (2014), que considera esse fato como um grande obstáculo para a consolidação das políticas de segurança cibernética do bloco europeu.

As informações sobre a coordenação da segurança cibernética trazem algumas pistas sobre como o discurso securitizador pode ou não estar influenciando a agenda cibernética do bloco europeu. Primeiramente, com base nos argumentos apresentados anteriormente por Lene Hansen e Helen Nissenbaum (2009), desde a implementação da Estratégia da UE para a Cibersegurança em 2013 nota-se uma expansão significativa dos instrumentos normativos da União Europeia no que concerne a agenda cibernética, principalmente através da implementação da NIS e de sua versão mais recente, a NIS 2. Além disso, a expansão das atividades da ENISA também chamou a atenção, todavia ainda é possível notar uma certa cautela por parte de Bruxelas ao tratar do tema. Ou seja, apesar da expansão das normas, não

é possível afirmar com precisão que há uma hiper securitização da segurança cibernética no escopo da União.

No que diz respeito ao segundo conceito, sobre as práticas diárias de segurança (Hansen, Nissenbaum, 2009), percebe-se que muitas dessas práticas foram difundidas através do discurso econômico ao longo dos anos, principalmente através da proteção do Mercado Único Europeu. Entretanto, parece que foi delegada à ENISA a função de propagar essas práticas diárias, visto que o órgão é responsável pela conscientização não somente dos Estados-membros, mas também da população em geral, através da criação do mês da segurança cibernética, do mapeamento e dos relatórios anuais sobre ataques cibernéticos.

Os fatos descritos não são irrefutáveis e dependem de análises mais robustas, porém a expansão normativa e a implementação dessas atividades focais auxiliam a percepção de que a ameaça cibernética está presente no cotidiano do cidadão europeu. Dessa forma, gera o entendimento de que o ciberespaço precisa ser regulamentado, pois se tornou essencial não somente para a economia europeia, mas também para a segurança e integridade física da população em geral.

Além disso, a ENISA também desempenha um papel crucial ao se observar a tecnificação descrita por Hansen e Nissenbaum (2009). Segundo Cavelty e Smeets (2023), a agência foi fortalecida por meio de novos instrumentos e legislação da UE sob o contexto de uma narrativa crescente de que o bloco está bem posicionado para lidar com ameaças transnacionais à segurança cibernética. Essas medidas demonstram que Bruxelas busca fortalecer sua legitimidade através da agência demonstrando para os cidadãos europeus, bem como para a comunidade internacional, que dispõe de técnicos eficientes e capazes de lidar com os desafios impostos pelo ciberespaço e, consequentemente, pela segurança cibernética, que por sua vez passou por uma mudança radical a partir do fim dos anos 1990 (Geraldes, 2019).

Dessa forma, nota-se que já existem medidas que denotam o avanço da securitização no contexto da UE. Na Europa, o caso notório dessa tentativa de securitizar a segurança cibernética ocorreu nos ataques cibernéticos a Estônia em 2007, visto que, segundo Hansen e Nissenbaum (2009) à medida que as manifestações se espalharam das ruas para a internet as autoridades estonianas elevaram o discurso da securitização afirmando que os ataques às redes representavam uma ameaça a soberania estoniana, bem como a identidade cultural do país. Em última instância, as autoridades da Estônia tentaram vincular práticas cotidianas, a exemplo da queda dos serviços essenciais, a questões de segurança individual. Além disso, a capacidade dos estonianos de “vender” o discurso de primeira guerra cibernética no

ciberespaço através das mídias influenciou diretamente no sucesso parcial da securitização cibernética (Hansen, Nissenbaum, 2009).

O caso é notório não somente pela influência que exerceu na legislação da UE, como citado no início do capítulo, mas também pela forma como o bloco se portou durante os ataques. Segundo Hansen e Nissenbaum (2009, p. 1169), apesar da invocação de "guerra", as autoridades estonianas tiveram dificuldades em convencer grandes entidades internacionais, como aliados da OTAN e da União Europeia que, apesar de enviar forças da ENISA ainda assim, segundo Salma e Munabari (2023), optaram por adotar uma postura mais pragmática. É possível observar que a UE ainda mantém uma postura parecida, visto que, apesar da urgência da segurança cibernética, o bloco ainda adota um discurso moderado. Isso pode significar que a securitização vem ocorrendo de maneira gradativa ao longo da última década. Isso também pode ser identificado através do entendimento de figuras proeminentes do bloco.

