INSTITUTO SUPERIOR DE CIÊNCIAS SOCIAIS E POLÍTICAS
UNIVERSIDADE DE LISBOA

U LISBOA | UNIVERSIDADE DE LISBOA

O Ciberespaço no Conceito atual de Estratégia de Segurança Nacional da Rússia

Diogo André Sá Marques Ladeira

Orientador: Prof. Doutor Marcos Farias Ferreira

Dissertação para obtenção de grau de Mestre em Estratégia

Lisboa
2024

Folha de Rosto

O Ciberespaço no Conceito atual de Estratégia de Segurança Nacional da Rússia

Diogo André Sá Marques Ladeira

Orientador: Prof. Doutor Marcos Farias Ferreira

Dissertação para obtenção de grau de Mestre em Estratégia

Júri:

Presidente:
- Doutora Sandra Maria Rodrigues Balão, Professora Associada do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa;

Vogais:
- Doutora Maria João Militão Ferreira de Sousa Pereira, Professora Associada com Agregação do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa;
- Doutor Marcos Farias Ferreira, Professor Auxiliar com Agregação do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa, na qualidade de Orientador;
- Doutor Luís Eduardo Matos Dias Ramos, Professor Auxiliar Convidado do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa.

Lisboa
2024

Agradecimentos

À minha família pela paciência e pelo apoio que me deram durante esta etapa. Em especial quero agradecer aos meus pais que sempre tentaram dar-me as melhores condições para estudar e sempre acreditaram nas minhas capacidades, mesmo quando tinha notas menos positivas.

Aos meus amigos pelo incentivo que me deram neste processo, principalmente nos momentos mais difíceis e de maior dúvida. Todos os meus amigos tiveram relevo em conseguir o sucesso final, mas quero destacar a Catarina pela insistência e a Covaci pelos inúmeros debates sobre a dissertação.

Ao Professor Doutor Marcos Farias Ferreira por ter aceitado ser o meu orientador. A orientação do Prof. Marcos foi essencial para precisar o tema e o desenvolvimento da dissertação. Eu não fui o aluno mais fácil ou comunicador, mas o Prof. Marcos esteve sempre disponível para ajudar e discutir ideias que enriqueceram o trabalho final.

Ao ISCSP, especialmente aos Professores do mestrado em Estratégia, pela oportunidade de estudar esta área fascinante. A fase curricular do mestrado foi fundamental para desenvolver esta dissertação, seja pelas aulas lecionadas pelos Professores, e os debates entre colegas, como pelos trabalhos desenvolvidos no âmbito de cada unidade curricular.

Muito Obrigado!

Resumo

A presente dissertação desenvolvida no contexto do mestrado em Estratégia pretende analisar o ciberespaço, um novo espaço estratégico, e compreender que papel tem na Estratégia de Segurança Nacional da Rússia, uma potência em que procura estabelecer-se novamente como uma superpotência.

O objetivo principal da dissertação é responder à pergunta "que importância tem o ciberespaço no Conceito atual de Estratégia de Segurança Nacional da Rússia?", assim como analisar a evolução do ciberespaço enquanto espaço estratégico, contextualizar a cultura estratégica da Rússia e compreender a evolução da preponderância do ciberespaço em documentos estratégicos russos ao longo do tempo.

A investigação parte de um método dedutivo, focando-se na análise de documentos oficiais de estratégia russos, em especial o *Conceito de Segurança Nacional da Rússia* de 2021, a partir de uma ontologia construtivista e epistemologia interpretativa. Neste ponto destaca-se a Escola de Copenhaga, nomeadamente *Security: A new framework for analysis* (1998) de Buzan, Wæver e & De Wilde, mas especialmente *Digital disaster, cyber security, and the Copenhagen School* (2009) de Hansen e Nissenbaum. Para estabelecer bases teóricas recorreu-se à *Teoria Geral da Estratégia: o essencial ao processo estratégico* (2009), do Professor António Silva Ribeiro do ISCSP. Na análise da cultura estratégica destacam-se o Professor Heitor Romana do ISCSP, e na Universidade de Copenhaga, Götz e Staun (2022).

A dissertação conclui que o ciberespaço é uma prioridade estratégica, hipersecuritizada, no conceito atual de Estratégia de Segurança Nacional da Rússia, mas nem sempre foi assim. Este espaço começou por ser um espaço científico, para troca de conhecimento entre universidades, e evoluiu para um espaço securitizado, principalmente após os ciberataques à Estónia em 2007. A cultura estratégica russa é definida pelo sentimento de vulnerabilidade, motivado por fatores "geohistóricos", e pela obsessão de ser uma superpotência, ambos refletidos no ciberespaço.

Palavras-chave: Ciberespaço, Segurança Nacional, Estratégia, Rússia, Cultura Estratégica

Abstract

This dissertation developed in the context of a master's degree in Strategy, aims to analyse cyberspace, a new strategic space, and understand what role it plays in the National Security Strategy of Russia, a nation seeking to re-establish itself as a superpower.

The main objective of the dissertation is to answer the question 'what importance does cyberspace have in Russia's current Concept of National Security Strategy?'. The secondary goals consist of analysing the evolution of cyberspace as a strategic space, contextualizing Russia's strategic culture, and understanding the evolution of the prominence of cyberspace in Russian strategic documents over time.

The research is based on a deductive method, focusing on the analysis of official Russian strategic documents, particularly the *Russian National Security Concept* of 2021, from a constructivist ontology and interpretivist epistemology. Here emphasis is placed on the Copenhagen School, namely *Security: A new framework for analysis* (1998) by Buzan, Wæver and & De Wilde, but especially *Digital disaster, cyber security, and the Copenhagen School* (2009) by Hansen & Nissenbaum. *Teoria Geral da Estratégia: o essencial ao processo estratégico* (2009), by Professor António Silva Ribeiro from ISCSP, was another important theoretical foundation. Professor Heitor Romana from ISCSP, and Götz & Staun (2022) from the University of Copenhagen stand out when analysing strategic culture.

The dissertation concludes that cyberspace is a hyper-securitised strategic priority in Russia's current Concept of National Security Strategy, but this was not always the case. This space began as a scientific space, for the exchange of knowledge between universities, and evolved into a securitised space, especially after the cyberattacks on Estonia in 2007. Russia's strategic culture is defined by a sense of vulnerability, motivated by 'geohistorical' factors, and an obsession with being a superpower, both of which are reflected in cyberspace

Keywords: Cyberspace, National Security, Strategy, Russia, Strategic Culture

Índice

Introdução **1**

Ontologia e Epistemologia 4

A Escola de Copenhaga e o Ciberespaço 5

Enquadramento Teórico 10

Opções Metodológicas 16

Capítulo I. O Ciberespaço **19**

A História da Internet 19

Quadro Legal Internacional 24

Capítulo II. A Cultura Estratégica da Rússia **32**

As linhas culturais estraégicas da Rússia 32

Cultura Estratégica no Ciberespaço 35

Capítulo III. O Conceito de Estratégia de Segurança Nacional da Rússia **38**

A evolução do Conceito de Segurança Nacional e da Doutrina de Segurança das Informações 38

O Conceito atual de Estratégia de Segurança Nacional 57

Conclusão **63**

Referências Bibliográficas **68**

Lista de Figuras

Figura 1. Diagramas originais da ARPANET de setembro e dezembro de 1969 19
Figura 2. O mapa da Arpanet em 1977 20
Figura 3. Tráfego de Informação na USENET em 1993 23
Figura 4. Ataques DDoS 26
Figura 5. As diferentes estruturas de Botnet 27
Figura 6. "Heartlandic Russia and Periphery: Major Geopolitical Features" 33
Figura 7. A Cultura Estratégica no Ciberespaço 36

Lista de Abreviaturas

ARPA Agência de Projetos de Pesquisa Avançados

CAIH Centro de Excelência para a Ciberdefesa em Cooperação

CCDCOE Cooperative Cyber Defence Centre of Excellence

CDMA Cyber Defence Management Authority

CERN Organização Europeia para a Pesquisa Nuclear

CERT Equipa de Resposta a Emergências Informáticas

CESN Conceito de Estratégia de Segurança Nacional da Rússia

CNCS Centro Nacional para a Cibersegurança Português

CSIRT Equipas de resposta a incidentes de segurança informática

CSTB Computer Science and Telecommunications Board

DARPA Agência de Projetos de Pesquisa Avançados de Defesa

DDoS Ataque Distribuído de Negação de Serviço

EI Esfera de Informações

ENISA Agência da União Europeia para a Cibersegurança

EUA Estados Unidos da América

EUROPOL Serviço Europeu de Polícia

FSB Serviço Federal de Segurança da Rússia

GGE Group of Governmental Experts

HTCC High Tech Crime Centre da EUROPOL

HTTP HyperText Transfer Protocol

ICI Infraestrutura Crítica de Informação

ISCSP Instituto Superior de Ciências Sociais e Políticas

ISD Doutrina de Segurança das Informações da Rússia

NATO Organização do Tratado do Atlântico Norte

ONU Organização das Nações Unidas

OEWG Open-Ended Working Group

PCUS Partido Comunista da União Soviética

PESC Política Externa e de Segurança Comum da UE

PICI Proteção das infraestruturas críticas da informação

TIC Tecnologias de Informação e Comunicação

UCLA Universidade da Califórnia e Los Angeles

UE União Europeia

URL Uniform Resource Locator

URSS União das Repúblicas Socialistas Soviéticas

WWW WorldWideWeb

Introdução

A presente dissertação foi desenvolvida no âmbito do Mestrado em Estratégia do Instituto Superior de Ciências Sociais e Políticas (ISCSP) da Universidade de Lisboa, visando a obtenção do grau de Mestre em Estratégia. Este trabalho tem como tema "O Ciberespaço no conceito atual de Estratégia de Segurança Nacional da Rússia". A análise da preponderância do ciberespaço no conceito atual de Segurança Nacional da Rússia, enquadra-se no estudo das Estratégias Nacionais e Internacionais de Segurança e Defesa, área do eixo central de investigação para o Laboratório de Estudos Estratégicos, Políticos e Internacionais do ISCSP.

O principal objetivo da dissertação é compreender a preponderância do ciberespaço na definição atual do Conceito de Estratégia de Segurança Nacional da Rússia (CESN). O ciberespaço é um espaço estratégico cada vez mais relevante e securitizado, e importa compreender a sua importância na Segurança Nacional de uma grande potência.

O trabalho tem ainda três objetivos específicos, o primeiro é analisar a evolução do ciberespaço enquanto espaço estratégico, diferente dos espaços tradicionais. Para tal, serão acompanhados os estágios iniciais da Internet, e o desenvolvimento do quadro legal internacional, nomeadamente nas Nações Unidas (ONU), na União Europeia (UE) e na Organização do Tratado do Atlântico Norte (NATO).

O segundo objetivo específico é a contextualização da cultura estratégica russa, de maneira compreender os elementos culturais presentes na securitização do ciberespaço e a sua importância no Conceito de Segurança Nacional.

Apesar do foco da dissertação ser o Conceito atual, o terceiro objetivo específico passa por compreender a evolução da preponderância do ciberespaço nos documentos estratégicos russos ao longo do tempo, principalmente a partir de 2000.

Importa agora explicitar as abordagens onto-epistemológicas utilizadas, coerentes com as opções teóricas e metodológicas que serão desenvolvidas ao longo da dissertação. A ontologia é a "teoria da existência", reflete a visão que o investigador tem do mundo, ligada à epistemologia, a "teoria do conhecimento", o conhecimento que procuramos e como o procuramos (Furlong & Marsh, 2010, p. 185). Neste trabalho optou-se pela ontologia construtivista e pela epistemologia interpretativa.

O construtivismo defende que a realidade que o investigador observa é uma construção social, que apesar de ser pessoal, é afetada pelo ambiente que o rodeia (Furlong & Marsh, 2010). Este opõe-se às teorias mais tradicionais como o realismo e o positivismo que defendem a separação entre o mundo e o investigador. (Furlong & Marsh, 2010). A abordagem interpretativa funciona com o construtivismo porque procura compreender e interpretar "'subjective' meanings" (Ezzamel & Willmott, 2010, p. 81). Na ontologia construtivista "intersubjective understandings of security is one key to understanding behavior" (Buzan, Wæver & de Wilde, 1998, p. 31).

Após o fim da Guerra Fria, observou-se uma mudança paradigmática na conjuntura internacional, a nível geopolítico, econômico e social. O fim do conflito bipolar entre os Estados Unidos da América (EUA) e a União das Repúblicas Socialistas Soviéticas (URSS), que terminou com a última derrotada, mudou o equilíbrio de poder, os EUA são agora a grande potência mundial, enquanto a Rússia, estado sucessor da URSS, viveu um período de menor fulgor (McFaul, 2020). Durante este período, houve maior cooperação entre as duas potências, mas com o fortalecimento sustentado da Rússia e de Vladimir Putin como líder, a conflitualidade regressou gradualmente (McFaul, 2020).

Putin é eleito presidente no ano 2000, numa fase em que a Rússia vivia uma crise identitária e estratégica, especialmente na sua relação com o Ocidente (Roberts, 2017). O novo líder russo identificou o Ocidente, como o "inimigo comum" que procurava expandir a sua influência na esfera russa (Roberts, 2017). Esta retórica pretendia consolidar uma "identidade nacional" russa pós-URSS, assim como consolidar a posição de Putin enquanto líder incontestado que protege a sua nação do inimigo ocidental (Roberts, 2017, p. 13).

A Internet como a conhecemos surge apenas em 1990 (Singer & Friedman, 2014), e as preocupações em relação à cibersegurança estavam relacionadas principalmente com falhas tecnológicas (Hansen & Nissenbaum, 2009). A expansão e universalização da Internet fez evoluir o espectro da cibersegurança, passando a analisar "cyber security" em vez de "computer security" (Hansen & Nissenbaum, 2009, p. 1160). Esta é uma das razões para a Escola de Copenhaga desvalorizar o ciberespaço como uma questão securitária inicialmente (Hansen & Nissenbaum, 2009).

A 24 de Fevereiro de 2022, a Rússia iniciou uma tentativa de invasão total da Ucrânia após

anos de ocupação de vários territórios ucranianos. Em 2014, a anexação da Crimeia não foi conseguida apenas por meios convencionais, a Rússia terá utilizado ciberataques e campanhas de desinformação que amplificaram o efeito surpresa da sua operação militar (Wirtz, 2015). A conciliação de meios militares tradicionais e meios de base cibernética popularizou o conceito de conflito híbrido, uma nova "war-winning formula" (Renz, 2018, p. 2).

A escolha do tema justifica-se pela crescente preponderância do ciberespaço na estratégia de segurança dos Estados, num mundo cada vez mais conectado. Os ciberataques são muitas vezes analisados individualmente, sem relacionar com estratégia integral dos Estados (Wirtz, 2015).

O Conceito atual de Segurança Nacional da Rússia é um objeto de estudo de interesse inegável dado o contexto geopolítico atual. Esta dissertação foi motivada pela procura de compreender a Estratégia da Rússia, uma das grandes potências mundiais, em especial no ciberespaço. A análise proposta não procura limitar-se a relações causa-efeito, pretende-se alcançar uma compreensão de como e que fatores influenciaram a securitização do ciberespaço.

A investigação seguirá o método dedutivo, o que significa que a investigação segue "uma cadeia de raciocínio em ordem descendente, de análise do geral para o particular, chega a uma conclusão" (Prodanov & de Freitas, 2013, p. 27). A base teórica da dissertação é a Teoria Geral da Estratégia, principalmente pela letra do Professor António Silva Ribeiro (2009) do ISCSP, e a Escola de Copenhaga, fundamental para analisar a securitização do ciberespaço. Estas bases permitem-nos deduzir a preponderância do ciberespaço no conceito atual de Segurança Nacional da Rússia.

Ao longo do trabalho serão analisados obras e documentos em vários idiomas, que serão quase sempre citados diretamente na sua língua original. A principal exceção são os elementos escritos em russo, onde serão utilizadas traduções em inglês.

Ontologia e Epistemologia

A ontologia construtivista surgiu com notoriedade após a Guerra Fria, devido ao falhanço das teorias tradicionais das Relações Internacionais e da Geopolítica em projetar a queda da URSS e o fim do conflito entre blocos (Parsons, 2010, p. 81). As teorias mais tradicionais como o objetivismo e o realismo defendem que o mundo existe independentemente do observador, a realidade é a realidade, o observador procura causa-efeito no fenómeno observado (Furlong & Marsh, 2010, p. 30) (Parsons, 2010).

O construtivismo partiu das ideias de Durkheim, que defendia que as sociedades não são definidas apenas por fatores objetivos, mas também por fatores subjetivos (Durkheim, 1984, 1893, citado por Parsons, 2010, p. 81). Desta forma, o construtivismo não separa o mundo do observador, porque a sua análise não é feita a um mundo real, mas sim a um "world of our making" (Onuf, 1989, citado por Parsons, 2010, p. 80), uma construção social pessoal do observador (Parsons, 2010) (Furlong & Marsh, 2010).

Nesta ontologia, o observador analisa um fenómeno com o conhecimento que as suas ideias e experiências vão influenciar a análise e a interpretação ao fenómeno que estuda, e por isso procura compreender o fenómeno em estudo (Parsons, 2010). Uma análise construtivista não se limita a identificar causa-efeito, é necessário compreender "como?" e "que?" fatores influenciam o fenómeno em estudo (Wendt, 1998, 1999, citado por Parsons, 2010, p. 86) (Furlong & Marsh, 2010).

A epistemologia interpretativa está umbilicalmente ligada à ontologia construtivista, partindo de uma dupla hermenêutica, no primeiro nível o mundo é interpretado por atores, que num segundo nível é interpretada pelo observador (Furlong & Marsh, 2010, p. 19). A ideia de uma dupla hermenêutica foi inicialmente projetada por Wendt, que defendia que a visão construtivista procurava sempre compreender o fenómeno e não o justificar, e que para o compreender tinha de o interpretar (Parsons, 2010). A epistemologia interpretativa parte do princípio de que o mundo e o nosso conhecimento estão interligados, a realidade é construída socialmente e para estudá-la é necessário compreender e conhecer o contexto em que se insere (Furlong & Marsh, 2010). Contudo, o próprio observador é afetado pelo seu contexto social e ideias, e por isso a interpretação do observador também é influenciada

pela sua visão do mundo (Furlong & Marsh, 2010, p. 26).

A Escola de Copenhaga e o Ciberespaço

A Escola de Copenhaga ganhou notoriedade nos estudos securitários porque expandiu a abrangência do conceito de Segurança, argumentando que a Segurança "is a speech act that securitizes, that it constitutes one or more referent objects, historically the nation or state, as threatened to their physical or ideational survival and therefore in urgent need of protection" (Hansen & Nissenbaum, 2009, p. 1156). A teoria dos atos de linguagem (Speech Act Theory), o debate sobre a expansão do conceito de Segurança, e a compreensão clássica e schmittiana do Estado, são as bases teóricas que influenciam o conceito de Segurança de Copenhaga (Hansen & Nissenbaum, 2009, p. 1157). Desta forma, para a Escola de Copenhaga a Segurança está umbilicalmente ligada à linguagem empregada pelo Estado, a linguagem dos órgãos de poder em relação às ameaças e inimigos, demonstra a preponderância securitária que determinado fenómeno tem para esse Estado (Hansen & Nissenbaum, 2009, p. 1157).

Buzan, Wæver e de Wilde procuraram estruturar a análise à Segurança, afirmando que "the exact definition and criteria of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects" (Buzan et al., 1998, p. 25). Nesta afirmação é possível identificar alguns critérios para o que é uma ameaça, nomeadamente o risco que esta apresenta, que medidas são necessárias tomar, e a urgência de resposta (Hansen & Nissenbaum, 2009, p. 1158).

Os autores defendem que existem três níveis de "problemas", os não-politizados, aqueles que afetam apenas os indivíduos; os politizados, relacionados com a política pública e requerem ação do governo; e os securitizados, "an issue is no longer debated as a political question, but dealt with at an accelerated pace and in ways that may violate normal and social rules" (Hansen & Nissenbaum, 2009, p. 1159) (Buzan et al., 1998, p. 23). As principais diferenças entre os problemas politizados e os securitizados são os critérios referidos anteriormente, os efeitos políticos e a urgência de resposta, um problema apenas é securitizado se representar uma ameaça para o Estado (Hansen & Nissenbaum, 2009).

O binómio ameaça-urgência é central para identificar ameaças securitárias para a Escola de

Copenhaga, este critério permitiu a expansão do que se compreende como um problema securitário, que não se limita à compreensão clássica de Segurança (Hansen & Nissenbaum, 2009). O conceito "segurança social" surge neste contexto, e corresponde à segurança individual, onde um indivíduo ou grupo se pode sentir ameaçado pelo seu próprio Estado, seja por perseguição racial, religiosa ou de outro tipo (Wæver et al., 1993, citado por Hansen & Nissenbaum, 2009, p. 1159) (Buzan et al., 1998, p. 120). A Escola de Copenhaga já não ignora totalmente a segurança individual, mas continua a dar primazia à segurança coletiva e ao protagonismo histórico do Estado em matérias securitárias, seguindo a compreensão schmittiana do Estado (Hansen & Nissenbaum, 2009, p. 1159).

Numa fase inicial da Internet, a Escola de Copenhaga defendia que os hackers "could possibly lead to actions within the computer field but with no cascading effects on other security issues" (Buzan et al., 1998, p. 25), considerando até que a cibersegurança não passava duma tentativa de securitização do Pentágono (Buzan et al., 1998, p. 25). Desta forma, a Escola de Copenhaga argumentava que o ciberespaço não era um setor que necessita securitização por si só (Buzan et al., 1998) (Hansen & Nissenbaum, 2009, p. 1156).

Hansen e Nissenbaum (2009) argumentam que o paradigma mudou e aplicaram a framework da Escola de Copenhaga à securitização do ciberespaço. Estes autores destacam que um dos primeiros usos do conceito "cyber security" foi num relatório da Computer Science and Telecommunications Board (CSTB) de 1991, que define cibersegurança como "protection against unwanted disclosure, modification, or destruction of data in a system and also to the safeguarding of systems themselves" (CSBT, 1991, p. 2), deixando o aviso que "many disasters may result from intentional attacks on systems, which can be prevented, detected, or recovered from through better security" (CSBT, 1991 p. 2) (Hansen & Nissenbaum, 2009, p. 1160). Hundley e Anderson teorizam que um fator importante no âmbito da cibersegurança é "cyberspace safety", referente a questões relacionadas com falhas de software (sistema operativo/programas) ou de hardware (o computador em si), ou seja, falhas que não resultam da ação propositada de um ator externo e que são riscos inerentes da tecnologia em si (Hansen & Nissenbaum, 2009, p. 1160).

Nissenbaum (2005) faz a uma divisão entre dois conceitos principais de "computer security", o primeiro é o conceito de "Technical computer security", que tem como principais

preocupações ataques à "availability", "integrity" e "confidentiality" de um sistema, ou seja ataques que impedem o acesso a sistemas ou sites, ataques que corrompem a integridade da informação através da sua corrupção ou destruição e ataques que procuram o acesso a informação confidencial ou privada (Nissenbaum, 2005, p. 63-64). O segundo conceito de Nissenbaum é "cyber security", que prossupõe três ameaças principais, a primeira ameaça é o uso da internet como "medium or staging ground for antisocial, disruptive, or dangerous organizations and communications", ou seja o uso da internet para ações subversivas, desde crimes de fraude, distribuição de pornografia infantil e a coordenação de ataques terroristas (p. 64). A segunda ameaça são os ataques à infraestrutura vital de um país, seja o seu sistema de comunicações, energético ou bancário, estes ataques podem ter consequências críticas por serem interdependentes (p. 64). Da segunda ameaça decorre a terceira ameaça enumerada por Nissenbaum, que são as ameaças ao sistema de informação de um Estado no seu todo, podendo resultar em "complete debility" (Nissenbaum, 2005, p. 64).

Nissenbaum (2005) afirma que existem quatro diferenças principais entre os dois conceitos, a primeira diferença e a mais óbvia é a amplitude, "cyber security" e "computer security" convergem, mas "cyber security" é um conceito mais abrangente (p. 64). A segunda diferença está relacionada com o risco e a origem da ameaça, "computer security" lida com ameaças menores, como "damage to property, incursions on autonomy, privacy, and productivity", enquanto "cyber security" lida com ameaças que podem ter consequências graves, "possibly existential" (p. 69). A terceira diferença está relacionada com uma questão tradicional da Escola de Copenhaga, que é o alvo preferencial da ameaça, em "computer security" os alvos costumam ser pessoas ou empresas (segurança individual), enquanto em "cyber security" o alvo são os Estados (segurança coletiva) (p. 69). Finalmente, existe uma diferença nas "justifications each offers for actions taken in the name of security" (Nissenbaum, 2005, p. 69), no caso da "cyber security" o Estado age para proteger a sua soberania.

Hansen e Nissenbaum (2009) defendem que o ciberespaço pode ser comparado com outros meios não tradicionais que são securitizados pela Escola de Copenhaga, como o sistema económico e a segurança ambiental. Estes argumentam que tanto o sistema económico como o ciberespaço são setores de natureza ambígua, onde as ameaças são mais difíceis de identificar, localizar e responsabilizar (Hansen & Nissenbaum, 2009, p. 1162). O ciberespaço representa um risco acrescido para estes autores porque existe uma ligação mais direta com

a segurança militar, do que acontece no sistema económico (Hansen & Nissenbaum, 2009, p. 1162).

A multiplicidade de conceitos e linguagens para o ciberespaço e a cibersegurança é uma das principais críticas de Hansen e Nissenbaum aos autores dos Estudos de Segurança, uma vez que a utilização de "terms that overlap, but also have distinctive meanings that separate them from cyber security" leva a que haja lacunas na abordagem da Escola de Copenhaga (Hansen & Nissenbaum, 2009, p. 1156). Hansen e Nissenbaum enumeram uma multitude de conceitos como "cyber war", "net war", "network security", "Infrastructure protection", "information security", "information warfare", que foram explorados por vários autores como Der Derian, Deibert & Stein, Bendrath e Latham (Hansen & Nissenbaum, 2009, p. 1156).

Hansen e Nissenbaum (2009) identificam três "modalidades de segurança" específicas do ciberespaço, a "hypersecuritization" (hipersecuritização), "everyday security practice" (práticas de segurança quotidiana) e "technification" (tecnicidade) (p. 1165). As modalidades de segurança são o que distingue determinado setor de segurança, uma linguagem específica que conecta “referent objects, threats, and securitizing actors" (Hansen & Nissenbaum, 2009, p. 1163), e mesmo que alguns elementos destas modalidades de segurança estejam presentes em outros setores securitizados, no ciberespaço estes são especialmente preponderantes e interligados (Hansen & Nissenbaum, 2009, p. 1163).

A hipersecuritização na sua teorização original, é um fenómeno que ocorre quando se exagera o risco que uma ameaça representa, o que resulta num exagero nas medidas usadas para combater essa ameaça (Hansen & Nissenbaum, 2009, p. 1163-1164). Hansen e Nissenbaum (2009) argumentam que definir ameaças como exageradas é complicado conceptualmente, até porque normalmente os Estudos Securitários baseiam a sua análise das ameaças a partir de exemplos históricos que permitem compreender o risco que estas apresentam. Até aos ciberataques à Estónia em 2007, não existiam grandes referências históricas que demonstrassem o risco que um ciberataque representa, e por isso a securitização do ciberespaço passava muito por cenários hipotéticos (Hansen & Nissenbaum, 2009). Os ciberataques à Estónia afetaram várias instituições governamentais, mas mesmo assim não têm o mesmo impacto que as bombas nucleares de Hiroshima e Nagasaki tiveram

e que provocaram a política de dissuasão nuclear durante a Guerra Fria (Hansen & Nissenbaum, 2009, p. 1164). Os autores acrescentam que "cyber security discourse hinges on multi- dimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence and the fact that neither of these scenarios has so far taken place" (Hansen & Nissenbaum, 2009, p. 1164).

Nesta modalidade de segurança é mais lógico comparar o ciberespaço com o meio ambiente, que tal como no ciberespaço o discurso está mais virado para o futuro, e que é necessário agir no presente para prevenir ameaças futuras (Hansen & Nissenbaum, 2009, p. 1164). No entanto, no ciberespaço há maior urgência de atuação, as ameaças são imediatas e tal como com as bombas nucleares, é mais fácil visualizar as ameaças ambientais, como a poluição, a desflorestação ou o degelo do Ártico (Hansen & Nissenbaum, 2009, p. 1165).

As práticas de segurança quotidiana têm como base a relação entre os atores securitários (o Estado, organizações e empresas) e o público em geral, ou seja, a audiência (Hansen & Nissenbaum, 2009, p. 1165). Nesta modalidade securitária os atores securitários procuram mobilizar os indivíduos a ter uma participação na segurança da internet, e convencer o público em geral que os cenários de hipersecuritização podem ocorrer (p. 1165). Como foi referido anteriormente, a Escola de Copenhaga dá primazia à segurança coletiva sobre a segurança individual, neste caso a segurança individual contribui para a segurança coletiva (Hansen & Nissenbaum, 2009).

No ciberespaço o indivíduo pode ter um papel preponderante porque para além de contribuir para a segurança, este também pode representar uma fraqueza, ou até mesmo uma ameaça securitária, podendo-se comparar ao setor da saúde, onde também existem "vírus" e um indivíduo que não se proteja devidamente pode colocar outros em risco (Hansen & Nissenbaum, 2009, p. 1166). A importância de convencer a audiência que a cibersegurança é necessária deve-se à abrangência que o ciber tem nas suas vidas, mesmo quem não utilize a internet ou computador no seu quotidiano é-lhe dependente (Hansen & Nissenbaum, 2009). Os autores lembram que uma securitização bem-sucedida deve ir ao encontro da vontade e necessidade da opinião pública, e por isso é necessário convencer a audiência que certo fenómeno necessita de securitização (Hansen & Nissenbaum, 2009).

A tecnicidade está caracteristicamente ligada à inovação tecnológica, e por isso a opinião de

especialistas técnicos das tecnologias de informação e comunicação (TIC) toma um papel central na securitização do ciberespaço (Nissenbaum, 2005) (Hansen & Nissenbaum, 2009). As inovações tecnológicas têm ocorrido a um ritmo que é difícil de acompanhar para aqueles que não são especialistas, e por isso é necessário recorrer a engenheiros informáticos que participam no processo de securitização (Hansen & Nissenbaum, 2009, p. 1166-1167). A participação dos especialistas leva a que a securitização ocorra através de atos de linguagem que recorrem a vários tecnicismos, que permite estabelecer "an issue as reliant upon technical, expert knowledge" aliado a "politically and normatively neutral agenda" (Hansen & Nissenbaum, 2009, p. 1167). A tecnicidade é baseada em conhecimento objetivo e científico, neutro do ponto de vista político, contudo os autores avisam que esta característica pode ajudar a esconder interesses políticos (Hansen & Nissenbaum, 2009, p. 1167-1168). A neutralidade inerente à tecnicidade não despolitiza, ou seja, não provoca a "dessecuritização" do ciberespaço, provoca sim a credibilização do processo de securitização (Hansen & Nissenbaum, 2009). A dessecuritização ocorre quando um fenómeno perde urgência ou risco e por isso passa a ser um problema não-politizado para a Escola de Copenhaga (Buzan et al., 1998, p. 29).

Em todos os setores é necessário recorrer a especialistas que guiem a atuação dos poderes de decisão e por isso a tecnicidade não é exclusiva do ciberespaço, mas tanto o ritmo de inovação neste setor, como a disparidade de conhecimento entre um técnico e o público em geral provoca que a tecnicidade tenha maior preponderância (Hansen & Nissenbaum, 2009). Compara-se novamente o ciberespaço ao setor ambiental, em que a opinião pública pressiona os atores com poder de decisão porque existe uma consciencialização maior da audiência sobre o problema que está a ser securitizado (Hansen & Nissenbaum, 2009, p. 1168).

Enquadramento Teórico

Inicialmente o estudo da Estratégia focava-se na "arte do comando" e na "descrição de combates" (Ribeiro, 2009, p.23). A teorização estratégica utilizava técnicas empíricas provenientes das disciplinas da Tática e da História, algo que só começou a mudar a partir do século XVIII quando o foco do passou dos campos de batalha e dos militares para o campo da política e dos políticos, e por consequência "os estudos estratégicos incorporaram

perspectivas e técnicas de outras ciências sociais, das quais a ciência política é a principal" (Ribeiro, 2009, p.23). A palavra estratégia é utilizada atualmente de forma generalizada, contudo só depois do fim da 2º Guerra Mundial começou a ser utilizada fora do contexto militar (Ribeiro, 2009, p.21).

Ribeiro (2009) define Estratégia como “a ciência e arte de edificar, dispor e empregar meios de coação num dado meio e tempo para materializar objetivos fixados pela política, superando problemas e explorando eventualidades em ambiente de desacordo” (p. 22). Nesta definição há vários elementos que merecem ser dissecados e explorados, principalmente os "meios de coação num dado meio e tempo".

Os meios de coação são meios "de qualquer natureza, que podem ser aplicados em esforços estratégicos substanciais e prolongados, de forma a influenciar as acções do contrário com previsibilidade, garantindo assim a materialização dos objetivos nacionais" (Ribeiro, 2009, p. 35). A coação distingue a estratégia de um plano onde não há um adversário, a coação procura influenciar o comportamento do outro, "demonstrando-lhe benefícios em caso de conformidade, ou custos em caso de rejeição" (p. 35-36). No processo estratégico os meios de coação "traduzem o potencial estratégico dos contendores, a empregar na acção estratégica (com quê?)"(Ribeiro, 2009, p. 107).

Ribeiro (2009) afirma que quanto à estruturação dos meios do Estado, a estratégia tem três níveis, a estratégia estrutural, que supervisiona a disposição dos meios e a “composição, organização e articulação em capacidades coerentes, interdependentes e colaborantes” (p. 83), a estratégia operacional, relacionada com o emprego dos meios para alcançar os objetivos propostos pela estratégia estrutural, e a estratégia genética, relacionada com a edificação de novos meios a serem utilizados na estratégia operacional (Ribeiro, 2009, p. 82).

Beaufre (2004) defende que, quanto aos meios de coação utilizados por um Estado, a estratégia estruturam-se numa “pirâmide que desdobra, em planos analíticos decrescentes, a estratégia integral, as estratégias gerais e as estratégias particulares, segundo os objetivos a materializar e as acções a realizar” (Ribeiro, 2009, p. 75). O objeto de estudo da dissertação é o conceito de Segurança Nacional da Rússia, por isso importa focar na estratégia integral. A estratégia integral era inicialmente entendida como a “grande estratégia” (Ribeiro, 2009, p. 78), estando diretamente relacionada com o poder militar e com a guerra, hoje a

estratégia integral “abarca o estudo e a aplicação de todas as formas de coação (política, económica, psicossocial e militar)” (Ribeiro, 2009, p. 77).

Na fase primitiva do pensamento estratégico o meio estava associado “à geografia física para a grande tática e à topografia para a pequena tática” (Charnay, 1990, citado por Ribeiro, 2009, p. 36), Sun Tzu definia o meio como “espaço” que se refere “às distâncias grandes e pequenas; aos locais perigosos e seguros; aos campos abertos e às passagens estreitas, às probabilidades de vida ou morte” (Tzu, p. 21).

O meio estratégico era apenas a "área estratégica onde se desenvolviam os planos e as manobras" (Ribeiro, 2009, p. 36), numa compreensão mais atual um espaço estratégico é "em simultâneo, um lugar e um conjunto de comportamentos que aí se podem exercer" (Charnay, 1990, citado por Ribeiro, 2009, p. 36) e que "à medida que mudam os elementos do meio, os componentes do conceito de estratégia devem ser adaptados" (Ribeiro, 2009, p. 36). Posteriormente, Ribeiro (2009) afirma que no processo estratégico, o meio estratégico estipula “as condições de realização estratégica (onde?) e obedece ao requisito de proporcionar a melhor materialização do objetivo fixado pela política” (p. 107).

No que diz respeito ao meio/espaço estratégico, a Geopolítica é outra disciplina que surge no âmbito da Estratégia e das Relações Internacionais, no século XIX, por Ratzel que defendia que “the state as an organism fixed in the soil whose spirit derived from mankind’s ties to the land” (Cohen, 2014, p. 17). No início da disciplina, os principais autores debatiam qual dos dois espaços era mais importante estrategicamente, Mackinder defendia a primazia do meio terrestre, enquanto Mahan defendia o meio marítimo (Cohen, 2014). O debate sobre os espaços expandiu-se a um terceiro espaço após a invenção da aeronave, resultante da evolução tecnológica (Cohen, 2014).

Nesta dissertação considera-se que a invenção da Internet e o subsequente crescimento do ciber, criaram um novo meio estratégico, o ciberespaço. A definição de ciberespaço não é pacífica, não só por se tratar de uma realidade relativamente recente e pela "sua natureza expansiva e global" (Singer & Friedman, 2014, p. 13). A evolução do ciberespaço será desenvolvida posteriormente, mas importa explicitar o que é o ciberespaço, e como pode ser conceptualizado.

O principal responsável pela instrumentalização do ciberespaço enquanto meio estratégico, o departamento de Defesa dos EUA, já produziu várias definições diferentes, a definição atual surge em 2008 e define o ciberespaço como “the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers” (Singer & Friedman, 2014, p. 13). O Centro Nacional para a Cibersegurança (CNCS) português declarou que o "Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação" (Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, 2019, p. 2089).

A doutrina mais recente da Rússia para o ciberespaço segue uma linha holística e descreve uma “sphere of informations” (esfera de informações) como

> a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet [...], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere. (Federação Russa, 2016)

Singer e Friedman (2014) definem ciberespaço como "the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online" (p. 13). Contudo, os autores argumentam que mais importante que ter uma definição concreta de ciberespaço, é fundamental compreender os seus principais elementos, que as várias definições citadas deixam evidentes serem as informações, as máquinas e os utilizadores (Singer & Friedman, 2014).

O ciberespaço é assim um meio híbrido, com fronteiras menos rígidas que os meios estratégicos tradicionais, mas que ainda assim está dependente de máquinas físicas e das pessoas que as controlam (Singer & Friedman, 2014).