No dia 5 de setembro de 2021, durante o discurso do Estado da União, Ursula von der Leyen, presidente da Comissão Europeia disse que a União Europeia não deve se contentar em somente responder às ciberameaças, mas deve aspirar a se tornar uma liderança no domínio da segurança cibernética quando se trata da regulamentação e investimentos. A presidente da Comissão Europeia também salientou a necessidade de desenvolver ferramentas de ciberdefesa no continente, bem como a adoção de uma política europeia de ciberdefesa (Estado da União, 2021).

Em complemento, um debate crescente no âmbito da UE se concentra na regulamentação da inteligência artificial e esse debate pode ser crucial para determinar não somente a relevância do bloco no domínio cibernético, mas também na forma como Bruxelas vai se portar no que concerne à cibersegurança nos próximos anos. Em abril de 2021, a Comissão Europeia propôs a primeira lei da UE sobre Inteligência Artificial, estabelecendo um sistema de classificação de IA baseado no risco. Segundo a proposta, os sistemas de Inteligência Artificial, que podem ser aplicados em diferentes domínios, são analisados e classificados conforme o risco que representam para quem utilizá-los (Parlamento Europeu).

4 REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA UE

4.1 A Estratégia da UE para a Inteligência Artificial

Com base em dados da Organização para a Cooperação e Desenvolvimento Econômico (OECD), Jobin et al. (2019) destaca que nos últimos anos diversos Estados e organizações estão se articulando para implementar medidas normativas que possam lidar com a crescente presença da inteligência artificial no cotidiano da grande maioria das pessoas ao redor do mundo. Essa articulação é decorrente dos medos e da insegurança que cerca o tema, dada a elevada capacidade da ferramenta para causar danos no tecido social. É inegável que a IA traz, sim, inúmeros benefícios nos mais variados domínios sociais, todavia também desencadeou um amplo debate sobre princípios e valores que devem orientar seu desenvolvimento (Jobin et al., 2019, p. 3). Algumas dessas questões incluem o medo de que a IA coloque em risco empregos, que seja utilizada por atores prejudicialmente, bem como possa disseminar preconceitos e minar o sistema de justiça.

Em adição, de acordo com Igna Ulnicane (2022), o uso da IA nas áreas de educação, transporte e até no domínio militar pode gerar benefícios sociais, econômicos, bem como preocupações sobre o seu impacto problemático na democracia e nas áreas citadas anteriormente. É neste quadro que a União Europeia vem discutindo ativamente maneiras para facilitar o desenvolvimento e o uso da inteligência artificial nas suas instituições e Estados-membros. O bloco europeu estabeleceu como prioridade nesta agenda trabalhar no tipo e na forma que gostaria de desenvolver e contribuir para o desenvolvimento da IA em nível global, visto que Bruxelas entende que está sendo deixada para trás por grandes potências como Estados Unidos e China (Ulnicane, 2022). Em complemento, um relatório elaborado pela Mckinsey & Company para a Cúpula Digital de Chefes de Estado da UE em Tallinn em setembro de 2017 apontou que a UE tem dado passos pequenos em termos de investimento em IA. Segundo os dados apresentados, a América do Norte investiu em 2016 entre 15 e 23 bilhões de dólares em IA, enquanto a Ásia, entre 8 e 12 bilhões. Já a Europa investiu, cerca de 4 bilhões no total (Mckinsey & Company, 2017).

Segundo Ulnicane (2022), a agenda de IA no âmbito da UE é relativamente recente, entretanto as preocupações acerca do maior bloco econômico do mundo ficar atrás dos Estados Unidos e de países da Ásia no campo da ciência, tecnologia e inovação se tornaram um propulsor para a integração europeia no que concerne aos esforços para investir em pesquisa e tecnologia desde seus estágios iniciais na década de 1950. Dessa forma, a União Europeia desenvolve suas atividades com base em dois conceitos. O primeiro conceito é o Normative Power Europe, no qual o bloco ressalta a importância de difundir suas normas,

que foram firmadas mediante declarações, tratados e políticas. O segundo conceito é o de Market Power Europe, fundamentado no preceito de que, embora o bloco europeu possa ter características normativas, ainda assim é fundamentalmente um grande mercado comum. Ademais, na Estratégia de 2018 a UE define Inteligência Artificial da seguinte forma:

> A inteligência artificial refere-se a sistemas que exibem comportamento inteligente analisando seu ambiente e tomando ações – com algum grau de autonomia – para atingir objetivos específicos. Os sistemas baseados em IA podem ser puramente baseados em software, atuando no mundo virtual (assistentes de voz, software de análise de imagem, mecanismos de pesquisa, sistemas de reconhecimento de fala e rosto) ou a IA pode ser incorporada em dispositivos de hardware (Comissão Europeia, 2018).