O tempo é um elemento estratégico que se divide entre momento, que “traduz o quadro global da realidade política, económica, psicossocial e militar”, duração, que “define o

período de tempo", e ritmo, que "caracteriza a variação da intensidade e de velocidade" (Ribeiro, 2009, p. 37) O tempo (quando?) é fundamental no processo estratégico porque "está intimamente ligado às mudanças de situação e ao emprego dos meios (manobra e tipo)" (Ribeiro, 2009, p. 109). Martins afirma que "a projeção do tempo para a rede geograficamente localizada no ciberespaço renúncia às características tradicionais, nas quais o Estado operava e se baseava desde os tempos mais remotos na definição das suas políticas e na defesa do interesse nacional" (Martins, 2012, p. 34).

Ainda sobre o conceito de Estratégia importa referir o conceito de cultura estratégica, que nasce dos "estudos sobre "cultura nacional" e da análise sobre os "processos de tomada de decisão estratégica" aplicados a cenários de segurança e defesa" (Romana, 2016, p. 14), sendo cada vez mais relevantes nos estudos estratégicos, securitários e em outras áreas como as relações internacionais, nomeadamente na corrente construtivista (Romana, 2016, p. 19-20).

A cultura estratégica ganhou notoriedade com Snyder em 1977, definindo-a como "o somatório de ideais, respostas emocionais e padrões de comportamento que os membros de uma comunidade estratégica nacional adquirem." (Snyder, 1977, citado por Romana, 2016, p. 16). Nesta obra, Snyder analisa a estratégia e a tomada de decisão dos líderes da URSS, e observa que a cultura estratégica soviética é diferente da cultura norte-americana, não sendo "suficiente" analisá-los por via da "teoria de escolha racional" (Romana, 2016, p. 16). Na conceptualização de cultura estratégica destaca-se a visão de Colin Gray (1986), que segundo Romana (2016)

> Explora o conceito de Cultura Estratégica por meio de um insight sistémico, afirmando que toda a acção de uma comunidade de segurança, se não constitui uma manifestação de cultura estratégica, é pelo menos expressão de um processo em que os indivíduos são enculturados, e as organizações, os procedimentos e a gestão militar, são resultado de fatores culturais permanentes. (p. 17)

Na Escola de Copenhaga, Götz e Staun (2022) definem cultura estratégica como um conjunto de "discursive expressions and narratives related to security-military affairs, which are shared by a country's political leaders and elites. These discursive expressions and narratives are rooted in socially constructed interpretations of history, geography, and domestic

traditions" (p. 482).

A cultura estratégica não dever ser confundida com doutrina, Ribeiro refere que "a doutrina indica soluções fundamentadas para problemas tácticos ou técnicos repetitivos" (Ribeiro, 2009, p. 45), mas "só faz sentido na medida em que produzir efeitos práticos" (p. 43). A doutrina deve conseguir "seleccionar, disciplinar, simplificar e estabilizar procedimentos em múltiplas actividades, para que elas sejam racionalmente articuladas, produzindo efeitos eficazes com a maior eficiência" (Ribeiro, 2009, p. 43).

Ribeiro (2009) afirma que a Segurança Nacional está associada à "conservação da sociedade política" (p. 48), optando por uma definição clássica centrada "na capacidade do Estado conter autonomamente as ameaças" (Ribeiro, 2009, p. 49).

Couto defende uma definição de segurança mais abrangente, que incluí "o acesso a matérias-primas essenciais", "a proteção de investimentos e cidadãos nacionais no estrangeiro" e "controlo do nível de capacidade militar de adversários potenciais e vizinhos" (Couto, 1988, citado por Ribeiro, 2009, p. 51), que motiva um aviso que "a preocupação da segurança pode tornar-se tão ambiciosa, que acabe por se transformar em aspiração de ilimitada expansão" (Ribeiro, 2009, p. 51).

Ribeiro afirma que a Segurança Nacional está alicerçada na força dos Estados, teorizada por Aron, que defende que “um Estado será tanto mais seguro, quanto mais forte” (Ribeiro, 2009, p. 52). Charles-Philippe David destaca as capacidades militares, por serem “para uma maioria dos Estados uma das garantias essenciais da sua sobrevivência” (David, 2001, citado por Ribeiro, 2009, p. 52), mas nem sempre um Estado forte militarmente está seguro, até porque uma “edificação extrema de capacidades militares” pode provocar uma resposta dos países vizinhos ou competidores e criar um paradoxo de segurança (Ribeiro, 2009, p. 52).

Atualmente, a Rússia define Segurança Nacional como

> The state of protection of national interests of the Russian Federation from external and internal threats, which ensures the implementation of constitutional rights and freedoms of citizens, decent quality and standard of living, civil peace and accord in the country, protection of the sovereignty of the Russian Federation, its independence and national integrity, the socio-economic development of the country (Federação

Russa, 2021, p. 2).

Opções Metodológicas

O estudo da Estratégia era na sua génese a análise de batalhas e conflitos, "com recurso às técnicas da História e na Tática", mas com o tempo o estudo estratégico centrou-se cada vez mais na política (Ribeiro, 2009, p. 23). Esta mudança de foco, aliada ao aparecimento e evolução de outras ciências sociais, transformou o estudo da Estratégia num estudo pluridisciplinar (p. 23). Desta forma, serão utilizadas ferramentas, técnicas e perspetivas de outras ciências sociais, como a Ciência Política. as Relações Internacionais e a Geopolítica (Ribeiro, 2009).

A pergunta de partida que esta dissertação procura responder é **"Que importância tem o ciberespaço no conceito atual de Estratégia de Segurança Nacional da Rússia?"**. A questão central é complementada por três perguntas específicas que permitem ter uma compreensão mais completa do ciberespaço e a estratégia da Rússia.

- Como é que o ciberespaço se tornou num espaço estratégico?
- Qual é a cultura estratégica russa?
- Como evoluiu a preponderância do ciberespaço no conceito de Segurança Nacional da Rússia?

A dissertação é um case-study que parte do método dedutivo, o que significa que a investigação segue "uma cadeia de raciocínio em ordem descendente, de análise do geral para o particular, chega a uma conclusão" (Prodanov & de Freitas, 2013, p. 27)." O estudo de caso permite orientar "a busca de explicações e interpretações convincentes para situações que envolvam fenómenos sociais complexos" (Martins, 2006, citado por Prodanov & de Freitas, 2013, p. 61)

A dissertação parte da compreensão do ciberespaço enquanto espaço estratégico e da cultura estratégia russa (geral), descendendo para análise da doutrina russa do ciberespaço e outros documentos oficiais de Estratégia russos (particular), para finalmente compreender e concluir que preponderância tem o ciberespaço no conceito atual de Segurança Nacional

da Rússia.

As opções ontológicas e epistemológicas impactam as opções metodológicas adotadas para a realização da dissertação, o construtivismo e a visão interpretativa dão primazia a fontes documentais e literárias, ao contrário do realismo ou do positivismo que preferem análises quantitativas (Furlong & Marsh, 2010, p. 21). A análise e pesquisa de documentos qualitativos permite-nos "compreender" o significado das ações em estudo, não se limita a "explicar" esse fenómeno (Furlong & Marsh, 2010, p. 21).

A técnica de observação documental e bibliográfica, será a principal ferramenta de recolha de dados e investigação, recorrendo a documentos físicos e à Internet (Prodanov & de Freitas, 2013). A pesquisa documental e bibliográfica tem como base obras literárias, artigos científicos, relatórios oficiais e notícias que permitem analisar o processo estratégico “a qualquer nível de decisão” (Ribeiro, 2015, p. 26).

A dissertação vai analisar documentos oficiais russos, que podem ser classificados como fontes primárias por serem produzidas diretamente por órgão de poder, como o Presidente ou pelo Ministério da Defesa (Fernandes, 2012). Estes documentos explicitam o conceito atual de Segurança Nacional da Rússia, permitindo compreender como ocorreu a securitização do ciberespaço. A análise destes documentos seguirá a lógica construtivista de interpretar e compreender o discurso e a linguagem utilizada pelo órgão de poder "knowledge is theoretically or discursively laden" (Furlong & Marsh, 2010, p. 26).

As fontes primárias vão ser complementadas por fontes secundárias, como artigos científicos, dissertações e outras obras literárias, que nos permitem compreender o contexto em que a securitização do ciberespaço ocorreu (Fernandes, 2012). A utilização de fontes primárias e secundárias permite-nos ter uma visão mais completa do fenómeno em estudo, neste caso as fontes secundárias são fundamentais para contextualizar a atuação da Rússia com a sua cultura estratégica, enquanto as fontes primárias permitem acompanhar e interpretar a evolução da preponderância do Ciberespaço no conceito de Segurança Nacional russo. Apesar da grande preponderância da análise qualitativa, não serão ignorados fatores e fontes quantitativas que enriqueçam o estudo e nos permitam ter uma compreensão mais completa do contexto em que insere a securitização do ciberespaço por parte da Rússia.

As fontes utilizadas na realização deste trabalho foram consultadas maioritariamente através da internet, em plataformas como a JSTOR, B-ON, Google Scholar e Academia.edu. Os documentos oficiais foram retirados sempre que possível dos sites oficiais das instituições que os produziram, sejam documentos estratégicos russos, da NATO ou da UE. A leitura de outras dissertações de mestrado na área da Estratégia, foi feita em plataformas como o Repositórios Científicos de Acesso Aberto de Portugal (RCAAP).

Capítulo I. O Ciberespaço

Neste capítulo procura-se compreender o desenvolvimento do ciberespaço enquanto meio estratégico. Em primeiro lugar será realizada uma contextualização histórica sobre a origem e evolução da Internet, em particular na URSS e na Rússia, depois será analisado o quadro legal internacional para o ciberespaço.

A História da Internet

A primeira mensagem transmitida entre computadores resultou de um erro, quando investigadores da Universidade da Califórnia e de Los Angeles (UCLA) tentaram conectar-se a um computador do Stanford Research Institute, em 1969 (Singer & Friedman, 2014, p. 16). Estes investigadores faziam parte do projeto ARPANET que impulsionou "the modern cyber era", iniciado com objetivo de criar uma rede entre universidades (Singer & Friedman, 2014, p. 18).

O projeto ARPANET surge no âmbito da Agência de Projetos de Pesquisa Avançados (ARPA), agência que nasceu em 1958, em resposta ao sucesso o satélite Sputnik 1 da URSS, esta agência viria a mudar de nome para Agência de Projetos de Pesquisa Avançados de Defesa (DARPA), em 1972 (Konradova, 2020, p. 39) (Singer & Friedman, 2014, p. 17). Anatoly Kitov tentou implementar um projeto de redes de computadores em 1959, mas foi rejeitado pelo Partido Comunista da URSS (PCUS) e pelo Ministério da Defesa (Konradova, 2020, p. 40).

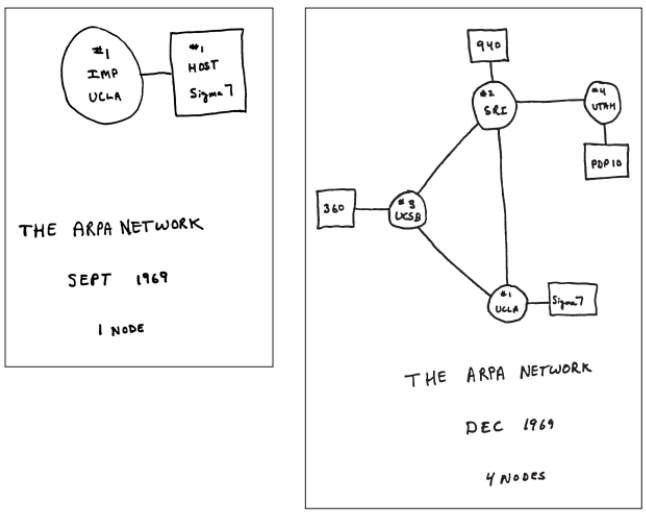

Figura 1. Diagramas originais da ARPANET de setembro e dezembro de 1969 (Dodge & Kitchin, 2001, p. 16)

Até 1970 a ligação entre computadores necessitava de ligação direta, a “Internet” permitiu que as ligações deixassem de funcionar em circuitos para funcionarem em "packets", garantindo maior flexibilidade e resiliência (Singer & Friedman, 2014, p. 17). Nesta década surgiram algumas inovações tecnológicas importantes, em 1972 Ray Tomlinson inventou o primeiro serviço de e-mail, e em 1973 surge um “protocol” que permitiu a evolução de uma “rede de computadores” para uma “rede de redes” (Singer & Friedman, 2014, p. 18-19). A URSS continuava a tentar estabelecer uma rede própria e criou a All-State Automated System (OGAS), mas esta perdeu apoio durante a década de 1970 (Konradova, 2020, p. 40).

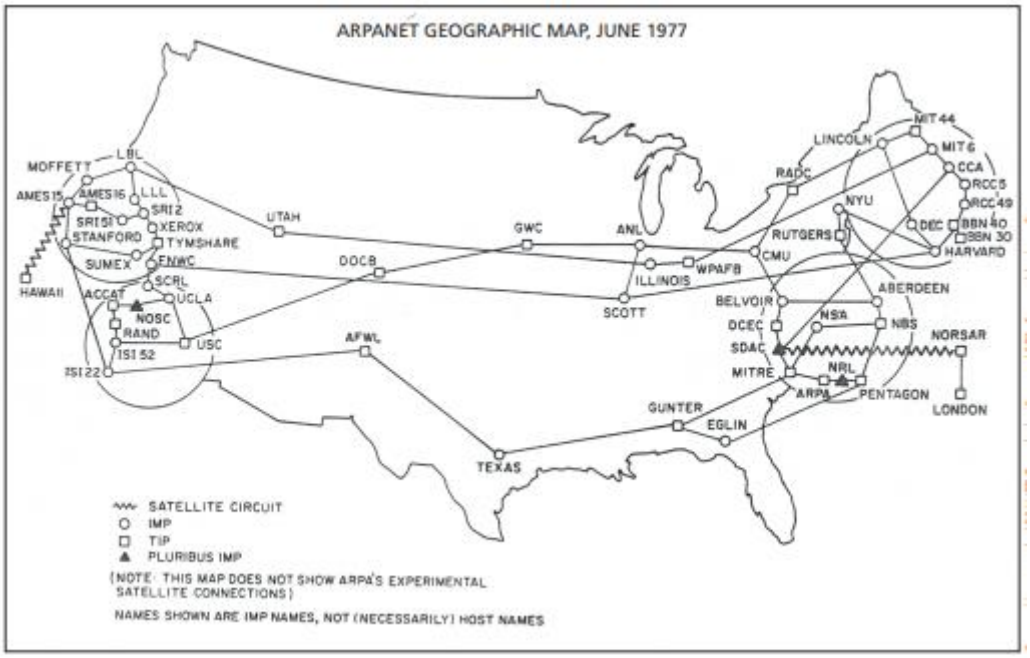

Figura 2. O mapa da Arpanet em 1977 (Dodge & Kitchin, 2001, p. 19)

Na década de 1980 surgem redes alternativas à ARPANET, maioritariamente de gênese académica, mas a expansão da “internet” deve-se também à vontade de outras áreas participarem na partilha remota de informações e conhecimento (Singer & Friedman, 2014, p. 19). Esta expansão marcou o início da democratização dos computadores, que inicialmente estavam reservados aos setores militares e governamentais (Konradova, 2020, p. 40) (Singer & Friedman, 2014). A popularidade crescente dos computadores, promoveu a “introduction of the profit motive in internet expansion” (Singer & Friedman, 2014, p. 19), as empresas começaram a querer participar e em 1983 surge o MCI, o primeiro serviço de e-mail comercial.

Entre as novas redes destaca-se a USENET, que tem especial importância por ter sido uma

rede onde programadores soviéticos interagiram com programadores americanos (Konradova, 2020, p. 40). No dia 1 de abril de 1984, foi publicada na ARPNET uma carta com assinatura de Konstantin Chernenko, Secretário-Geral do PCUS, uma partida de "Dia das Mentiras" que terá motivado uma discussão "at the Pentagon in the context of information security" (Konradova, 2020, p. 41). Em 1983, uma cópia do sistema operativo Unix foi transferida da Universidade de Berkeley, dos EUA, e levada para a URSS, para que fosse desenvolvido um sistema operativo próprio, que acabou por se chamar Demos (Konradova, 2020, p. 42). Os especialistas soviéticos demoraram cinco anos a desenvolver o Demos, até que em 1988 Andrej Kolesnikov foi o primeiro soviético a publicar na USENET (Konradova, 2020, p. 42).

Nos EUA, os finais da década ficam marcados pelo início da campanha para a "privatização" da internet, passando a responsabilidade de desenvolver o ciberespaço para os atores comerciais (Singer & Friedman, 2014, p. 19). O plano inicial da Casa Branca projetava que a privatização fosse completada no final da década de 1990, mas o processo foi acelerado graças à High Performance Computing and Communication Act de 1991 (Singer & Friedman, 2014, p. 19-20).

Os primeiros anos da década de 1990 são ricos em desenvolvimentos, que permitiram que a internet se tornasse ainda mais popular, tanto nos EUA como na URSS (Singer & Friedman, 2014, p. 20). Em 1990, surge a WorldWideWeb (WWW), uma inovação de Tim Berners-Lee, investigador da Organização Europeia para a Pesquisa Nuclear (CERN) (Singer & Friedman, 2014, p. 20). Nesta inovação a internet transforma-se na internet que conhecemos atualmente, surgem também o HyperText Transfer Protocol (HTTP), protocolo que permitia transferir páginas da Internet e dados entre um servidor a WWW, e o Uniform Resource Locator (URL), que permite localizar os conteúdos da internet e criar ligações para essas localizações (Singer & Friedman, 2014). A WWW revolucionou o ciberespaço porque deu um papel ativo na Internet aos utilizadores, através da criação de sites pessoais (Konradova, 2020, p. 51).

Na URSS, a primeira rede de computadores foi estabelecida em agosto de 1990, pela Demos, cooperativa formada pelos investigadores que criaram o sistema operativo com o mesmo nome (Konradova, 2020, p. 42) (Galushkin, 2015, p.305). Esta rede partia do Instituto

Kurchatov de Energia Atómica em Moscovo, e conectava instituições de Leningrado, Novosibirsk e Moscovo (Galushkin, 2015, p.305). A primeira conexão à internet global ocorreu ainda nesse mês, através de uma ligação dial-up (por linha telefónica) entre Moscovo e a Universidade de Helsínquia (Konradova, 2020, p. 42-43) (Galushkin, 2015, p. 305).

Em agosto de 1991, há uma tentativa de golpe de estado na URSS, que tem a duração de quatro dias, de 18 a 22 de agosto (Dunlop, 2003, p. 111). Neste período, a imprensa escrita e a Televisão Central Soviética foram tomadas pelos golpistas, que tentaram evitar que os meios de informação estrangeiros transmitissem o que estava a acontecer (Konradova, 2020, p. 43).O golpe liderado por Gennadii Yanaev, Vice-Presidente da URSS, falhou em parte porque a Relcom (antiga Demos) conseguiu comunicar com o Ocidente através da USENET, por e-mail e fax (Konradova, 2020, p. 43) (Dunlop, 2003, p. 116).

O golpe de Estado fracassou, mas teve impactos imediatos, com várias Repúblicas Populares a declararem-se independentes da URSS, nomeadamente a República Socialista Federativa Soviética da Rússia, liderada por Boris Yeltsin, que a 22 de agosto decretou a soberania económica da região (Dunlop, 2003, p. 116). A URSS dissolveu-se oficialmente a 26 de dezembro de 1991, depois do Acordo de Belavezha, celebrado pelos líderes das repúblicas soviéticas da Bielorrússia, Ucrânia e Rússia (Dunlop, 2003, p. 127). O fim da URSS resultou no estabelecimento da Federação Russa enquanto Estado soberano e independente, a 25 de dezembro de 1993 a Constituição votada entrou em vigor (Federação Russa, 1993).

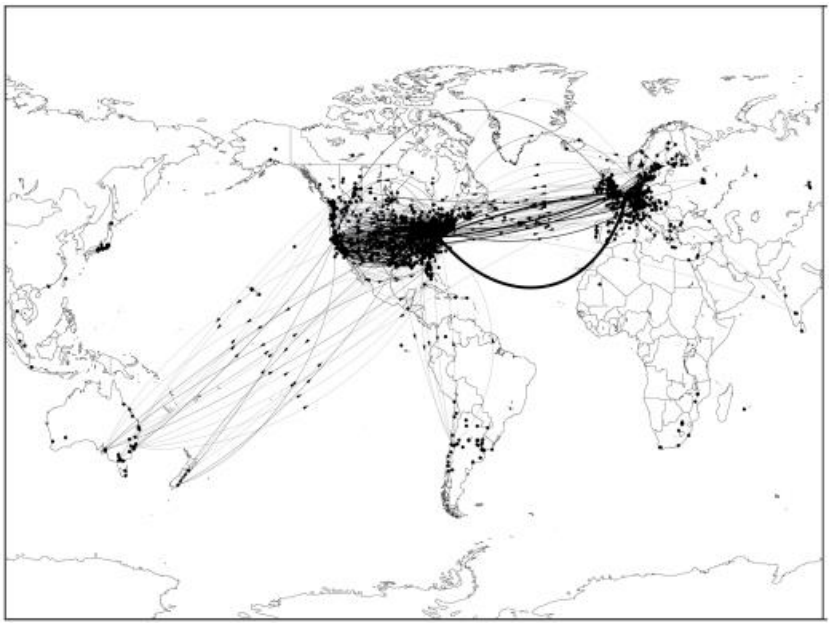

Figura 3. Tráfego de Informação na USENET em 1993 (Dodge & Kitchin, 2001, p. 53)

A USENET continuou a ser a plataforma mais utilizada na Rússia durante a primeira metade da década de 1990, que coincidiu com o aparecimento de fornecedores de internet comerciais (Konradova, 2020, p. 44). A dissolução da URSS era um dos temas mais discutidos nos fóruns da USENET, até pelo papel que a plataforma tinha tido na tentativa de golpe de estado (Konradova, 2020). A USENET manteve a sua popularidade porque existiam várias newsrooms programados em alfabeto cirílico, destinados apenas para internautas russos (Konradova, 2020, p. 49). Neste contexto, a expressão "Relcolm", mesmo nome que a empresa, fica associada à internet (USENET) destinada à comunidade russófona (Konradova, 2020, p. 49).

A democratização da internet na Rússia nos últimos anos do século XX, levou os utilizadores a migrar da USENET para WWW, que na Rússia ficou conhecida por Runet, a internet da Rússia (Konradova, 2020, 49). A runet "described not only language but also the special atmosphere of Russian Internet" (p. 48), para os russos a internet era uma nova fonte informação, a socialização virtual não era o foco (Konradova, 2020, p. 49).

Nos anos 2000, e com a chegada de Vladimir Putin ao poder, o governo russo começa a intervir mais na internet, através da criação de sites governamentais e a organização de concursos, como o Runet Award (Konradova, 2020). A participação do Estado começa por ser inofensiva, mas com o tempo começam a ser desenvolvidos "security and control programmes" (p. 54), onde se destaca o programa SORM 2, que permitia que os serviços de

segurança russos pudessem monitorizar o que os utilizadores faziam nos seus computadores (Konradova, 2020, p. 57).

A runet, e a internet a nível global, sofrem uma mudança paradigmática com o aparecimento das redes sociais, como o Livejournal e o Facebook, que tiveram direito a clones russos (Konradova, 2020, p. 56). As redes sociais serviram de plataforma para que vários movimentos ideológicos e políticos mais radicais se tornassem “mainstream” (Konradova, 2020, p. 56).

Quadro Legal Internacional

As primeiras discussões sobre a Segurança das TIC e da Internet surgiram ainda na década de 90 do século XXI, em 1998, por iniciativa russa na ONU (Tiirmaa-Klaar, 2021, p. 3) (Ramich & Piskunov, 2022). Na carta escrita ao Secretário-Geral da ONU, Kofi Annan, o ministro dos negócios estrangeiros russo, Igor Ivanov, pretendia discutir as possíveis ameaças resultantes da inovação tecnológica e colocassem em causa “maintaining international stability and security” (Federação Russa, 1998).

Esta proposta culminou na elaboração da "Declaração de Princípios da Construção da Sociedade Informática: um desafio global no novo Milénio" (2003) e na criação do Group of Governmental Experts (GGE), composto por especialistas da Segurança nas TIC (Tiirmaa-Klaar, 2021, p. 3).

O primeiro relatório da GGE (2004-2005) não terminou em acordo devido à "unwillingness of the UN Security Council permanent members to agree on the direction of the report, and the lack of broader international interest toward cyber stability issues at that time" (Tiirmaa-Klaar, 2021, p. 3).

O ano 2001 foi marcante para a discussão do Ciberespaço na UE, em janeiro a Comissão Europeia lança o comunicado "Criar uma Sociedade da Informação mais segura reforçando a segurança das infraestruturas de informação e lutando contra a cibercriminalidade", lançando o desafio aos Estados Membros para convergirem e discutirem a Segurança das TIC no espaço Europeu (Hermenegildo, 2020, p. 19) (Beláz, 2019, p. 19-20).

Este desafio foi correspondido em Junho com proposta de estratégia das redes e informações

da UE, e em Novembro com a Convenção de Budapeste sobre a Cibercriminalidade, com o propósito de

> ajudar na luta contra os crimes que apenas podem ser cometidos através da utilização de tecnologia, nos casos em que os dispositivos sejam simultaneamente a ferramenta para a prática da criminalidade e o objetivo da criminalidade, bem como contra crimes em que a tecnologia tenha sido utilizada para potenciar outro crime, tal como a fraude. (União Europeia, 2023)

O tratado entra em vigor em 2004, ano em que é estabelecida a Agência da União Europeia para a Cibersegurança (ENISA), com o objetivo final de "manter a segurança digital da sociedade e dos cidadãos europeus" (ENISA). Beláz (2019) e Hermenegildo (2020) afirmam que nesta fase a cibersegurança ainda era vista como "complementar" (Hermenegildo, 2020, p. 21), o que só mudou após os ciberataques à Estónia em 2007.

Em 2002, é a primeira vez que a ciberdefesa está na sua agenda política numa cimeira da NATO, a Declaração dos Chefes de Estado presente na cimeira de Praga dedica-lhe apenas uma linha de texto "f. Strengthen our capabilities to defend against cyber attacks" (NATO, 2002, p. 53).

O ano de 2007 mudou o paradigma internacional para o Ciberespaço a Estónia sofreu, de 27 de abril até 18 de maio de 2007, os primeiros ciberataques "directed as a coercive instrument in a political conflict against a nation" (Schmidt, 2013, p. 1). Os ciberataques incidiram sobre as principais instituições e figuras políticas, agências noticiosas e o sistema bancário (Schmidt, 2013, p. 4).

Os ataques terão sido orquestrados e coordenados através de fóruns e outras plataformas virtuais de hackers russos, como forma de protesto à relocalização do monumento erguido em 1947 para celebrar a vitória do Exército Vermelho sobre a Alemanha Nazi em Tallinn (Schmidt, 2013, p. 8) (Herzog, 2011, p. 50-51). Após a sua independência a Estónia renomeou o monumento, e mais tarde decidiu movê-lo porque a estátua do soldado com a farda do Exército Vermelho era vista como "a symbol not of the achievements of the Red Army in WWII, but of its subsequent role as a suppressor of Estonian independence" (Schmidt, 2013, p. 8).

Nesta primeira fase foram utilizadas várias modalidades de ciberataques, "Distributed Denial of Service (DDoS) attacks, website defacements, DNS server attacks, mass e-mail, and comment spam" (Schmidt, 2013, p. 1). A principal modalidade utilizada foram os ataques DDoS, que o CNCS português define como "uma forma maliciosa de interromper o tráfego serviço, servidor ou rede, através da sobrecarga do mesmo" (CNCS, n.d.), ou seja são ataques que conseguem tornar sites e servidores inacessíveis através de um número de estímulos exagerado (Figura 4).

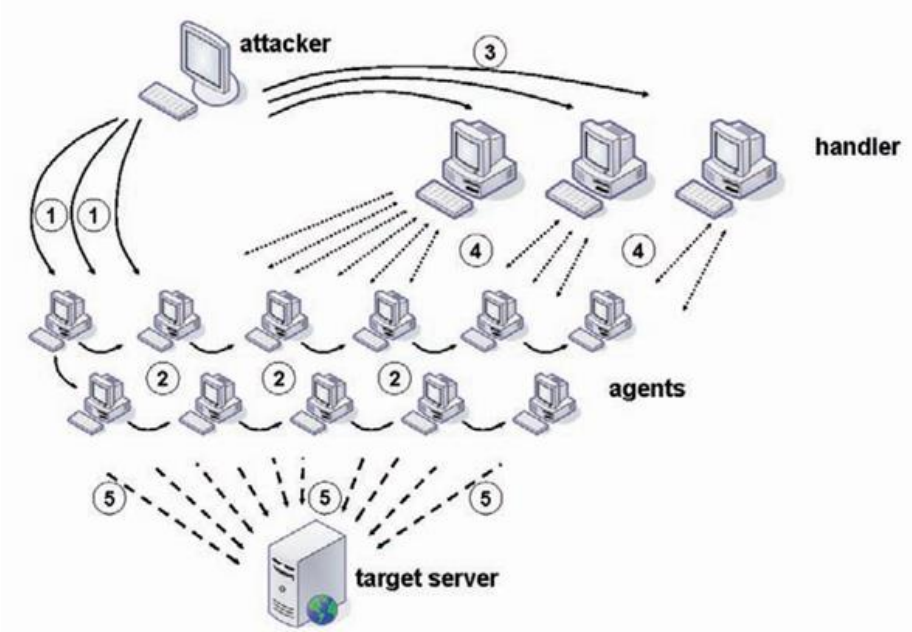

Figura 4. Ataques DDoS (Disterer, Alles, & Hervatin, 2007, p. 264)

O spam de e-mails provoca o superlotar das caixas de entrada, o que não só sobrecarrega os servidores, como atrasa e coloca em causa uma via de comunicação importante (Schmidt, 2013). Nas primeiras horas, os ataques estavam a ser tratados como um ataque DDoS comum, mas em menos de um dia, o ministro da Defesa estónico Jaak Aaviksso afirmou que estes representavam um risco de Segurança Nacional (Schmidt, 2013, p. 8).

A 30 de Abril entramos na segunda fase dos ciberataques, e nesta fase as botnets (Figura 5.) tornam-se preponderantes (Schmidt, 2013, p. 9). O CNCS português segue a convenção europeia e define uma botnet como "Rede de computadores infetados [drones] por software malicioso e controlados à distância, sem o conhecimento dos utilizadores, com a finalidade de enviar mensagens eletrônicas não solicitadas, roubar informações ou lançar ciberataques coordenados." (CNCS, n.d.).

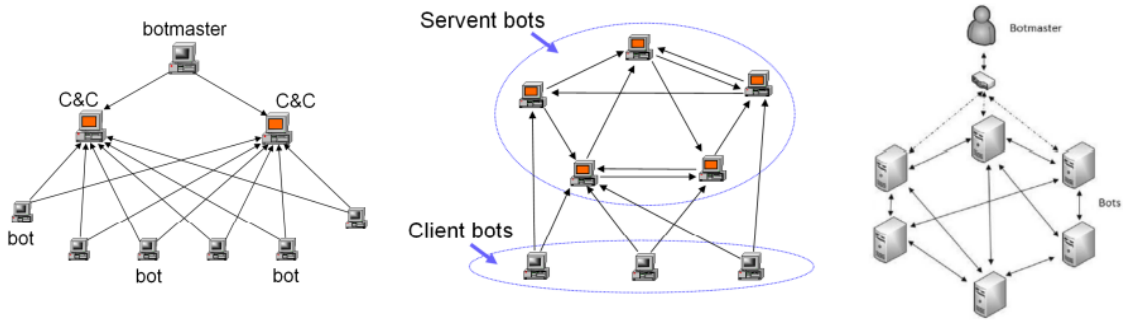

Figura 5. As diferentes estruturas de Botnet. À esquerda: Botnets Centralizadas; ao centro: Botnets Híbridas (Wang, Sparks & Zou, 2008); à direita: Botnets Descentralizadas (Hyslip & Pittman, 2015, p. 12).

Os meios e a escala dos ataques abalaram a comunidade internacional, motivando uma "rapid international response" (Herzog, 2011, p.54) (Ciolan, 2014). A Equipa de Resposta a Incidentes de Segurança Informática (CERT)[1] da Estónia recebeu apoio internacional para conseguir restabelecer e manter a sua cibersegurança, de CERT de países aliados, como a Alemanha e a Finlândia, da ENISA e da NATO (Herzog, 2011, p.54) (Schmidt, 2013, p. 13).

No rescaldo dos ataques, a UE e a NATO procuram reforçar urgentemente a sua cibersegurança, através de planos de ação e de cooperação (Herzog, 2011, p. 54-55). Logo em 2008, na Cimeira de Bucareste a NATO define a sua primeira Estratégia de Ciberdefesa (Ciolan p. 127, 2014) e estabelece a Cyber Defence Management Authority (CDMA) em Bruxelas, que funcionou como centro operacional de cibersegurança (Herzog, 2011, p. 54). Ainda em 2008, é estabelecido o Cooperative Cyber Defence Centre of Excellence (CCD CoE), o "cyber-security headquarters" (Herzog, 2011, p. 55). O CCD CoE foi estabelecido precisamente em Tallinn, na Estónia (CCDCOE).

Em 2010, na Cimeira de Lisboa a NATO passa a considerar que "cyber attacks could reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability." (NATO, 2024), em 2011 a NATO elabora a sua segunda Política de Defesa para o Ciberespaço e em 2012, o Processo de Planeamento de Defesa da NATO (NDPP) inclui finalmente a ciberdefesa no seu programa (NATO, 2024). O maior ponto de transformação na política da

[1] As CERT são semelhantes às Equipas de resposta a incidentes de segurança informática (CSIRT), nesta dissertação CERT engloba ambas as designações.

NATO para o Ciberespaço começa na cimeira de 2014, no País de Gales, quando os aliados reconhecem o ciberespaço "as part of NATO's core task of collective defence, which means that a cyber attack could be grounds to invoke Article 5 of NATO's founding treaty" (NATO, 2024).

O artigo 5º afirma que "um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas" (NATO, 1949), qualquer ciberataque a um país aliado merecerá resposta de toda a aliança. Esta ideia foi reforçada na cimeira de Varsóvia em 2016, Jens Stoltenberg, então Secretário-geral da NATO declara num artigo que "Cyberspace is the new battleground and making Nato cyber ready—well-resourced, well-trained, and well equipped—is a top priority" (Stoltenberg 2019, p. 14). Em 2007, as autoridades estónias queriam a aplicação do artigo 5º, contudo era impossível de imputar nequivocamente a responsabilidade dos ataques à Rússia (Hansen & Nissenbaum, 2009) (Herzog, 2011, p. 53). A aplicação do artigo 5º da NATO é a demonstração inequívoca que o Ciberespaço é um meio securitizado por parte da NATO.

Na cimeira de Varsóvia também foi assinada a "Cyber Defense Pledge", onde os países da NATO comprometeram-se a investir e reforçar a sua ciberdefesa, renovada em 2023, na cimeira de Vilnius (NATO, 2024). A cimeira de Bruxelas em 2021 culminou com uma nova política de ciberdefesa, que determinava que a "NATO must actively deter, defend against and counter the full spectrum of cyber threats at all times – during peacetime, crisis and conflict – and at the political, military and technical level" (NATO, 2024). Em 2024, a NATO continua a investir na sua infraestrutura e rede de centros de cibersegurança (NATO, 2024).

A UE "desperta" (Beláz, 2019, p. 21) e entra numa nova fase de abordagem ao Ciberespaço, que se torna uma prioridade estratégica de Segurança europeia (Hermenegildo, 2020, p. 21), para além dos ciberataques sofridos pela Estónia, a crise de 2008 também forçou mudanças na abordagem europeia (Beláz, 2019) (Hermenegildo, 2020). O plano de "Proteção das infraestruturas críticas da informação" (PICI) foi a primeira tentativa da UE para sistematizar a abordagem ao Ciberespaço a nível europeu, mas ainda subjugado às políticas e práticas de cada Estado Membro, o que impediu atingir o ideal de segurança projetado (Hermenegildo, 2020, p.22-23) (Beláz, 2019, p. 21-22).

O Tratado de Lisboa, que entrou em vigor em 2009, foi fundamental para esta evolução

porque aboliu a política de pilares da UE, possibilitando uma abordagem holística à Cibersegurança (Beláz, 2019, p. 22) (Hermenegildo, 2020, p. 23-24). O artigo 69.ºB do Tratado de Lisboa (2007) estabelece ainda que o cibercrime pertence a "domínios de criminalidade particularmente grave com dimensão transfronteiriça", onde a UE tem força legislativa para "estabelecer regras mínimas" (UE, 2007) (Beláz, 2019, p. 22).

Em 2013 surge a "Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido", que estabelece as prioridades estratégicas da UE:

- Garantir a resiliência do ciberespaço;
- Combater a cibercriminalidade;
- Enquadrar a ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD) e na Política Externa Europeia.
- Investimento na indústria tecnológica (Comissão Europeia, 2013).

Este documento reforçou o papel da ENISA enquanto porta-estandarte da cibersegurança europeia, a agência ficou responsável de criar uma rede de CERT de Estados membros, educar os membros sobre ciberdefesa e estabelecer os parâmetros mínimos de cibersegurança na Europa, entre outras responsabilidades (Beláz, 2019, p. 22-23). Contudo, a Estratégia que a Comissão pretendia implementar só é atingida com a Diretiva de Segurança das Redes e da Informação (SRI) de 2016 (Hermenegildo, 2020, p. 24) (Beláz, 2019, p. 24). Para Beláz (2019), a SRI marca o começo da abordagem atual de ciberdefesa europeia, a autora classifica-a como a fase Centralizadora (p. 23). A SRI é a "first piece of EU-wide cyber legislation " (Beláz, 2019, p.23), e estabeleceu as regras que os Estados membros tinham de seguir, como a obrigação de ter uma CERT nacional, o investimento nas TIC e garantir a proteção das instituições mais importantes (Beláz, 2019, p.23).