Essa definição passou por algumas atualizações ao longo dos anos seguintes, a exemplo da adição da IA como um conjunto de técnicas que incluem o aprendizado de e o raciocínio de máquinas além de robótica (Comissão Europeia, 2019). Outrossim, as descrições da IA em documentos das políticas da UE demonstram altas expectativas em relação a ferramentas, descrevendo-a como uma tecnologia transformadora com impactos abrangentes (Ulnicane, 2022, p. 256). Além disso, Bruxelas já considera o setor de inteligência artificial como uma das indústrias mais importantes do século XXI, sendo equiparada aos impactos da máquina à vapor e da eletricidade. Dessa forma, segundo Ulnicane (2022), a maneira como abordamos a IA definirá o mundo em que vivemos, logo, em meio a feroz competição global, uma sólida estrutura europeia é necessária.

Ainda no âmbito da Estratégia para a IA, a União Europeia lista os benefícios e as urgências advindas da ferramenta. Segundo o bloco, o uso da inteligência artificial será essencial para melhorar os cuidados de saúde, aumentar a eficiência da agricultura, bem como contribuir para mitigar e adaptar questões acerca das mudanças climáticas através da melhoria e da eficiência dos sistemas de produção por meio de manutenção preditiva. Em complemento, o documento ainda deixa claro que o uso da IA será essencial para aumentar a segurança dos europeus. Além disso, a Estratégia reafirma o desejo da UE em se tornar uma liderança global quando se trata do tema. Segundo o documento, a União Europeia pode liderar o caminho no desenvolvimento e uso da IA para o bem e para todos (Comissão Europeia, 2018).

Não obstante, a Estratégia tem três eixos principais como base, que segundo Inga Ulnicane (2022) se tornaram os pilares da política de IA da União Europeia. O primeiro busca impulsionar a capacidade tecnológica e industrial da UE e a implementação da Inteligência Artificial em toda a economia, no setor privado, bem como no setor público. Sob

esse entendimento, o bloco estabeleceu uma meta para investimentos conjuntos entre Bruxelas e os Estados-membros, na qual definiu investimentos de 20 bilhões de euros por ano no setor de IA (Comissão Europeia). O segundo eixo da Estratégia visa criar mecanismos para lidar com as mudanças socioeconômicas impostas pelo uso da IA. As ações para esse objetivo incluem a modernização dos sistemas de educação e treinamento, antecipando mudanças no mercado de trabalho, apoiando transições no mercado de trabalho e auxiliando na adaptação de sistemas de proteção social. Em adição, o terceiro eixo estabelece a necessidade de garantir uma estrutura ética e legal apropriada que seja baseada nos valores da UE, obedecendo a Carta dos Direitos Fundamentais (Comissão Europeia).

4.2 O Livro Branco da União Europeia sobre IA

Outrossim, em fevereiro de 2020, a União Europeia lançou o Livro Branco do bloco sobre Inteligência Artificial. Nele a UE reafirma grande parte dos objetivos traçados pela Estratégia, adicionando novos pontos e complementando outros. De início, o documento já destaca que não irá se aprofundar no debate acerca do uso militar da IA no contexto europeu e, segundo especialistas envolvidos na elaboração do documento, esse foi um dos erros cometidos pela UE. As críticas apontam que omitir sistemas de armas autônomas letais do Livro Branco prejudica o debate acerca do tema, visto que na época a UE já havia começado a trabalhar na investigação acerca do uso da Inteligência Artificial no domínio de defesa. Dessa forma, excluir o tópico do documento para consulta pública foi entendido como uma atitude questionável advinda da Comissão Europeia (Ulnicane, 2022).

Em complemento, o Livro Branco elenca os benefícios da Inteligência Artificial para os europeus. O documento enfatiza que a regulamentação da IA serve para os cidadãos colherem novos benefícios como, por exemplo, a melhoria dos cuidados de saúde, menos avarias nos eletrodomésticos, sistemas de transporte mais seguros e menos poluentes e melhores serviços públicos. Além disso, argumenta que a ferramenta será útil para o desenvolvimento das empresas na geração de produtos em áreas que são a força do bloco, como máquinas, transportes, segurança cibernética, agricultura e economia verde e circular. O outro ponto que chama a atenção e a melhoria dos serviços de interesse público, como educação e energia, segundo o documento a UE tornar-se líder mundial na inovação irá melhorar a sustentabilidade dos produtos e deixará as autoridades responsáveis pela aplicação da lei mais bem equipadas com os instrumentos necessários para garantir a proteção dos cidadãos (Comissão Europeia, 2020).