Nesta fase, tal como aconteceu com a NATO, a UE securitiza efetivamente a Cibersegurança, a resiliência do Ciberespaço europeu é uma prioridade estratégica, como ficou claro com o contínuo reforço de medidas preventivas, nomeadamente a criação da CERT-UE, com carácter permanente (Beláz, 2019, p.23) (Consilium, 2024). Em 2022 esta ideia foi reforçada quando a SRI 2 entrou em vigor em finais de 2022 (Consilium, 2024), com o objetivo de

estabelecer "medidas que visam a consecução de um elevado nível comum de cibersegurança na União, com vista a melhorar o funcionamento do mercado interno" (Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, 2022).

A UE e a NATO são duas organizações que procuraram fortalecer a sua posição no ciberespaço através da cooperação, destacando-se o acordo de 2016, com mais de 40 medidas dedicadas a combater ciberameaças (NATO, 2024).

A ONU continuou a ter o GGE como principal "órgão" para a discussão de Cibersegurança, após os ataques à Estónia o grupo voltou a reunir-se em 2009, o primeiro encontro desde 2005 (Tiirmaa-Klaar, 2021). O relatório foi finalizado em 2010, e apesar de ter sido um relatório pouco extenso, contribuiu para reabrir o diálogo e para trazer a discussão da Ciberdefesa para o 1º Comité da ONU (Tiirmaa-Klaar, 2021, p. 5).

O relatório de 2012-2013 é ainda mais impactante, uma vez que "It claims that international law, and in particular the UN Charter as well as the Universal Declaration of Human Rights, apply in cyberspace" (Tiirmaa-Klaar, 2021, p. 5). Este ponto, reviveu o ponto de disputa sobre um Código de Conduta para o Ciberespaço, entre a Rússia e os Estados Unidos (p. 5-6). A Rússia, com apoio da China, queria um Código de Conduta, juridicamente vinculativo, de forma a terem mais controle sobre o ciberespaço, enquanto os países ocidentais eram contra por temerem um controlo exagerado de estados autocráticos sobre a Internet (p. 5-6). Apesar do clima de ligeira tensão, Putin e o presidente Obama conseguiram estabelecer um grupo de trabalho entre Rússia e EUA (Tiirmaa-Klaar, 2021, p. 9).

O relatório de 2015 é para Tiirmaa-Klaar (2021, p.6) o "gold standard for setting boundaries of state behavior in cyberspace through its eleven non-binding voluntary peacetime norms for responsible state behavior", pois estabeleceu os moldes em que os Estados devem interagir e cooperar no ciberespaço. O relatório de 2015 deixava algum espaço para consensos mais abrangentes nas reuniões de 2017, mas tal não aconteceu e o relatório foi um falhanço (Tiirmaa-Klaar, 2021, p. 6-7).

O falhanço do 5º encontro do GGE e a tensão entre o Ocidente e a Rússia, levaram a que em 2018 existissem 2 resoluções concorrentes na ONU relacionadas com o ciberespaço (Tiirmaa-Klaar, 2021, p. 7). A resolução proposta pela Rússia pretendia que fosse criado um grupo de

discussão para o Ciberespaço, o Open-Ended Working Group (OEWG) para a evolução no domínio da informação e das telecomunicações no contexto da segurança internacional, mas que ao contrário do GGE, estivesse aberto a qualquer membro da ONU (p. 7). A resolução proposta pelos EUA propunha um novo GGE em que os países participantes discutem as questões das TIC e cibersegurança em separado das questões de aplicação do Direito Internacional, cujas conclusões seriam anexadas ao relatório, de forma a conseguir atingir um consenso (Tiirmaa-Klaar, 2021, p. 7).

As potências ocidentais temiam que o "OEWG would become a battlefield between two different visions of the future of cyberspace, democratic and autocratic" (Tiirmaa-Klaar, 2021, p. 7), e criou dúvidas por uma questão de execução, de como seria possível compatibilizar calendários para os países que participassem em ambos os grupos, mas mesmo com as dificuldades impostas pela pandemia, tal acabou por não ser um problema e tanto o GGE como OEWG publicaram relatórios em 2021 (p. 7-8). Os dois relatórios podem ser considerados um sucesso, nomeadamente o GGE "where all parties to negotiations felt that they had won something" (Tiirmaa-Klaar, 2021, p. 8).

Concluindo, é possível apontar para os ataques à Estónia em 2007 como o ponto de viragem da securitização do ciberespaço. Até 2007, a cibersegurança era discutida a um nível técnico e auxiliar a outras seguranças mais importantes, nomeadamente com crimes económicos como a fraude. Os ciberataques à Estónia forçaram as principais organizações internacionais a olhar para o ciberespaço como um meio que precisa de ser securitizado e por ser vital para a Segurança Nacional.

Capítulo II. A Cultura Estratégica da Rússia

Neste capítulo procura-se explicar a cultura estratégica russa e de que forma esta permeia para o ciberespaço. A cultura estratégica contextualiza "how government officials understand the world" e como isso afeta o seu processo de tomada de decisão (Götz & Staun, 2022, p. 483). Um líder como Putin pode ter a capacidade de "adjust and, within limits, reshape particular narratives" (Götz & Staun, 2022, p. 483), mas a sua atuação é condicionada pela cultura estratégica.

As linhas culturais estraégicas da Rússia

Como referido anteriormente, o conceito de cultura estratégica ganha especial relevância depois de Snyder (1988), que contrasta o comportamento dos decisores políticos soviéticos com o processo de decisão americano, afirmando que "os decisores soviéticos não são estrategos, mas burocratas" (Romana, 2016, p. 16). Por sua vez, Maltez (1993) afirma que a "visão de encerclement", ou seja, a desconfiança perante os seus vizinhos e outras potências, define a estratégia da "Rússia czarista, soviética e pós-soviética" (Romana, 2016, p. 23).

Romana (2016), coloca a geografia, "Topos", no centro da cultura estratégica russa, ao contrário da americana focada na moralidade, "Ethos", e da chinesa centrada no "tempo", "Cronos". Romana (2016) define esta geografia como

> o espaço transeslavo e ortodoxo, que tem em Moscovo a "Terceira Roma", tutelar, que dá coerência a uma geografia imaginada, à "russkaya ducha" – a alma russa, e a uma "geosofia" primordialista, nas palavras de Troubetzkoy, definidora de uma topogénese que orienta o destino dos povos que ocupam o espaço euro-asiático. (p. 23)

Götz e Staun (2022) identificam duas linhas principais da cultura estratégica russa, a primeira é o sentimento de vulnerabilidade, e a segunda linha refere-se ao "feeling of entitlement to great power status" (p.483). Estas duas linhas estão interligadas, a Rússia vê-se como uma superpotência capaz de ser "um contra poder aos EUA" (Romana, 2016, p. 24), contudo as potências ocidentais, seja os EUA ou a UE, ameaçam o seu controlo sobre os territórios ex-URSS, a tradicional esfera de influência russa (Götz & Staun, 2022).

O sentimento de vulnerabilidade a um ataque externo é "o resultado da confluência de um

processo geohistórico fortemente assente num mito fundador de defesa face às permanentes tentativas de ocupação por partes de poderes hegemónicos" (Romana, 2016, p. 24). Nesta afirmação podemos identificar as "four interrelated narratives" Götz & Staun (2022, p.484) presentes nesta linha da cultura estratégica russa, a grande dimensão territorial, a invasões sofridas ao longo da história, as guerras do passado e a influência ocidental na sua esfera de influência.

No fator geográfico, a dimensão territorial da Rússia é uma força geoestratégica, mas também uma possível fraqueza porque, a sua extensão "makes it difficult to defend all of the country, everywhere, at the same time" (Götz & Staun, 2022, p. 484).

Figura 6. "Heartlandic Russia and Periphery: Major Geopolitical Features" (Cohen, 2014, p. 235)

No vetor histórico, as invasões sofridas fazem parte da "collective memory" russa (Götz & Staun, 2022, p. 484), e por isso a defesa das fronteiras é um elemento fundamental do pensamento estratégico russo. Neste sentido, a procura de "profundidade geoestratégica" (Romana, 2016, p. 24) é essencial, nomeadamente através de buffer zones que impeçam uma ameaça imediata às fronteiras russas (Götz & Staun, 2022, p. 484).

A terceira narrativa refere-se às guerras disputadas com adversários ocidentais, particularmente com a França no século XIX e a Alemanha nazi no século XX, que marcharam

sobre solo russo, mas também a disputa com os EUA durante a Guerra Fria (Götz & Staun, 2022, p. 484). A quarta narrativa refere-se à ameaça que as potências ocidentais representam ao regime político russo e à esfera de influência russa, nomeadamente através de "machinations and color revolution techniques to remove pro-Russian leaders in other states, particularly in the post-Soviet region" (Götz & Staun, 2022, p. 485).

A segunda linha da cultura estratégica russa é "a narrativa de Grande Potência em reformulação" (Romana, 2016, p. 24), que procura recuperar o estatuto de Superpotência após a queda da URSS. A ambição russa é de se estabelecer como uma superpotência, que consiga concorrer com o Ocidente e não ser apenas uma potência regional (Götz & Staun, 2022, p. 485) (Romana, 2016). No entanto, o primeiro passo para atingir este estatuto passa por estabelecer o seu poder sobre aquela que é a sua tradicional esfera de influência, ou seja, o antigo espaço soviético (Götz & Staun, 2022, p. 485-486) (Romana, 2016).

Romana (2016) afirma que o conflito com a Ucrânia demonstra as "componentes essenciais da cultura estratégica da Rússia: a interdependência das vulnerabilidades; uma concepção messiânica da posição da Rússia no espaço religioso ortodoxo (Moscovo como a Terceira Roma) combinada com o eurasianismo; e uma interpretação parabellum das relações internacionais" (p. 24). Götz e Staun (2022) concordam com a ideia de que este conflito resulta sobretudo da cultura estratégica da Rússia, e não apenas da ideologia pessoal de Putin sobre a Ucrânia (p. 491-492).

No que diz respeito às narrativas geohistóricas, a Ucrânia foi um dos pontos de entrada dos exércitos franceses e alemães no território russo, e Kiev é "the historical epicenter and cradle of Russian civilization" (Götz & Staun, 2022, p. 486), algo que fica claro num artigo em que Putin cita Oleg, "Let it be the mother of all Russian cities “(Putin, 2021), referindo-se a Kiev.

O sentimento de vulnerabilidade em relação ao ocidente também está presente, porque a anexação da Crimeia e subsequente invasão de 2022 resultaram das lideranças pró-ocidente ucranianas, que surgiram após a revolução de 2013-14 que depuseram um governo pró-russo (Götz & Staun, 2022, p. 487). Uma possível adesão ucraniana à UE, e posteriormente à NATO, são vistos pela Rússia não só como uma possível ameaça securitária às fronteiras russas, algo várias vezes reforçado por Putin (Götz & Staun, 2022, p. 489), como também um "desrespeito" ao estatuto de superpotência da Rússia, porque nenhuma superpotência vai

permitir que interferência na sua esfera de influência.

Desta forma, a invasão da Ucrânia também explicita o segundo fio da cultura estratégica russa, a aproximação do Ocidente à Ucrânia é vista como um desafio ao estatuto da Rússia enquanto superpotência, um desafio que à luz dos princípios da cultura estratégica é "legitimador do alargamento da profundidade geostratégica [sic] da Rússia e da tentativa de preservar influência no “near-abroad” "(Romana, 2016, p. 24).

Os ataques à Estónia, mesmo que não tenham uma ação direta do estado russo, também demonstraram a importância que a história e o espaço que pertencia à URSS têm na cultura russa. Ainda antes dos ciberataques, a Estónia foi palco de manifestações por parte da minoria étnica russa que viram a deslocação da estátua como “a threat to their cultural and political status” (Hansen & Nissenbaum, 2009, p. 1169).

A Estónia, antiga república soviética, mover um monumento que glorifica o Exército Vermelho, significa um desrespeito à história russa por parte de um país da esfera da sua esfera de influência.

Cultura Estratégica no Ciberespaço

O ciberespaço é único, sem fronteiras como as planícies da Ucrânia que foram o ponto de entrada de invasões no passado, mas como observamos com os ataques à Estónia, tal não significa que não existem ameaças a "superar" e fragilidades a "colmatar" (Ribeiro, 2009, p. 16). A cultura estratégica é uma força que afeta e influencia a estratégia integral de um Estado e por permear todos os setores e espaços estratégicos, incluindo o ciberespaço.

O sentimento de vulnerabilidade à ameaça externa não desaparece no ciberespaço (Kari, 2019, p.75), tal como não desaparece a ambição russa de ser uma superpotência, neste caso uma ciberpotência, não só num sentido "defensivo" dentro da sua esfera de influência, mas também num sentido ofensivo, onde procura expandir a sua influência.

Como observado no capítulo anterior, a superioridade tecnológica causa apreensão aos líderes russos desde finais da década de 90, e por isso a Rússia teve iniciativa em discutir a segurança no ciberespaço na ONU. Os ataques à Estónia com suposta ação russa, e a utilização de ciberataques nos conflitos com a Geórgia (2008) e a anexação da Crimeia,

deram à Rússia um estatuto de ciberpotência, pelo menos aos olhos da maioria dos observadores. Contudo, segundo Kari (2019) o atraso tecnológico que a Rússia tem em relação a outras grandes potências, nomeadamente os EUA, é o maior desafio da cibersegurança russa, e por consequência "this gap strengthens the Russian perception of its strategic vulnerability in cyberspace" (p. 76).

O sentimento de vulnerabilidade não nasce apenas da inferioridade em relação às potências ocidentais, existe também o risco de ameaças internas que coloquem em causa o regime atual, risco exponenciado pela popularidade das redes sociais que são pontos de mobilização importantes da população, como aconteceu na Primavera Árabe (Kari, 2019, p.78). Apesar do controlo exercido sobre a internet, esta continua a ser um espaço onde as pessoas têm mais liberdade sobre a informação e entretenimento que consomem, "since the early 2010s, Internet users have organised political meetings and protests, exchanged actual information, taken a stand against fake news, hosted free discussions about politics and social issues, developed new ethical guidelines" (Konradova, 2020, p. 56).

Apesar deste capítulo ter sido mais curto, este cumpriu o objetivo de providenciar o contexto necessário para compreendermos a ação dos decisores políticos e as suas prioridades securitárias no ciberespaço. Apesar da influência da cultura estratégica russa no ciberespaço tornar-se mais óbvia no próximo capítulo, a esquematização Figura 7. é demonstrativa

Figura 7. A Cultura Estratégica no Ciberespaço (Kari, 2019, p. 77)

A cultura estratégica não é determinista e inamovível, mas possui uma inércia que move os

decisores políticos no sentido de priorizar aquelas que são as linhas condutoras da cultura estratégica. No caso da Federação Russa estas linhas são o sentimento de vulnerabilidade, ou seja, a defesa da sua soberania contra a ameaça externa, e o estatuto de superpotência mundial, a ambição de ser respeitado pelas outras grandes potências (Romana, 2016, p. 24).

Capítulo III. O Conceito de Estratégia de Segurança Nacional da Rússia

Neste capítulo, acompanha-se o processo russo de securitização do Ciberespaço, através da análise da evolução do Conceito de Segurança Nacional (CESN), da Doutrina de Segurança das Informações (ISD) e outros documentos relevantes, para finalmente compreender a importância do ciberespaço no Conceito atual de Estratégia de Segurança Nacional da Federação Russa.

A evolução do Conceito de Segurança Nacional e da Doutrina de Segurança das Informações

Em 1997 é finalmente publicado o primeiro CESN[2], por decreto presidencial de Yeltsin, definido como

> a political document reflecting the aggregate of officially accepted views regarding goals and state strategy in the sphere of ensuring the security of the individual, society, and the state from external and internal threats of a political, economic, social, military, man-made [tekhnogenyi], ecological, informational, or other nature in the light of existing resources and potential (Federação Russa, 1997)

Este documento também "formulates key directions and principles of state policy" (Federação Russa, 1997) e funciona como "the basis for the elaboration of specific programs and organizational documents in the sphere of ensuring the national security of the Russian Federation" (Federação Russa, 1997).

O CESN1997 foi antecedido por publicações de outros documentos importantes como o "Conceito de Política Externa da Federação Russa" e a "Doutrina Militar da Federação Russa", ambos em 1993, mas não deixa de ilustrar a desorientação estratégica pós-colapso da URSS, que tenha demorado 6 anos a estabelecer a Estratégia de Segurança Nacional (Godzimirski,

[2] A tradução utilizada traduz o título para “Russian National Security Blueprint” em vez de “Russian National Security Concept”, contudo “Concept” (Conceito) é a tradução mais correta e aceite.

2000, p. 76) (Fânzeres, 2014).

O CESN está dividido em 4 seções principais, o primeiro define o papel da Rússia na Comunidade Internacional, o segundo aborda os interesses nacionais russos, o terceiro ponto aborda as ameaças securitárias e por fim define-se tarefas para assegurar a Segurança Nacional russa (Godzimirski, 2000, p. 77). Neste documento, e apesar de ser o último ponto, a esfera de informações (EI) já é considerada como um dos interesses nacionais, onde o Estado deve garantir as liberdades e direitos dos cidadãos, nomeadamente o direito a "to receive reliable information", enquanto assegura "the protection of national spiritual values; the propagandization of the national cultural heritage, ethical norms, and public morality" (Federação Russa, 1997). A Rússia pretende investir no desenvolvimento tecnológico, e ser "one of the centers of world development in the 21st century" (Federação Russa, 1997).

As ameaças securitárias dividem-se em cinco tópicos principais, econômicos, "inter-ethnic relations", polarização social, internacionais e de Defesa (Federação Russa, 1997). Apesar da EI não estar discriminada nesta lista, é estabelecido que é do interesse nacional que "the state's information assets must be protected against" (Federação Russa, 1997). O documento conclui que as principais ameaças "right now and in the foreseeable future do not have a military orientation and are of a predominantly internal nature and are concentrated in the domestic political, economic, social, environmental, information, and spiritual spheres" (Federação Russa, 1997).

Em relação à salvaguarda da Segurança Nacional, o CESN1997 define cinco tarefas essenciais para garantir a segurança da EI:

- the establishment of the requisite balance between the need for the free exchange of information and permissible restrictions on its dissemination;
- the improvement of the informational structure, the acceleration of the development of new information technologies and their widespread utilization, and the standardization of systems for the retrieval, collection, storage, processing, and analysis of information taking account of Russia's becoming part of the global information infrastructure;
- the formulation of an appropriate statutory legal base and the coordination --

with the Federal Government Communications and Information Agency Under the Russian Federation President playing the leading role -- of the activity of federal organs of state power and other organs resolving information security tasks;

- the development of the Russian telecommunications and information systems industry and the priority dissemination of these systems on the domestic market in comparison with foreign counterparts;

- the protection of state information assets [resurs], primarily in federal organs of state power and at defense complex enterprises. (Federação Russa, 1997)

Neste documento fica ainda estabelecido que o Conselho de Segurança da Federação Russa será o órgão responsável por "examinar" os problemas da EI, e "coordinates the activity of the system for safeguarding the Russian Federation's national security" (Federação Russa, 1997), que inclui a EI.