Não obstante, o documento do bloco enfatiza que o uso e a devida regulamentação da IA vão impactar diretamente em domínios mais amplos, visto que IA não deve ser interpretada por uma perspectiva individual, mas também coletivamente na sociedade. Dessa forma, o documento chama a atenção por destacar temas que são considerados essenciais para a integração europeia, bem como para alavancar o protagonismo mundial do bloco. Segundo o Livro Branco, o uso da IA deve desempenhar um papel crucial para o alcance dos Objetivos de Desenvolvimento Sustentável da ONU (ODS), bem como para o processo democrático e para a preservação dos direitos sociais. Além disso, deve ter reflexos no Pacto Ecológico Europeu, auxiliando nos desafios climáticos e ambientais. Segundo o documento, as tecnologias digitais, como a IA, são um fator crítico para concretizar os objetivos do Pacto Ecológico (Comissão Europeia, 2020). Dessa forma, o documento está fundamentado nos direitos fundamentais, nos valores e na ética (Ulnicane, 2022).

4.3 O Regulamento sobre Inteligência Artificial

O regulamento de Inteligência Artificial da UE visa assegurar que os sistemas de IA sejam desenvolvidos e utilizados de forma responsável. Além disso, a norma impõe obrigações aos fornecedores e aos responsáveis por implementar as tecnologias referentes a esta agenda, regulando a utilização de sistemas de inteligência artificial no mercado único do bloco europeu. Ademais, o Regulamento de Inteligência Artificial da UE se destaca por ser o primeiro ato legislativo do mundo em matéria de IA, reforçando novamente as aspirações de liderança de Bruxelas nesta agenda ao se tornar uma referência mundial na regulamentação da IA (Conselho Europeu).

Em complemento, o regulamento enfatiza que o uso da inteligência artificial nos mais diversos setores já é uma realidade entre os Estados-membros do bloco, incluindo o setor econômico e até o setor transfronteiriço. O documento também destaca que alguns países da UE já exploram a adoção de normas nacionais para garantir que a IA seja confiável e segura, para assim garantir o uso da ferramenta conforme as obrigações dos direitos fundamentais. Todavia, segundo o Regulamento, regras nacionais diferentes podem levar à fragmentação do mercado interno e diminuir a segurança jurídica para os operadores que desenvolvem, importam ou usam sistemas de IA (Conselho da União Europeia).

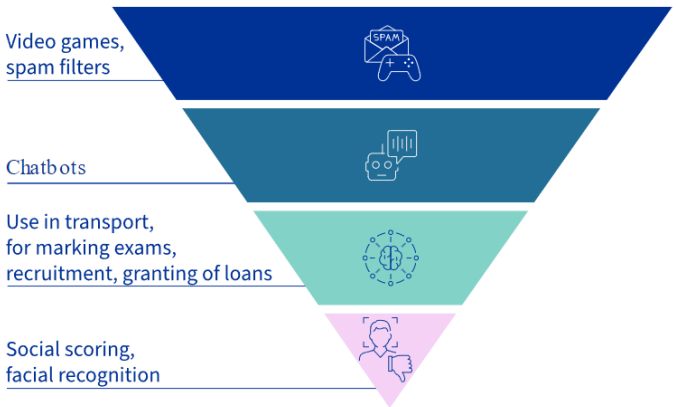
Sendo assim, o documento estabelece que é preciso assegurar um nível de proteção elevado e consistente em todo o bloco, estabelecendo obrigações uniformes para os operadores, bem como para questões cruciais que sejam de interesse público com o intuito de proteger o direito das pessoas em todo o mercado interno, considerando o artigo 114 do

Tratado sobre o Funcionamento da União Europeia. Conforme o regulamento, são definidas como questões de interesse público pautas que alcancem a saúde, a segurança e os direitos fundamentais dos cidadãos europeus (Conselho da União Europeia).

Não obstante, o documento enfatiza que a segurança cibernética desempenha um papel crucial para garantir que os sistemas de IA sejam resilientes contra tentativas de alterar seu uso, comportamento, desempenho ou comprometer suas propriedades de segurança contra terceiros com interesses escusos. Outrossim, ataques cibernéticos contra sistemas conseguem danificar capacidades específicas dos sistemas de IA, a exemplo do conjunto de dados de treinamento ou modelos treinados, provocando também danos nas infraestruturas das TIC. Em adição, o Regulamento também eleva as atribuições da ENISA, destacando que a agência tem uma elevada experiência no que tange à política de cibersegurança, como já observado no capítulo II desta pesquisa. Dessa forma, estabelece que a Comissão Europeia deve cooperar com a agência em questões relacionadas com a cibersegurança dos sistemas de IA (Conselho da União Europeia).