No CESN1997, das três modalidades de segurança identificadas por Hansen e Nissenbaum (2009), só as práticas de segurança quotidianas estão presentes, sob forma da construção do quadro legal para a EI. A tecnicidade está presente de forma indireta, no sentido em que o CESN1997 pretende que a indústria de informação seja desenvolvida. A hipersecuritização está completamente ausente, não existe nenhuma indicação de urgência na segurança da EI, não é uma prioridade estratégica.

Em setembro de 1998, a Rússia submente uma proposta que pode ser considerada como a primeira demonstração securitária em relação às TIC, por parte de uma grande potência no panorama internacional.

Neste documento, a Rússia afirma que é importante ter uma atitude preventiva e discutir ameaças que “for the time being only potential but nevertheless serious” (Federação Russa, 1998, p. 2). Apesar de não ser denominado como ciberespaço, a Rússia avisa que este é “a fundamentally new area of international confrontation” (p. 2) e do possível desenvolvimento de uma “information weapon, the destructive “effect” of which may be comparable to that of weapons of mass destruction” (p. 2). Para além de conflitos entre países, neste documento também se refere ao uso de “information resources may be used for terrorist or criminal

purposes" (Federação Russa, 1998, p. 2). Esta proposta difere do CESN1997, porque nestespontos observamos hipersecuritização, nomeadamente quando se compara uma "information weapon" (Federação Russa, 1998, p. 2) a uma arma de destruição maciça.

A Rússia propõe que a ONU facilite a discussão e a cooperação internacional da evolução das TIC entre as principais potências e outros autores que estiverem interessados, o que foi conseguido com a criação do GGE em 2004, que já foi discutido anteriormente. Sendo um novo fenómeno, num novo espaço, também foi estabelecido como prioritário a "definition of the concepts "information weapon", and "information war", and other hostile or unsanctioned use of information and telecommunications systems and information resources" (Federação Russa, 1998, p. 4). A definição destes conceitos é importante para outro objetivo da proposta russa, que é a criação de um quadro legal "to prohibit the development, production or use of particularly dangerous forms of information weapons, and of taking measures to combat information terrorism and crime" (Federação Russa, 1998, p. 4). Nestes pontos observamos o fator de tecnicidade identificado por Hansen e Nissenbaum (2009), porque a Rússia pretende recorrer a especialistas da TIC para construir o quadro legal e conceptual do ciberespaço.

A linguagem desta proposta também é bastante interessante, principalmente compreendendo não só o contexto geopolítico, poucos anos depois do fim da URSS, mas também a cultura estratégica russa, nomeadamente do sentimento de vulnerabilidade. Em pouco mais de uma página de texto, Ivanov utiliza quatro vezes palavras relacionadas com "concern" (preocupação) (Federação Russa, 1998, p. 3), destaca-se ainda o uso de "anxiety" (ansiedade) (p. 3) para descrever o sentimento russo perante às ameaças das TIC. Neste ponto é referida a "scale" (Federação Russa, 1998, p. 3) deste novo espaço, o que nos permite fazer um paralelismo com o sentimento de vulnerabilidade que a Rússia tem em relação às suas fronteiras físicas, em grande parte devido à sua extensão.

Em agosto de 1999, Yeltsin nomeia para primeiro-ministro Vladimir Putin, então Secretário do Conselho de Segurança e chefe do Serviço Federal de Segurança (FSB), um dos órgãos que sucedeu ao KGB (Trenin, 2019) (Fânzeres, 2014). Putin foi escolhido tendo já em vista a sucessão de Yeltsin, que já tinha problemas de saúde para além de problemas políticos, nomeadamente a guerra da Chechénia (Trenin, 2019). A questão da chechena desgastou

Yeltsin, mas fortaleceu Putin que ganhou bastante popularidade pela forma que lidou com o conflito (McFaul, 2001, p.362), e a 31 de dezembro de 1999 Yeltsin abdica, deixando Putin no poder interinamente (Trenin, 2019). O ano de 2000 que marca uma mudança de paradigma na Rússia (Fânzeres, 2014, p.63-64), ainda antes das eleições que consagraram Putin como presidente, é estabelecido um novo CESN e é publicada a primeira "Doutrina de Segurança da Informação da Federação Russa" (ISD).

O novo CESN é assinado por Putin a 10 de janeiro de 2000, ainda como Presidente interino, o que leva a que o documento seja mais uma revisão do CESN1997 do que uma remodelação estratégica à imagem do novo presidente (Godzimirski, 2000, p. 78).

O CESN2000 é definido como “a system of views on ensuring the security of the individual, society and the state from external and internal threats in all spheres of life in the Russian Federation. The Concept formulated the key directions of the state policy” (Federação Russa, 2000a). Em adição à definição do Conceito, no preâmbulo do CESN2000 define-se Segurança Nacional como “the security of its multinational people as the bearer of sovereignty and the only source of power in the Russian Federation” (Federação Russa, 2000a) (Godzimirski, 2000, p. 77).

As revisões "reflect the experiences and conclusions of the two years separating the two texts" (Godzimirski, 2000, p. 78), nomeadamente o conflito da Chechénia, a crise económica russa e as tensões com a NATO (Godzimirski, 2000, p. 78). Godzimirski (2000) destaca o conflito do Kosovo e o alargamento da NATO como os principais fatores de preocupação para Rússia em relação ao Ocidente (Godzimirski, 2000, p. 78), mas para este trabalho importa referir as revisões feitas em relação à EI.

No CESN2000, os interesses nacionais na EI mantêm quase todos do Conceito de 1997, à exceção do ponto sobre a proteção cultural (Federação Russa, 2000a). Contudo esta é uma pequena diferença quando comparada com a secção das Ameaças, que no CESN1997 agrupavam as ameaças da EI num conjunto de possíveis ameaças internas, apenas referidas numa frase. No CESN2000, na secção das ameaças a EI tem direito ao seguinte parágrafo:

> There are growing threats to the national security of the Russian Federation in the information sphere. There is a major threat in the striving of some countries to

> dominate the world information space and oust Russia from the foreign and domestic information market; the elaboration by some countries of a concept of information wars, which provides for the creation of means of dangerous influence on the information spheres of other world countries; the disruption of the normal operation of the information and telecommunication systems and of the safety of the information resources, as well as attempts to gain unwarranted access to them. (Federação Russa, 2000a)

Neste parágrafo estão reforçadas as ideias da carta submetida na ONU em 1998, ou seja, o sentimento de vulnerabilidade em relação aos avanços tecnológicos na EI, nomeadamente dos países que têm uma superioridade tecnológica em relação à Rússia. Também é possível identificar outro fator diferenciador, em 1997 a preocupação centrava-se em fatores internos, enquanto neste parágrafo o foco está na ameaça externa, tanto numa possível "information war", como na possível influência externa à EI russa.

Esta mudança de postura também está presente na consolidação das tarefas para assegurar a segurança na esfera de informações, que em 1997 eram cinco e no CESN2000 passam a três:

- to implement the constitutional rights and freedoms of the citizens of the Russian Federation in the sphere of information;
- to improve and protect the national information infrastructure and integrate Russia into the world information space;
- to counter the threat of the development of rivalry in the information sphere (Federação Russa, 2000a)

Os primeiros dois pontos consolidam quatro das cinco prioridades de 1997, a questão dos direitos dos cibernautas e da evolução tecnológica, enquanto o terceiro ponto expande a quinta prioridade de 1997, e adaptada à visão do documento.

Em 1997, o quinto ponto referia-se à "protection of state information assets" (Federação Russa, 1997), que no segundo o documento eram "predominantly internal nature and are concentrated in the domestic" (Federação Russa, 1997), enquanto no CESN2000 observa-se

que existe a questão da "rivalidade", ou seja só pode ser relativo a uma ameaça externa, porque seguindo uma interpretação clássica das relações internacionais e da ciência política, um Estado soberano só pode ser rivalizado por outro Estado soberano (Lara, 2015). No entanto, esta referência a rivalidade não é muito vincada, por isso volta a não existir hipersecuritização neste CESN. A tecnicidade e as práticas de segurança quotidiana continuam presentes a um nível semelhante ao CESN1997.

A 9 de Setembro de 2000, o já eleito Presidente Vladimir Putin aprova a primeira "Doutrina de Segurança das Informações", redigida pelo Conselho de Segurança da Federação Russa (Boudarina, n.d.). O documento está dividido em quatro capítulos, o primeiro explora os pontos gerais de Segurança na EI já destacados no CESN2000, o segundo foca-se nos métodos para assegurar a Segurança, o terceiro capítulo enumera as principais medidas para realizar a política de segurança, e o último capítulo aborda a base organizacional russa para a Segurança das Informações (Federação Russa, 2000b).

No preâmbulo fica explícito que esta Doutrina explora o CESN2000 na EI, servindo de base para "shaping government policy on information security in the Russian Federation; preparing suggestions to improve the legal, procedural, scientific-technical and organizational framework for ensuring information security in the Russian Federation; devising targeted national information security programs" (Federação Russa, 2000b).

O primeiro capítulo explora os pontos discutidos no CESN2000, mas antes de começar a discutir os interesses nacionais russos, o documento define EI como "an assemblage of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, and a system governing public relations arising out of these conditions" (Federação Russa, 2000b). A EI é ainda descrita como um "system-forming factor of societal life" (Federação Russa, 2000b), que abrange várias áreas da segurança nacional russa, e que com o avanço das TIC vai ganhar cada vez mais preponderância securitária (Federação Russa, 2000b).

A Doutrina define ainda "information security" como "the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state" (Federação Russa, 2000b). Se os documentos anteriores securitizavam tacitamente, na ISD2000 a securitização da EI é

explícita.

No que diz respeito aos interesses russos na EI, a ISD2000 divide-os em três níveis diferentes: os interesses pessoais de cada um cidadão, os interesses da sociedade, e por fim os interesses do Estado (Federação Russa, 2000b). Estes níveis enquadram-se perfeitamente na perceção da Escola de Copenhaga explorada anteriormente, os interesses pessoais correspondem aos problemas não-politizados, os da sociedade aos politizados e os do Estado aos securitizados.

Entre os interesses nacionais, a ISD destaca "four ingredients" (Federação Russa, 2000b):

- Garantir as liberdades e direitos dos cidadãos, e a preservação da cultura e identidade russa na esfera das informações;
- Publicitar as políticas do Estado, para que qualquer pessoa tenha acesso livre e fiável à "state policy of the Russian Federation and about its official position on socially significant events" (Federação Russa, 2000b);
- Promover inovações da TIC e o reforçando a indústria tecnológica da Rússia;
- Proteger os sistemas de informações e telecomunicações, e promover a cooperação internacional “against the threat of rivalry" (Federação Russa, 2000b).

Esta lista não adiciona substancialmente aos interesses identificados no CESN1997 e 2000, mas interessantemente inclui a ideia de defesa da identidade nacional e da "spiritual renewal of Russia" (Federação Russa, 2000b), que está ausente do Conceito de 2000, mas presente em 1997. No primeiro ponto reforça-se a ideia de garantir os direitos e liberdades dos internautas e de criar um quadro legal. O segundo ponto é talvez o mais diferente, porque demonstra a vontade do Estado russo em estabelecer uma presença ativa no ciberespaço. No terceiro ponto é reforçada a intenção de investir nas TIC, com o objetivo de tornar a Rússia numa ciberpotência. O quarto ponto faz a ligação entre a ideia de proteção de informações relevantes nas diversas áreas de segurança do CESN1997, e a ideia de rivalidade introduzida no CESN2000.

Estes quatro interesses correspondem a quatro tipos de ameaças:

- Ameaças aos direitos e liberdades dos cidadãos e "to Russia's spiritual revival" (Federação Russa, 2000b);
- Ameaças "to information support to Russian Federation state policy" (Federação Russa, 2000b);
- Ameaças ao desenvolvimento das TIC e à indústria tecnológica da Rússia;
- Ameaças à segurança dos sistemas de informação e comunicação.

No primeiro ponto, destaca-se a importância que a ISD dá ao controlo dos meios de comunicação, alertando para o perigo não só de influência externa na esfera russa, mas também do "establishment of monopolies on forming, receiving and disseminating information in the Russian Federation with the use of telecommunication systems or otherwise" (Federação Russa, 2000b). O segundo ponto reforça a ideia de que o Estado deve controlar esta esfera, e que os meios de comunicação do Estado não devem ser impedidos de informar o público sobre a sua política (Federação Russa, 2000b).

No terceiro ponto destaca-se a reprovação de "purchases of imported means of informatization, telecommunication and communication by government bodies" (Federação Russa, 2000b), e a ameaça da fuga de cérebros para o estrangeiro. No quarto ponto, as ameaças enumeradas estão associadas principalmente ao acesso indevido a informações privadas, à proteção das informações de segurança dos estados e uso indevido da tecnologia, e não com ciberataques (Federação Russa, 2000b).

A ISD divide as ameaças em ameaças de natureza interna e externa, (Federação Russa, 2000b). A nível interno, o ponto fundamental é o controle do Estado sobre a EI, o Estado deve ser capaz de manter a ordem, através de um quadro legal que não dê espaço à atividade criminosa. A capacidade económica e financeira do Estado também é fundamental para manter a segurança e garantir que a Rússia não "lag behind the world's leading countries in level of informatization" (Federação Russa, 2000b).

A nível externo, a ISD2000 reforça as ameaças identificadas na proposta à ONU, em 1998, referindo a crescente competição nas TIC, organizações terroristas, e o "development by a number of states of information war concepts that provide for creating means for dangerous

attack on the information spheres of other countries of the world" (Federação Russa, 2000b).

O Capítulo I termina com a identificação dos principais desafios para assegurar a segurança de informações e o estado desta no ano 2000. A ISD2000 destaca uma evolução positiva na segurança na EI, "Yet analysis of the state of information security in the Russian Federation shows that its level is not fully consistent with the requirements of society and the state" (Federação Russa, 2000b).

O documento descreve as dificuldades de encontrar o equilíbrio entre as liberdades dos cidadãos e o controlo que o Estado tem de exercer nesta esfera, dificuldade que é agravada pela "immaturity of the legal governance of social relations in the information sphere" (Federação Russa, 2000b). Outra dificuldade identificada é o atraso tecnológico que a Rússia tem perante outras potências, que cria um círculo vicioso, onde para garantir a sua segurança é necessário importar tecnologia estrangeira, o que por sua vez enfraquece a indústria russa Federação Russa, 2000b). A dependência de tecnologia estrangeira, aumenta "the threats of the use of the “information weapon” against the Russian information infrastructure" (Federação Russa, 2000b).

O Capítulo II foca-se nos métodos para assegurar a Segurança, "subdivided into legal, organizational-technical and economic" (Federação Russa, 2000b). O primeiro consiste no desenvolvimento do quadro legal, nomeadamente através de emendas e revisões de leis e tratados internacionais, assim como de novas leis que garantam a segurança na EI; o método técnico-organizacional refere-se ao desenvolvimento tecnológico e técnico do sistema para que o Estado consiga manter a segurança; finalmente, o método económico está relacionado com financiamento dos programas de desenvolvimento de segurança (Federação Russa, 2000b).

No segundo ponto deste capítulo, a ISD2000 explora a relação da EI com outras esferas da sociedade, desde a política externa à "spiritual life" (Federação Russa, 2000b). A esfera económica é a primeira a ser enumerada, destacando-se a necessidade de proteger o sistema de estatísticas estatal e os sistemas bancários e de crédito. De seguida explora-se a ligação à política interna e externa, mantendo as prioridades e preocupações do capítulo anterior. A ciência e tecnologia são outra esfera intimamente ligada à EI, e as preocupações centram-se no desenvolvimento tecnológico, como vimos anteriormente, mas destaca-se a preocupação

com "the policy of western countries aimed at further destroying the unified techno-scientific space inherited from the USSR" (Federação Russa, 2000b). Na esfera da vida espiritual, destacam-se as liberdades e direitos dos cidadãos e a defesa das "languages, moral values and cultural legacy of the peoples and nationalities of the Russian Federation" (Federação Russa, 2000b).

A Esfera da Defesa, dividida entre ameaças internas e externas, que ao contrário das ameaças exploradas no capítulo I, identifica "electronic attacks" (Federação Russa, 2000b) como uma ameaça securitária. As ameaças internas são virtualmente as mesmas identificadas anteriormente, mas o texto deixa o aviso que "internal threats listed here will represent a special danger in conditions of an exacerbation of the military-political situation" (Federação Russa, 2000b).

A esfera judicial e das forças policiais, que também se divide entre ameaças internas e externas. As ameaças externas relacionam-se novamente com a intellegence de outros países, enquanto as questões internas estão relacionadas com as deficiências do quadro legal, da metodologia para lidar com a EI e dificuldades tecnológicas (Federação Russa, 2000b). Neste ponto é estabelecido como prioridade a "creation of a protected multilevel system of integrated databanks of an investigative, reference, criminalistic and statistical nature on the basis of specialized information technology systems" (Federação Russa, 2000b).

A ISD2000 explora ainda a importância da EI em emergências nacionais, porque os serviços de emergência são "the most vulnerable information security facilities" (Federação Russa, 2000b). Desta forma, é fundamental fortalecer a rede de resposta a emergências através do desenvolvimento de sistemas capazes de monitorizar e prever ameaças, e preparados para lidar com situações extremas.

Para concluir o Capítulo II, discute-se a importância da cooperação internacional na EI, repetindo os pontos expostos no CESN de 2000 e na proposta apresentada na ONU. Neste ponto, volta-se a destacar um contexto internacional de "toughened international competition for technological and information resources and for market dominance" (Federação Russa, 2000b), a ameaça do desenvolvimento de uma “information weapon". No que diz respeito à cooperação internacional na EI, a ISD2000 declara que "special attention

should be paid to problems of interaction with the member states of the Commonwealth of Independent States" (Federação Russa, 2000b).

O Capítulo III recapitula os princípios da política de segurança para a EI, e as "urgent measures" (Federação Russa, 2000b) necessárias para realizar esta política. Este capítulo acrescenta pouco ao documento, servindo mais como um resumo do que foi dito anteriormente.

O Capítulo IV, conclui o ISD de 2000 com as funções e elementos principais da base organizacional russa para a Segurança das Informações (Federação Russa, 2000b). Este capítulo reforça as ideias presentes ao longo do documento, contudo a discussão das funções dos elementos do Estado na Segurança da EI é uma novidade relevante, uma vez que no CESN1997 há apenas uma curta referência que às funções do Conselho de Segurança e no Conceito de 2000 não há qualquer informação. Neste ponto, a ISD distribui responsabilidades entre os poderes judicial, legislativo e executivo, enumerando a importância dos diferentes elementos na EI, do Presidente ao cidadão comum (Federação Russa, 2000b).

O Presidente da Rússia é o primeiro elemento enumerado neste capítulo, o chefe de Estado "directs within his Constitutional remit national information security agencies and forces" (Federação Russa, 2000), e define as prioridades estratégicas na política de segurança da EI.

Após o Presidente, a ISD coloca as câmaras da Assembleia Federal da Rússia como responsáveis pela "a legislative base in the realm of national information security" (Federação Russa, 2000b).

O Governo executa a estratégia definida pelo Presidente, estabelecendo orçamentos e coordenando "the activities of federal executive bodies" (Federação Russa, 2000b) na EI, responsáveis por desenvolver "normative legal acts" (Federação Russa, 2000b).

O Conselho de Segurança tem um papel mais preponderante em relação ao CESN1997, é responsável por identificar e analisar as ameaças securitárias e de informar e preparar as decisões do Presidente na EI (Federação Russa, 2000b). O Conselho de Segurança é ainda responsável por toda a implementação da estratégia do Presidente, coordenando as agências de informação e a ação dos órgãos executivos federais (Federação Russa, 2000b).

Num nível inferior ao Presidente, Assembleia Federal e Conselho de Segurança, estão os órgãos executivos federais já referidos, assim como outras comissões especializadas e "bodies of local self-government" (Federação Russa, 2000b). Este conjunto de entidades é fundamental para garantir que existe segurança a nível individual e da sociedade, o que facilitará a garantia da Segurança Nacional (Federação Russa, 2000b). Para garantir que há segurança na EI é necessário que haja "judicial protection" (Federação Russa, 2000b), ou seja que haja o garante dos direitos e liberdades dos cidadãos e das organizações, por parte do poder judicial.

ISD2000 foi o primeiro passo para estruturar e securitizar a EI na Rússia, as ameaças relacionadas com ataques informáticos ganham preponderância na Estratégia de Segurança Nacional e começa-se a definir a Infraestrutura Crítica de Informação (ICI) russa (Kari, 2019, p. 90). Contudo, este documento é "broad and almost all-encompassing" (p. 90), e por isso é difícil compreender quais são ao certo as prioridades estratégicas. O ISD2000 reforça as ideias de defesa de direitos liberdades, desenvolvimento tecnológico e proteção de informações durante todo o documento, mas as ideias são generalistas e no capítulo organizacional, pouco fica claro para além de que o Presidente é claramente o decisor estratégico (Kari, 2019).

A ISD2000 explora muito mais a tecnicidade e as práticas de segurança quotidianas, mas a hipersecuritização continua a não estar presente, seguindo a linha dos CESN anteriores. As ameaças não são referidas com a mesma urgência e “ansiedade” presente na proposta de 1998 à ONU.

No primeiro capítulo desta dissertação discutimos a importância que os ataques sofridos pela Estónia em 2007 tiveram no quadro legal internacional, e o próximo CESN russo só surge em 2009, já depois de uma invasão russa à Geórgia e do fim da segunda Guerra da Chechénia.

O CESN2009 é intitulado “National Security Strategy of the Russian Federation to 2020”, e foi aprovado por decreto presidencial de Dmitry Medvedev, sucessor de Putin, então primeiro-ministro russo (Schröder, 2009). O CESN2009 “is an officially acknowledged system of strategic priorities, goals and measures with regards to domestic and foreign policy, which determine the degree of national security and the level of stable, long-term development of the state" (Federação Russa, 2009). O documento está dividido em seis capítulos, em vez de

quatro como os seus antecessores, o primeiro consiste de disposições gerais, nomeadamente com a definição dos conceitos centrais do documento, definindo-se Segurança Nacional como

> the protection of the individual, society and the state from domestic and foreign threats, which in turn ensures constitutional rights and freedoms, an appropriate quality of life for citizens, sovereignty, territorial integrity and stable development of the Russian federation, the defense and security of the state. (Federação Russa, 2009)

O Capítulo II, que costumava ser dedicado aos interesses nacionais, contextualiza o papel da Rússia no mundo e o fenómeno da globalização (Federação Russa, 2009). A globalização é um ponto de preocupação, desde a crise econômica de 2008, que teve um impacto mundial, às novas ameaças que surgem.

No contexto das novas ameaças, surge a primeira referência ao domínio "cybernetic" (Federação Russa, 2009), o ciberespaço, num documento de Estratégia de Segurança Nacional russo. Nem a ISD2000, nem os CESN anteriores, utilizaram a expressão cyber ou internet, que é referida mais adiante, o discurso esteve sempre centrado na EI. Ainda neste capítulo, prevê-se que "the global information struggle will intensify" (Federação Russa, 2009).

O capítulo seguinte estabelece os interesses nacionais, definidos como "the aggregate of the internal and external needs of the state in ensuring the protection and stable development of the individual, society and the state" (Federação Russa, 2009), e não refere nem o ciberespaço, a internet ou a EI.

No Capítulo IV, acerca da garantia de Segurança Nacional, as Informações e a EI são discutidas no contexto de várias esferas de Segurança, não tendo um ponto "dedicado" de forma exclusiva, ao contrário dos CESN anteriores. No que diz respeito à Defesa refere a importância da tecnologia na prevenção e resposta a ameaças, e o risco apresentado por "high-precision, informational and other high-technology means of conducting armed warfare" (Federação Russa, 2009). Na proteção e promoção da qualidade de vida, volta a referir-se a importância de defender os direitos e liberdades na EI, assim como a cultura russa e "spiritual legacy" (Federação Russa, 2009).

O desenvolvimento das tecnologias de informação e telecomunicação volta a ser um dos pontos referidos no crescimento económico, assim como do sistema de "healthcare" (Federação Russa, 2009), no entanto a esfera de tecnologia e ciência não faz uma única referência à EI. A única referência do CESN2009 à internet ocorre na esfera da cultura, no ponto 83, onde é reforçada a necessidade de preservar a identidade e cultura russa através de apoios governamentais para a produção de "cinematographic and printed works, television and radio programmes and internet resources" (Federação Russa, 2009).

Até agora o CESN2009 não dá o mesmo destaque à EI que o seu antecessor, contudo o Capítulo V é intitulado "Organisational, legal-normative and informational foundations of the realisation fo the given Strategy" (Federação Russa, 2009), no qual as palavras “information" e "informational" surgem quase tantas vezes, 11, que no resto do documento, 12.

O capítulo destaca a o papel de "support" (Federação Russa, 2009) que as "IT", TIC, têm na Estratégia de Segurança Nacional. O uso da expressão IT também é uma novidade, e é utilizado no ponto 108, que avisa para a necessidade "to overcome technological lag in the most important areas of IT, telecommunications, and interconnectivity" (Federação Russa, 2009). No ponto seguinte destaca a importância securitária de proteger a integridade da ICI (Federação Russa, 2009).

O papel auxiliar da EI no CESN2009 contrasta com a securitização, e hipersecuritização, que as potências Ocidentais tiveram após os ciberataques à Estónia, analisada no Capítulo I. A EI até pode ter uma presença maior neste CESN do que em 2000, mas comparando a sua preponderância com o contexto internacional de hipersecuritização, o CESN2009 retira prioridade estratégica à cibersegurança. A perda de urgência securitária pode ser descrita como dessecuritização (Buzan et al., 1998, p. 29), contudo sem uma verdadeira hipersecuritização anterior o conceito não se aplica, não existe dessecuritização numa situação de neutralidade (Hansen & Nissenbaum, 2009).

Apesar de reconhecer que a EI afeta várias áreas de segurança, o CESN continua mais próxima da perspetiva inicial da Escola de Copenhaga (Buzan et al., 1998) e não a nova framework desenvolvida por Hansen & Nissenbaum (2008), na sequência dos ataques à Estónia.

Em 2011, o Ministério da Defesa pública a "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space", que define vários conceitos importantes:

> Information war: confrontation between two or more states in the information space for damaging the information systems, processes and resources, which are of critical importance, and other structures, to undermining the political, economic and social system, and massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party [...]
>
> Information space: area of activity related to the formation, creation, transformation, transmission, use and storage of the information affecting inter alia the individual and social consciousness, information infrastructure and the information per se [...].
>
> International information security: state of international affairs precluding the breach of the global stability and creation of threats for the security of the states and global community in the information space. (Ministério da Defesa da Federação Russa, 2011, p.5)

O documento aplica os princípios da ISD2000 às forças armadas, destacando a importância que a EI tem no "defensive potential of the Russian Federation" (Ministério da Defesa da Federação Russa, 2011, p. 13), o que volta a colocar um foco securitário nesta esfera.

Kari (2019) divide a "cyber threat perception" (p. 89) da Rússia em 3 fases, a primeira é uma fase anárquica e algo confusa e dura até 2012. Na segunda fase, o regime russo foca-se na oposição interna e produz legislação que aumenta o controle sobre o ciberespaço, acabando com a anonimidade dos internautas e aumentando a censura na internet (Kari, 2019, p. 90).

Em 2015, é publicado o novo CESN, já após a anexação russa da Crimeia, que marca a entrada na terceira fase de "cyber threat perception", focada em ameaças externas (Kari, 2019, p.90). O documento mantém a estrutura de 6 capítulos do CESN2009, no Capítulo I segurança nacional é definida como

> the state of protection of the individual, society, and the state against internal and

> external threats in the process of which the exercise of the constitutional rights and freedoms of citizens of the Russian Federation [...], a decent quality of life and standard of living for them, sovereignty, independence, state and territorial integrity, and sustainable socioeconomic development of the Russian Federation are ensured. National security includes the country's defense and all types of security envisioned by the Russian Federation Constitution and Russian Federation legislation – primarily state, public, informational, environmental, economic transportation, and energy security and individual security (Federação Russa, 2015, p.2)

O Capítulo II avalia o papel da Rússia no mundo, e foca-se em grande parte nas tensões russas com o Ocidente, nomeadamente com os EUA, a NATO, a UE, que "are turning Ukraine into a chronic seat of instability in Europe and in the immediate vicinity of Russia's borders" (Federação Russa, 2015, p. 4).

Neste capítulo também existe preocupação sobre "the intensifying confrontation in the global information arena caused by some countries' aspiration to utilize informational and communication technologies to achieve their geopolitical objectives" (Federação Russa, 2015, p. 5), sendo um desses objetivos "conter" a Rússia (p. 3). Ao contrário de 2009, não há qualquer uso de cyber, mas o ponto 21 refere que as TIC promovem "new forms of unlawful activity" (Federação Russa, 2015, p. 5).

O Capítulo III discute os interesses nacionais, definidos como os "objectively significant requirements of the individual, society, and the state with regard to ensuring their protection and sustainable development" (Federação Russa, 2015, p.2), e tal como em 2009, não refere diretamente o ciberespaço, a internet ou a EI.

No capítulo seguinte, acerca da garantia de Segurança Nacional, e tal como em 2009, a EI é discutida no contexto de outras esferas de Segurança. Na Defesa é referida a importância da EI na dissuasão de conflitos armados, reforçando a conceptualização do Ministério da Defesa em 2011 (Federação Russa, 2015, p.7). No que diz respeito à Segurança pública, destaca-se o ponto 43 que aborda as ameaças internas na EI, referindo que as TIC podem ser instrumentalizadas "to disseminate and promote the ideology of fascism, extremism, terrorism, and separatism, and to endanger the civil peace and political and social stability in Society" (p. 9). O ponto 47 volta a fazer referência influence of destructive information from

extremist and terrorist organizations, foreign special services, and propaganda structures" (Federação Russa, 2015, p. 10).

O desenvolvimento da indústria das TIC volta a ser parte integrante das secções relativas à qualidade vida, ao crescimento económico e à saúde pública. Para este desenvolvimento, o CESN2015 estabelece que para além de investimento na indústria, é necessário investir na educação e formação da população, para que o subir "the level of technological security, including in the information sphere" (Federação Russa, 2015, p. 17). A educação do cidadão é uma prática de segurança quotidiana fundamental, porque mobiliza os cidadãos a ser um ator de securitização, criando uma fundação de segurança da EI (Hansen & Nissenbaum, 2009. p.1165).

Na esfera da cultura, volta a repetir-se a importância de preservar a identidade e cultura russa na EI, nomeadamente através duma "state order to create cinematographic and printed output, television and radio programs, and Internet resources" (Federação Russa, 2009, p.22). A internet tem novamente apenas uma referência no documento, e exatamente com a mesma linguagem de 2009. No ponto de "Strategic Stability and Equal Strategic Partnership", a Rússia compromete-se a contribuir para "the formation of a system of international information security" (Federação Russa, 2015, p. 27).

O Capítulo V. volta a estar relacionado com "Organizational, Regulatory-Legal, and Information Foundation" (Federação Russa, 2015, p. 27), contudo este tem apenas sete pontos, em 2009 eram quinze. Este capítulo que era uma novidade do CESN2009, está assim mais consolidado e objetivo, e no ponto 113 estabelece que "in implementing this Strategy, particular attention shall be paid to ensuring information security in light of strategic national priorities" (Federação Russa, 2015, p. 28).

O CESN2015 conclui com os indicadores de Segurança Nacional, e volta a não haver referência à EI, tal como em 2009. Apesar disto, este documento reflete a evolução, aproximando-se à framework de Hansen e Nissenbaum (2009). O documento intensifica os alertas às ameaças na EI, mas prioriza o controlo estatal sobre a internet, não só para combater o cibercrime e influência externa, mas sobretudo para mitigar o crescimento de uma oposição interna (Kari, 2019). Desta forma começa a haver hipersecuritização, mais direcionada às “ameaças” internas, mas também é referida "the intensifying confrontation

in the global information arena" (Federação Russa, 2015, p.5).

Em 2016, é publicada a nova ISD, um texto mais curto que o de 2000, talvez a tentar criar uma Doutrina mais precisa. A ISD2016 está dividida em seis capítulos, as provisões gerais, interesses nacionais, ameaças, objetivos e áreas-chave estratégicas e "institutional framework" (Federação Russa, 2016). No primeiro capítulo define-se EI como

> a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet [...], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere. (Federação Russa, 2016)

"Information Security" é definida como:

> the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development of the Russia Federation, as well as defence and security of the State. (Federação Russa, 2016)

ISD2016 segue os princípios de segurança do CESN2015, contudo os interesses nacionais mantêm-se próximos aos de 2000. O Capítulo II, destaca a importância de garantir os direitos e liberdades dos cidadãos na EI, e da importância de preservar a identidade cultural russa, numa linguagem idêntica à ISD2000. Tal verifica-se nos restantes interesses nacionais, ou seja, o desenvolvimento tecnológico, informar sobre a política do Estado e a cooperação internacional para o desenvolvimento de um sistema de segurança global (Federação Russa, 2016). O interesse nacional que é articulado de uma forma diferente, e mais concisa, é a proteção da ICI russa (Federação Russa, 2016) (Kari, 2019).

No Capítulo III reflete-se sobre a universalização das TIC ser algo positivo, mas que também produz novas ameaças. A Doutrina afirma que existe "growing risk that information technologies will be used to infringe on the sovereignty" (Federação Russa, 2016), da Rússia,

que reforça o sentiment de desconfiança em relação a outros países, e a vontade de estabelecer um quadro legal que regule "inter-State relations in the information space" (Federação Russa, 2016). Para além dos estados, a ISD refere ameaças de origem extremista e terrorista, e ainda destaca "the rise in computer crimes, primarily in credit and financial sphere" (Federação Russa, 2016).

O Capítulo IV da ISD2016 reforça as ideias do Capítulo IV do CESN2015, sobre a importância que a EI tem em outras esferas de Segurança da Rússia. No contexto militar volta a destacar-se o papel de dissuasão de conflitos e de prevenção de ameaças, assim como a importância da proteção das Informações do Estado e da ICI russa (Federação Russa, 2016). Também se volta a explorar a importância que a EI tem para a competitividade dos setores econômicos e tecnológicos russos, e a proteção da sua identidade cultural (Federação Russa, 2016).

O último capítulo mantém a distribuição de competências entre o poder judicial, executivo e legislativo, estabelecida em 2000, assim como o Presidente da Rússia enquanto responsável por determinar "the structure of the information security system" (Federação Russa, 2016). O Banco Central e a Comissão Militar-Industrial da Rússia juntam-se à Assembleia Federal, ao Governo e ao Conselho de Segurança enquanto elementos fundamentais deste sistema (Federação Russa, 2016).

A ISD2016 define pragmaticamente os princípios, as ameaças e os objetivos estratégicos na EI, ao contrário do ISD2000. Este documento também é mais coerente com o CESN em vigor, explorando a importância das práticas de segurança quotidianas para uma fundação de segurança na EI (Hansen & Nissenbaum, 2009), e a necessidade de investir na formação de "cérebros" das TIC (Federação Russa, 2016). A proteção da ICI é o principal fator de hipersecuritização deste documento, que alerta para a necessidade de a proteger "in the event of a direct threat of aggression, and in wartime" (Federação Russa, 2016).

O Conceito atual de Estratégia de Segurança Nacional

A Estratégia de Segurança Nacional da Rússia atual é aprovada por decreto presidencial a 2 de julho de 2021, e caracteriza-se como um

> a basic strategic planning document that defines national interests and strategic

> national priorities of the Russian Federation, goals and objectives of state policy in the field of Ensuring national security and sustainable development of the Russian Federation in the long term. (Federação Russa, 2021, p. 1-2)

No Capítulo I Segurança Nacional é definida como

> the state of protection of national interests of the Russian Federation from external and internal threats, which ensures the implementation of constitutional rights and freedoms of citizens, decent quality and standard of living, civil peace and accord in the country, protection of the sovereignty of the Russian Federation, its independence and national integrity, the socio-economic development of the country. (Federação Russa, 2021, p. 2)

Esta definição é mais concisa que a anterior, não enumera as esferas securitárias mais importantes, onde se incluía a "informational" (Federação Russa, 2015, p. 2), mas mantém os elementos clássicos de Segurança Nacional (Ribeiro, 2009).

O Capítulo II analisa o papel da Rússia no mundo, partindo da ideia de que o contexto internacional está em transformação devido ao desenvolvimento de novas potências (Federação Russa, 2021, p. 3). Um novo contexto pode trazer oportunidades para a Rússia, contudo o Ocidente vai querer manter a sua hegemonia, e tem-se verificado "increasing instability in the world" (Federação Russa, 2021, p. 3).

Uma nova ordem mundial produz novas ameaças e instabilidade, como fica claro no ponto 17, que afirma: "The danger of armed conflicts escalating into local and regional wars, including those involving nuclear powers, is growing. Space and information space are being actively explored as new spheres of warfare" (Federação Russa, 2021, p. 5). Neste ponto destaca-se o uso de "information space" em vez de esfera de informações, uma constante desde 1997. O CESN2021 afirma ainda que se pretende isolar a Rússia, nomeadamente através de "Information campaigns" (Federação Russa, 2021, p. 6) que mancham a imagem russa.

O Capítulo III enumera os interesses nacionais, definidos como "objectively significant needs of individuals, society and the state in security and sustainable development" (Federação Russa, 2021, p. 2), e pela primeira vez desde 2000, inclui o ciberespaço, então referido como

esfera de informações. O desenvolvimento do ciberespaço é prioritário para a "protection of Russian society from destructive information and psychological impact; sustainable development of the Russian economy on a new technological basis" (p. 8). O ponto 26 coloca a "information security" (p. 9), a cibersegurança, entre as prioridades estratégicas da Rússia, "the most important directions of national security and sustainable development" (Federação Russa, 2021, p. 2).

O capítulo IV, "Ensuring national security" (Federação Russa, 2021, p. 9), evidencia a importância da cibersegurança com uma secção própria, em vez de estar apenas referida em outras esferas de segurança como acontecia desde 2009. Nesta secção é reforçada a ideia que o desenvolvimento das TIC corresponde ao desenvolvimento de novas ameaças, referindo que "the number of computer attacks on Russian information resources is increasing" (p. 19), a maioria de origem estrangeira. O CESN2021 revela a desconfiança que a Rússia tem com outros Estados, afirmando que estes querem "dominate the global information space", e que "are practicing actions to disable critical information infrastructure facilities of the Russian Federation" (Federação Russa, 2021, p. 19).