Dessa maneira, o Regulamento da UE para a Inteligência artificial entrou em vigor no dia 01 de agosto de 2024. Como citado ao final do capítulo anterior, o Regulamento estabelece quatro níveis de risco no que concerne ao uso da IA, os quais estão listados na figura a seguir:

Figura 1: Pirâmide de Riscos



Fonte: Conselho Europeu

O primeiro nível dos riscos - que engloba videogames e filtros de spam- representa um nível prejudicial mínimo, visto que não são regulamentados e também não são afetados diretamente pelo regulamento implementado pela UE. O nível dois da figura destaca o risco limitado, que atinge robôs de conversação, bem como sistemas de IA que geram conteúdos.

Segundo o documento, ferramentas de IA que se enquadrem nessas descrições estão sujeitas às obrigações de transparência. O nível de risco elevado no uso de IA corresponde às ferramentas utilizadas em diagnósticos de doenças, condução autônoma de veículos de transporte e identificação biométrica de pessoas envolvidas em atividades criminosas e segundo o regulamento deve cumprir requisitos e obrigações rigorosas para conseguirem acesso ao mercado do bloco (Conselho Europeu).

Em complemento, o quarto bloco da pirâmide refere-se ao risco inaceitável. Esse nível corresponde principalmente aos sistemas de inteligência artificial que ameacem a segurança, os direitos ou os meios necessários para a sobrevivência das pessoas. Ademais, esses sistemas estão terminantemente proibidos caso sejam utilizados para manipular comportamentos e nos estabelecimentos de ensino. Além disso, esse nível também proíbe o uso de sistemas de identificação biométrica em tempo real, como reconhecimento facial em espaços públicos, com algumas exceções (Conselho Europeu). O regulamento também estabelece os riscos dos modelos de IA para o uso geral. O documento lista que será passível de sanções qualquer ferramenta de IA que represente riscos sistêmicos negativos reais ou razoavelmente previsíveis com consequências graves para a saúde e segurança pública, bem como para o processo democraticos e segurança econômica do bloco.

Ademais, no primeiro relatório sobre o estado da segurança cibernética na União Europeia, a ENISA identificou o uso imprudente da inteligência artificial como uma das maiores ciberameaças ao bloco até 2030. Vale mencionar, que a IA aparece ao lado de ameaças como o aumento acentuado da vigilância digital e perda de privacidade, elevação da desinformação e operações com o intuito de influenciar campanhas eleitorais, aumento das ameaças híbridas, bem como o impacto físico, no meio ambiente e nas infraestruturas críticas digitais (ENISA). Dessa forma, o relatório da principal agência de segurança cibernética do bloco reafirma que a cibersegurança está intrinsecamente conectada ao uso da inteligência artificial, visto que ambos impactam diretamente os mais diversos setores da sociedade.

No capítulo anterior verificou-se que o discurso securitizador surgiu de forma gradativa durante o processo de formulação do arcabouço normativo da segurança cibernética da UE, com a adoção da Estratégia da UE para a cibersegurança, as diretivas NIS e a expansão das atividades da ENISA. Este capítulo traz algumas informações complementares interessantes. Primeiro, a Inteligência Artificial se tornou vital para a UE ao se observar as as as aspirações do bloco acerca de se tornar uma referência normativa global. Além disso, nota-se que o discurso ganhou tons mais urgentes visto que, tanto o Livro Branco quanto o Regulamento de Inteligência citam a regulamentação da IA como fator essencial para garantir

a segurança dos cidadãos europeus. O Livro Branco ainda cita que o bom uso da IA será de extrema importância para que a UE alcance os objetivos estabelecidos no Pacto Ecológico Europeu. Além disso, é possível notar uma ligação intrínseca entre cibersegurança e o uso e regulamentação da IA, visto que a cibersegurança é fator crucial para garantir o funcionamento das ferramentas de inteligência artificial

CONSIDERAÇÕES FINAIS

O presente trabalho buscou responder a seguinte pergunta: quais são as principais normas e regulamentos de segurança cibernética de que a União Europeia dispõe para proteger suas instituições, bem como os Estados-membros? Para tal, foi dado um contexto histórico de conjunturas críticas no continente europeu que influenciaram direta e indiretamente o arcabouço normativo do bloco. Além disso, foi feita uma análise descritiva das estratégias, regulamentos e diretivas que a UE já adicionou ao seu quadro normativo entre 2013 e 2024. Em adição, buscou-se ainda demonstrar a influência do surgimento da Inteligência Artificial e seus impactos no arcabouço jurídico da UE, bem como na segurança cibernética.

Ademais, as discussões conceituais, bem como as interpretações referentes ao campo de segurança cibernética foram fundamentadas através da perspectiva da securitização, tendo como base autoras como Lene Hansen e Helen Nissenbaum a partir da teoria da securitização de Buzan et al (1998). O uso do conceito foi essencial, visto que o debate sobre segurança cibernética e inteligência artificial está cada vez mais presente nos estudos sobre segurança internacional e atingem diretamente os mais diversos setores da sociedade, como o setor político, econômico, de segurança pública e meio ambiente.

Primeiramente, a partir da análise dos ataques sofridos pela Estônia e pela Geórgia em 2007 e 2008 respectivamente, constatou-se que a segurança cibernética tem a capacidade de transformar de forma radical o quadro normativo interno dos Estados. No caso da Estônia essa transformação ocorreu em menor grau, visto que o país já era uma referência em digitalização e segurança, todavia os estonianos transformaram o acontecimento em uma questão de existência e preservação de identidade, se enquadrando parcialmente nos conceitos de securitização descritos por Hansen e Nissenbaum (2009). No caso da Geórgia, as mudanças ocorreram de forma mais abrangente, no qual a segurança cibernética se tornou uma questão de segurança nacional, resultando na criação da Lei de Crime Cibernético e do Departamento de Segurança Cibernética. Dessa forma, com base no que diz Hansen e Nissenbaum (2009) houve uma tecnificação da segurança cibernética na Geórgia após os ataques de 2008.

Ademais, verificou-se que os ataques, principalmente os ocorridos na Estônia, tiveram influência direta nos debates jurídicos acerca do ciberespaço, isso é evidenciado pela criação do Manual de Tallinn e do CCDCOE, que facilitou a cooperação internacional no que tange o domínio cibernético. O fato também desempenhou um papel importante na articulação normativa da segurança cibernética da União Europeia. Todavia, com o que foi analisado na

pesquisa, o discurso existencial difundido pela Estônia, principalmente com relação à Rússia para se referir ao ocorrido, teve pouco impacto nas decisões da UE.

Outrossim, ao examinar o arcabouço normativo da União constatou-se que o bloco ainda mantém um discurso moderado – ainda que ambíguo – em relação à segurança cibernética, priorizando a segurança das instituições e da população através da preservação dos direitos fundamentais no domínio do ciberespaço. Em relação a securitização e segurança cibernética nota-se uma certa cautela da UE nesta abordagem, mas alguns alentos securitizadores já são identificados, principalmente nas atividades e atribuições de sua principal agência para a cibersegurança, a ENISA. A agência desempenha um papel ativo na adoção de medidas rotineiras na sociedade no que tange à cibersegurança.

Já no que concerne a regulamentação da inteligência artificial, nota-se que a UE adota um discurso mais enérgico, considerando que as normas e o bom uso da IA são essenciais para o alcance da liderança global do bloco, para a segurança pública e integridade física dos cidadãos, para a saúde e para o alcance dos objetivos audaciosos sobre mudanças climáticas. Dessa forma, a UE já transforma atividades consideradas corriqueiras em cenários críticos através do Regulamento para a Inteligência Artificial.

Diante do exposto, conclui-se que a União Europeia avançou significativamente na regulamentação da cibersegurança. Além disso, constatou-se que a necessidade de constante atualização normativa e o aprimoramento da cooperação internacional são fundamentais para mitigar os riscos emergentes e assegurar a estabilidade do espaço cibernético europeu. Dessa forma, a pesquisa contribui para o entendimento do papel da UE na construção de um modelo normativo de cibersegurança e abre caminhos para futuras pesquisas sobre a evolução das políticas cibernéticas e seu impacto na segurança global.

REFERÊNCIAS BIBLIOGRÁFICAS

AAVIKSOO, Jaak. Cyberattacks against Estonia raised awareness of cyberthreats. **Defense Against Terrorism Review**, v. 3, n. 2, p. 13-22. Disponível em: https://www.tmmm.tsk.tr/publication/datr/volumes/datr6.pdf.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. **Security: a new framework for analysis.** Estados Unidos da América, Lynne Rienner Publichers, 1998.

BEDERNA, Zsolt; RAJNAI, Zoltan. Analysis of the cybersecurity ecosystem in the European Union. **International Cybersecurity Law Review**, v. 3, n. 1, p. 35–49, 2022. Disponível em: https://link.springer.com/article/10.1365/s43439-022-00048-9.

CCDCOE. **Our mission & vision**. Disponível em: https://CCDCOE.org/about-us/.

CCDCOE. **The Tallinn Manual**. Disponível em: https://CCDCOE.org/research/tallinn-manual/.

CARVALHO, Antonio Augusto Ramos. Ciberespaço e os novos desafios à soberania e à segurança dos Estados. **IDN Cadernos.** Disponível em: https://www.idn.gov.pt/pt/publicacoes/idncadernos/Documents/Texto%20integral/idncadernos_36.pdf.

CHAVES, Daniel; SCHURSTER, Karl. Soberania nacional no pós-Guerra Fria: a Ossétia do Sul em questão. **Revista Intellector,** v. 5, n. 10, p. 1-10, Rio de Janeiro, 2009. Disponível em: https://biblat.unam.mx/pt/revista/intellector/articulo/soberania-nacional-no-pos-guerra-fria-a-ossetia-do-sul.

CAVELTY Myriam Dunn; WENGER, Andreas. Cyber security meets security politics: complex technology, fragmented politics, and networked science. **Contemporary Security Policy**, v. 41, n. 1, p. 5-32. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855.

CAVELTY Myriam Dunn; SMEETS, Max. Regulatory cybersecurity governance in the making: the formation of ENISA and the struggle for epistemic authority. **Journal of European Public Policy.** Disponível em: https://www.tandfonline.com/doi/full/10.1080/13501763.2023.2173274.

CONSELHO EUROPEU. **Como está a UE a reforçar a sua cibersegurança**. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/.

COMISSÃO EUROPEIA. **Primeiro relatório intercalar sobre a Estratégia da UE para a União da Segurança.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020DC0797.

CONSELHO EUROPEU. **Regulamento Inteligência Artificial**. Disponível: https://www.consilium.europa.eu/pt/policies/artificial-intelligence/.

DE SOUZA, Leonardo Rafael; FREITAS, Cinthia Obladen de Almendra. A construção da cibersoberania na União Europeia: a cibersegurança e a integração do ciberespaço europeu. **Revista de Direito Internacional**. v. 19, n. 3, p. 256-270, dez. 2022. Disponível em: https://core.ac.uk/download/568035873.pdf.

DIRECTIVE (EU) 2022/2555 of the European Parliament and of The Council of 14 december 2022. **Official Journal of the European Union.** Disponível em: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

ENISA. **What we do.** Disponível em: https://www-enisa-europa-eu.translate.goog/about-enisa/what-we-do?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc.

ENISA. **Cyber Hygiene.** Disponível em: https://www.enisa.europa.eu/topics/cyber-hygiene.

ENISA. 2024 Report on the state of cybersecurity in the union. Disponível em: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

EUROPEAN PARLIAMENT. **Estratégia da UE para a Cibersegurança**. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_PT.pdf?redirect.

EUROPEAN COMMISSION. **White Paper on Artificial Intelligence: a European approach to excellence and trust**. 2020. Disponível em: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

EUROPEAN COMMISSION. **Artificial Intelligence for Europe**. 2018. Disponível em:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018DC0237.

EUROPEAN COMMISSION. **European approach to artificial intelligence.** Disponível em: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

EUROPEAN COMMISSION. **Legal framework of EU data protection.** Disponível em: https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en.

FUSTER, Gloria Gonzalez; JASMONTAITE, Lina. Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. In: CHRISTEN, Markus; GORDIJN,

Bert; LOI, Michele. The Ethics of Cybersecurity. **Springer Open**, 2020. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-29053-5_5.

GERALDES, Sofia Martins. A estratégia de cibersegurança da União Europeia: catastrofista, realista e/ou otimista?. **Nação e Defesa.** n. 154, p. 91-108, 2019. Disponível em: https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD154/NeDef154_Abstract_SofiaMartinsGeraldes.pdf.

HANSEN, Lene; NISSENBAUM, Helen. Digital disaster, cyber security, and the Copenhagen School. **International Studies Quarterly**, v. 53, p. 1155-1175, 2009. Disponível em:https://nissenbaum.tech.cornell.edu/papers/Digital%20Disaster.pdf.

JOBIN, Anna, IENCA Marcello, VAYENA, Effy. The global landscape of AI ethics guidelines. **Nature Machine Intelligence**. v. 1, p. 389–399, 2019. Disponível em: https://www.nature.com/articles/s42256-019-0088-2.

KOZLOWSKI, Andrzej. Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. **International Scientific Forum**. v. 3, p. 237-245, 2014. Disponível em: https://test.eujournal.org/index.php/esj/article/view/2941.

KIANPOUR, Mazaher; RAZA, Shahid. More than malware: unmasking the hidden risk of cybersecurity regulations. **International Cybersecurity Law Review**. n. 5, p. 169-212. Disponível em: https://link.springer.com/article/10.1365/s43439-024-00111-7.

MIELNICZUK, Fabiano. O conflito entre Rússia e Geórgia: uma revisão histórica. **Estudos Internacionais.** v. 1, n. 2, p. 157-166, 2013. Disponível em: https://periodicos.pucminas.br/estudosinternacionais/article/download/6311/5790/24071.

MANYIKA, James. 10 imperatives for Europe in the age of IA and automation. **McKinsey & Company**, 02. out. 2017. Disponível em: https://www.mckinsey.com/featured-insights/europe/ten-imperatives-for-europe-in-the-age-of-ai-and-automation .

NATO. **Collective defence and article 5**. 2023. Disponível em: https://www.nato.int/cps/en/natohq/topics_110496.htm.

NATO. NATO Centres of Excellence – Cooperative Cyber Defence (CCDCOE). Disponível em:https://www.act.nato.int/article/nato-centres-of-excellence-cooperative-cyber-defence-ccd-coe/

NAPETVARIDZE, Vladimeri; CHOCHIA, Archil. Cybersecurity in the making - policy and law: a case study of Georgia. **Sciendo**, v. 19, n. 2, p. 155-180, 2019. Disponível em: https://sciendo.com/pdf/10.2478/iclr-2019-0019.

PERNIK, Piret. The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. In: POPESCU, Nicu; SECRIERU, Stanislav. Hacks, leaks and disruptions. **European Union Institute for Security Studies,** 2018. Disponível em: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

PARLAMENTO EUROPEU. **Lei da UE sobre IA: primeira regulamentação de inteligência artificial**. Disponível em: https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial.

REISDOERFER, Bruna Rohr; ALCÂNTARA, Bruno Toso. Alemanha como Líder na Determinação de Ameaças Cibernéticas na União Europeia? **Carta Internacional**, Belo Horizonte, v. 15, n. 2, p. 163-189, 2020. Disponível em: https://www.cartainternacional.abri.org.br/Carta/article/view/1063/786.

RAMOS, Hugo. Ciberguerra: Apropriação da tecnologia hoje, hegemonia das nações amanhã. **Instituto Universitário de Lisboa**.
REGULAMENTO(UE) 2019/881 do Parlamento Europeu e do Conselho. Jornal Oficial da União Europeia. Disponível em: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

SCHMITT. Michael N. The Tallinn Manual on The International Law Applicable to Cyber Warfare. **Cambridge University Press**. Disponível em:https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE.

SCHMITT, Michael N. Tallinn Manual 2.0 on The International Applicable to Cyber Operations. **Cambridge University Press.** Disponível em: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

SLIWINSKI, K. F. Moving beyond the European union's weakness as a cyber-security agent. **Contemporary Security Policy**, v. 35, n. 3, p. 468–486, 2014. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13523260.2014.959261.

SAVAŞ, Serkan; KARATAŞ, Suleyman. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. **Cybersecurity Law Review** , v. 3, p. 7-34, 2022. Disponível em:https://link.springer.com/article/10.1365/s43439-021-00045-4.

SALMA, Dita Aulia; MUNABARI, Fahlesa. Blockchain Technology: cyber security strategy in post-2007 cyber-attacks Estônia. **Deviance Jurnal Kriminologi**, v. 7, n. 1, p. 32-45, 2023. Disponível em: https://journal.budiluhur.ac.id/index.php/deviance/article/view/2412.

SCHMITZ-BERNDT, Sandra; CHIARA, Pier Giorgio. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS 2 directive. **International**

Cybersecurity Law Review, Itália, ed. 3, p. 289-311, 20 jul. 2022. Disponível em: https://link.springer.com/article/10.1365/s43439-022-00058-7.

TOAL, Gerard; O'LOUGHLIN, John. Inside South Ossetia: a survey of attitudes in a de facto state. Post-Soviet Affairs, v. 29, n. 2, p. 136-172. Disponível em: https://www.tandfonline.com/doi/full/10.1080/1060586X.2013.780417.

TRAYNOR, Ian. Russia accused of unleashing cyberwar to disable Estonia. **The Guardian**. Disponível: https://www.theguardian.com/world/2007/may/17/topstories3.russia.

ULNICANE, Inga. Artificial intelligence in the European Union: policy, ethics and regulation. **Routledge,** 2021. Disponível em:https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9780429262081-19/artificial-intelligence-european-union-inga-ulnicane.

VON DER LEYEN, Ursula. **Discurso do Estado da União. Comissão Europeia.** set. 2021 Disponível em: https://state-of-the-union.ec.europa.eu/state-union-2021_pt..

ZAHRA, Iradhati; HANDAYANI, Irawati; CHRISTIANTI, Diajeng Wulan. Cyber-attack in Estonia: a new challenge in the applicability of international humanitarian law. **Yustitia Jurnal Hukum**, v. 100, n. 1, p. 48-66, 2021. Disponível em: https://jurnal.uns.ac.id/yustisia/article/view/48336.