O ponto 52 refere-se à Internet como um espaço que pode "destabilize the social and political situation" (Federação Russa, 2021, p. 19), nomeadamente através da propagação de informação falsa e ilegal. A internet volta a estar incluída na secção cultural, pela importância que tem para preservar a identidade nacional, mas ao contrário dos outros CESN, este também destaca os riscos que da influência cultural dos EUA e da "Westernization" (p. 35), até porque "the main target of such destructive influence is young people" (p. 19). A internet é ainda um espaço que facilita o crime, nomeadamente o tráfico de droga e o terrorismo, devido à anonimidade (Federação Russa, 2021, p. 20).

A influência externa também é relevante numa questão puramente tecnológica, onde a Rússia é historicamente inferior a outras potências (Federação Russa, 2021, p. 20). O CESN2021 reforça a ideia que é necessário investir nas TIC, não só para o crescimento econômico (p. 25) e desenvolvimento científico (p. 30), mas principalmente por questões de segurança, a dependência de tecnologia estrangeira vai ser sempre uma vulnerabilidade estratégica (Federação Russa, 2021, p. 20).

O ponto 56 establece que, "the purpose of information security is to strengthen the

sovereignty of the Russian Federation in the information space" (Federação Russa, 2021, p. 20), e o ponto 57 concluí a secção com uma lista de 15 tarefas para alcançar os objetivos estratégicos de cibersegurança:

1) the formation of a secure environment for the circulation of reliable information, increasing the security of the information infrastructure of the Russian Federation and the sustainability of its functioning;

2) development of a system for forecasting, identifying and preventing threats to the information security of the Russian Federation, determining their sources, and promptly eliminating the consequences of the implementation of such threats;

3) Preventing destructive information and technical influence on Russian information resources, including critical information infrastructure facilities of the Russian Federation;

4) creating conditions for effective prevention, detection and suppression of crimes and other offenses committed through the use of information and communication technologies;

5) Increased security and resilience functioning of the unified telecommunications network of the Russian Federation, the Russian segment of the Internet, and other significant objects of information and communication infrastructure, as well as preventing foreign control over their functioning;

6) Reducing the number of leaks of restricted access information and personal data to the minimum possible level, as well as reducing the number of violations of the requirements established by Russian law to protect such information and personal data;

7) prevention and/or minimization of damage to national security associated with the conduct of technical intelligence by foreign states;

8) ensuring the protection of constitutional rights and freedoms of man and

citizen in the processing of personal data, including the use of information technology;

9) Strengthening information security of the Armed Forces, other troops, military formations and bodies, as well as the developers and manufacturers of weapons, military and special equipment;

10) development of forces and means of information confrontation;

11) Countering the use of the information infrastructure of the Russian Federation by extremist and terrorist organizations, special services and propaganda structures of foreign states to carry out destructive information influence on citizens and society;

12) Improvement of means and methods of information security based on the use of advanced technologies, including artificial intelligence and quantum computing technologies;

13) Ensuring the priority use of Russian information technologies and equipment that meet information security requirements in the information infrastructure of the Russian Federation, including when implementing national projects (programs) and solving tasks in the field of digitalization of the economy and public administration;

14) Strengthening cooperation of the Russian Federation with foreign partners in the field of information security, including for the purpose of establishing an international legal regime of security in the use of information and communication technologies;

15) Bringing reliable information about domestic and foreign policy of the Russian Federation to the Russian and international public; development of interaction between public authorities, civil society institutions and organizations in carrying out activities in the field of information security of the Russian Federation. (Federação Russa, 2021, p. 20-22)

Estas tarefas pretendem atingir objetivos a nível de segurança individual, social e nacional,

onde se destaca a 10ª medida. O CESN2021 é o primeiro que hipersecuritiza plenamente o ciberespaço, a ideia de rivalidade e confronto na IE já tinha sido referida em CESN anteriores, mas nunca tinha ficado expressa a necessidade de desenvolver "confrontation means" (Federação Russa, 2021, p. 5), que correspondem a meios de coação (Ribeiro, 2009). Até 2021 a ideia central era de prevenção, proteção e dissuasão, um confronto na EI pode ser considerada uma "information war" (Ministério da Defesa da Federação Russa, 2011, p.5) se as consequências forem graves o suficiente, nomeadamente se houver um ataque à ICI, cuja importância já tinha sido destacada no CESN2015 (Kari, 2019).

O CESN2021 marca uma mudança de paradigma na abordagem russa em relação ao ciberespaço, não só pela mudança de nome, mas também porque transmite uma urgência só comparável à carta de 1998 à ONU no que diz respeito às ameaças, principalmente externas. O destaque às ameaças externas, que contrasta com o CESN2015, enquadra o CESN2021 na framework de Hansen e Nissenbaum (2009), que apesar de respeitar as ameaças internas, mantêm o princípio da Escola de Copenhaga que prioriza o poder soberano dos Estados (p. 1159).

A hipersecuritização das ameaças externas era o principal fator que faltava para cumprir esta framework, a tecnicidade esteve sempre inerente, apesar ter sempre um papel mais neutro (p. 1166-67), as práticas de segurança quotidianas sempre foram exploradas, especialmente na necessidade de educar e mobilizar a população a desenvolver hábitos de segurança na EI (p. 1165). Esta hipersecuritização é clara quando a cibersegurança é estabelecida como prioridade estratégica, pois demonstra urgência de securitizar o ciberespaço e também implica que serão empregues meios consideráveis, nomeadamente meios de coação, para atingir os objetivos definidos pelos decisores políticos (Hansen & Nissenbaum, 2009, p. 1163-1164) (Ribeiro, 2009).

Conclusão

O objetivo central desta dissertação era compreender a importância do Ciberespaço no Conceito atual de Estratégia de Segurança Nacional da Rússia. Para além deste ficaram estabelecidos três objetivos específicos, analisar a evolução do ciberespaço enquanto espaço estratégico, contextualizar a cultura estratégica russa e compreender como evoluiu a preponderância do ciberespaço no conceito de Estratégia de Segurança Nacional da Rússia. Desta forma, iremos agora responder às perguntas de investigação.

Que importância tem o ciberespaço no conceito atual de Estratégia de Segurança Nacional da Rússia?

O CESN2021, coloca o ciberespaço entre as prioridades estratégicas de segurança da Rússia. O Ciberespaço é prioritário nos três níveis de segurança, o individual, relacionado com os direitos e liberdades e de proteção de informação pessoal, o social, nomeadamente através da proteção contra o cibercrime, mas também ao nível de segurança nacional, principalmente contra ciberataques.

No CESN2021 o Ciberespaço é considerado como um espaço que necessita de ser protegido e securitizado, particularmente contra as ameaças que estão no centro da cultura estratégica russa. A internet é vista como um ponto de entrada de influência ocidental na cultura e identidade russa, nomeadamente os mais jovens que são essenciais para assegurar a renovação cultural, tantas vezes sublinhada nos documentos de estratégia russos.

Neste documento também é referida a necessidade de desenvolver meios de confronto no ciberespaço, que demonstra a vontade russa de possuir meios de coação que permitam materializar os seus objetivos no ciberespaço. Desta forma, o CESN2021 enquadra o ciberespaço na framework de Hansen e Nissenbaum (2009), porque hipersecuritiza as ameaças externas e reforça a ideia que é necessário assegurar uma fundação de segurança interna, mobilizando os cidadãos com práticas de segurança quotidianas (p. 1165). A tecnicidade também está presente, mas como é característico, num papel neutro (Hansen & Nissenbaum, 2009, p. 1167-68).

Concluindo, o ciberespaço tem uma preponderância central no Conceito atual d Estratégia de Defesa Nacional da Rússia, é uma das prioridades estratégicas. A preponderância no

conceito atual é ainda mais notória quando comparada com o papel auxiliar e secundário que o ciberespaço tinha até 2021. O Ciberespaço foi durante décadas um espaço secundário na segurança russa, mas entre 2015 e 2021 tornou-se numa das prioridades de Segurança Nacional.

Como é que o ciberespaço se tornou num espaço estratégico?

O ciberespaço começou como um espaço de partilha de conhecimento científico, entre universidades americanas, primeiro em ligações diretas entre computadores, até evoluir lentamente para ligações entre redes de computadores. A internet como a conhecemos surge apenas no início da década de 1990, quando o ciberespaço começa a ser verdadeiramente universal e aberto ao público em geral, até fora dos EUA. Em 1993, a Internet foi um dos meios que conseguiu expor ao mundo a tentativa de golpe de Estado na URSS, que se tornou num dos tópicos de maior discussão na Runet posteriormente. A ideia inicial continua até aos dias de hoje, a internet é um espaço de informação, a diferença é que agora essa informação não está limitada a conhecimento científico.

O Capítulo I começou por acompanhar esta evolução tecnológica do ciberespaço e da internet, para compreender o processo de transformação do ciberespaço de um espaço científico, que necessitava proteção, para um espaço estratégico que necessita segurança. Contudo, a securitização do ciberespaço não ocorreu necessariamente por causa da evolução tecnológica, mas sim do sentimento de insegurança provocado pelos ciberataques à Estónia em 2007. A evolução tecnológica é a causa do perigo e é esta evolução que transformou computadores em instrumentos de troca de informação para instrumentos capazes de causar danos, no entanto só uma ameaça concreta levou os Estados e as Organizações Internacionais a priorizar o Ciberespaço na sua Estratégia de Segurança.

Qual é a cultura estratégica russa?

A cultura estratégica russa é definida por duas linhas centrais, o sentimento de vulnerabilidade, motivado por fatores "geohistóricos" (Romana, 2016, p. 24), e o estatuto de grande potência, em oposição ao Ocidente. Estas duas linhas cruzam-se e de certa maneira contradizem-se porque por um lado a Rússia vive num constante sentimento de ansiedade em relação à ameaça externa, enquanto quer ser que as potências externas respeitem a sua

força.

A grande dimensão geográfica da Rússia pode ser vista como uma vantagem, mas na cultura estratégica russa esta é um fator de vulnerabilidade devido às longas fronteiras e porque historicamente a Rússia já foi invadida duas vezes nos últimos séculos. A questão histórica é central no sentimento de vulnerabilidade russo, principalmente em relação às potências ocidentais, com quem o Império Russo, a URSS e, agora a Rússia têm estado em constante disputa. O Império Russo foi invadido pela França de Napoleão, a URSS foi invadida pela Alemanha nazi e disputou a Guerra Fria com os EUA, atualmente a Rússia está em conflito com a Ucrânia. A Ucrânia não é uma potência ocidental, aliás Kiev é central na identidade cultural russa, mas este conflito é resultado da aproximação ucraniana ao Ocidente, e a defesa da Rússia da sua esfera de influência.

A defesa da sua esfera de influência é fundamental para a Rússia se estabelecer plenamente como uma superpotência, voltando a dominar o antigo espaço soviético. Na cultura estratégica russa ser uma superpotência significa respeito internacional, e consequentemente segurança porque dificilmente uma superpotência é desafiada. Na perspetiva da Rússia, a aproximação da UE à Ucrânia demonstrou que a UE não respeita a esfera de influência russa.

Como evoluiu a preponderância do ciberespaço no conceito de Estratégia de Segurança Nacional da Rússia?

O Capítulo III, acompanhou a evolução do Conceito de Estratégia de Segurança Nacional da Rússia desde 1997. O CESN1997 é produzido numa fase muito embrionária do ciberespaço, e como tal não destacou a EI como uma área de segurança prioritária, mas sim auxiliar a outras esferas de segurança, e focada em fatores internos. O CESN2000 consolida as ideais gerais de 1997, e introduz a maioria dos pontos presentes na proposta feita à ONU em 1998, nomeadamente a ideia de rivalidade, e de ameaças externas, mas sem a mesma urgência, ou seja, sem hipersecuritizar.

Ainda em 2000, surge a primeira ISD, que tem o objetivo de aplicar os princípios estratégicos definidos pelo CESN2000 na EI. A ISD2000 é o primeiro documento estratégico russo que procura securitizar o ciberespaço, no entanto acaba por ser uma enumeração de objetivos e

ameaças, sem um plano de execução claro ou estrutura organizacional detalhada.

Em 2009, surge o novo CESN que pretendia sistematizar a Estratégia de Segurança russa até 2020. O CESN2009 pode ser considerado um passo atrás na securitização russa do ciberespaço, não só porque deixa de estar entre os interesses nacionais enquanto uma esfera independente, mas também porque em 2009 as potências Ocidentais estavam na fase inicial de securitizar efetivamente o ciberespaço. No entanto, não existe uma dessecuritização porque o CESN2000 também não securitizou propriamente, ou seja, com urgência e hipersecuritização (Hansen & Nissenbaum, 2009).

Neste CESN, refere-se pela primeira vez ao ciber e à internet, no entanto estas referências ocorrem no âmbito de outras esferas, a EI está entre "foundations of the realisation" (Federação Russa, 2015) da Estratégia russa, num papel auxiliar.

Apesar do contexto internacional e nacional ter mudado bastante, o CESN2015 mantém uma estrutura semelhante e a posição auxiliar da EI. No entanto, este faz mais referências, e explora melhor a evolução das TIC e das suas ameaças. O CESN2015 estabelece que é necessário investir nesta esfera e que esta é instrumental para os objetivos estratégicos russos. Esta ideia é reforçada em 2016, com a publicação da nova ISD, que conseguiu ser mais esclarecida e objetiva que a de 2000.

Os CESN, auxiliados por outros documentos, tornam claro que até 2015 o ciberespaço é um espaço com importância estratégica inegável para a Segurança Nacional da Rússia. No entanto, esta importância ocorre a um nível secundário e auxiliar, o que acaba por ser surpreendente quando a carta à ONU de 1998 já demonstrava urgência e "ansiedade" (Federação Russa, 1998, p. 3) em relação à segurança deste espaço em si mesmo.

Analisando a evolução do CESN, o ciberespaço só é um espaço verdadeiramente securitizado em 2021, onde é uma prioridade da Estratégia de Segurança Nacional, equiparado aos espaços tradicionais de segurança. A framework de Hansen e Nissenbaum (2009) define que a tecnicidade e as práticas de segurança quotidianas são fundamentais na securitização do ciberespaço, contudo por sí só estas não securitizam o ciberespaço nem demonstram prioridade estratégia. A hipersecuritização é o fator fundamental, porque este securitiza o ciberespaço ao nível da Segurança Nacional, não só na esfera individual e social,

nomeadamente através da urgência pela securitização em ambiente de confronto contra ameaças de outros Estados soberanos (Hansen & Nissenbaum, 2009).

Kari (2019), divide a perceção russa de ameaças no ciberespaço em três fases, a fase da anarquia até 2012, a fase focada em ameaças internas entre 2012 e 2014, e a fase de foco em ameaças externas a partir da anexação da Crimeia em 2014 (p. 90). Após a analise do CESN2021, podemos considerar que a Rússia entrou na fase de hipersecuritização das ameaças externas, pela maior preponderância que tem no CESN, particularmente na tarefa de "development of forces and means of information confrontation" (Federação Russa, 2021, p. 21).

Referências Bibliográficas

Beláz, A. (2019). The changing role of the EU in cybersecurity. *Biztonságtudományi Szemle*, 1(1-2), 17-30.

Boudarina, N. (n.d.). *Doctrine of Informational Security Adopted. IRIS Legal Observations of the European Audiovisual Observatory*. Acedido a 1 de setembro, 2024, em https://merlin.obs.coe.int/article/1811

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis.* Lynne Rienner Publishers.

CCDCOE. (n.d.). About us. CCDCOE - *The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.* Acedido a 1 de setembro 2024, Disponível em https://ccdcoe.org/about-us/

Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. *Revista de Administratie Publica si Politici Sociale*, 12(1), 40.

CNCS. (n.d.). *Negação de Serviço Distribuída | Distributed denial of service (DDoS). CNCS - Centro Nacional de Cibersegurança.* Acedido a 1 de Setembro, 2024, de https://www.cncs.gov.pt/intercop-ddos/

CNCS. (n.d.). *Glossário. CNCS - Centro Nacional de Cibersegurança.* Acedido a 1 de setembro de 2024, from https://www.cncs.gov.pt/pt/glossario/#linhasobservacao

Cohen, S. B. (2014). *Geopolitics: The geography of international relations.* Rowman & Littlefield.

Consilium. (2024, 24 de junho). *Cronologia – Cibersegurança.* Acedido a 1 de Setembro, 2024, Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/timeline-cybersecurity/

Comissão Europeia. (2013). *Comunicação conjunta ao Parlamento Europeu e ao Conselho: Uma estratégia da UE sobre adaptação às alterações climáticas* (JOIN/2013/01) Disponiível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:52013JC0001

CSTB. (1991). *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press

Disterer, G., Alles, A., & Hervatin, A. (2007). Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation. In *Cyber Warfare and Cyber Terrorism* (pp. 262-272). IGI Global.

Dodge, M., & Kitchin, R. (2001). *Atlas of cyberspace*. Addison-Wesley. Disponível em: https://personalpages.manchester.ac.uk/staff/m.dodge/atlas/Atlas_with_cover_low.pdf

Dunlop, J. B. (2003). The August 1991 coup and its impact on Soviet politics. *Journal of Cold War Studies*, 5(1), 94-127.

ENISA. (n.d.). *Sobre a ENISA — Agência Da União Europeia para a Cibersegurança*. Acedido a 1 de Setembro, 2024, em https://www.enisa.europa.eu/about-enisa/about/pt

Ezzamel, M., & Willmott, H. (2010). *Strategy and strategizing: A poststructuralist perspective. In The globalization of strategy research.* Emerald Group Publishing Limited.

Fânzeres, J. M. F. (2014). Geopolítica e geostratégia da Federação Russa. *Idn cadernos.* Disponível em: https://comum.rcaap.pt/bitstream/10400.26/7758/1/idncaderno_14.pdf

Federação Russa. (1993). *Constituiton of the Russian Federation*, disponível em: https://www.refworld.org/docid/3ae6b59f4.html acedido a 1 de setembro 2024 (versão inglesa)

Federação Russa. (1997). *Russian Federation national security blueprint* [Decreto Presidencial nº 1300, de 17 de dezembro de 1997]. Traduzido por Rossiiskaya Gazeta, 26 de dezembro de 1997, pp. 4-5. Reproduzido em FBIS-SOV-97-364, 30 de dezembro de 1997. Disponível em: https://nuke.fas.org/guide/russia/doctrine/blueprint.html

Federação Russa. (1998). *Carta datada de 23 de setembro de 1998 do Representante Permanente da Federação Russa junto às Nações Unidas dirigida ao Secretário-Geral* A/53/384). Assembleia Geral das Nações Unidas. Disponível em: https://digitallibrary.un.org/record/261158?v=pdf (versão em língua inglesa)

Federação Russa. (2000a). *Russian Federation national security blueprint* [Aprovado

pelo Decreto Presidencial nº 1300 de 17 de dezembro de 1999, na redação do Decreto Presidencial nº 24 de 10 de janeiro de 2000]. Traduzido e publicado em Rossiiskaya Gazeta, 18 de janeiro de 2000. Disponível em: https://nuke.fas.org/guide/russia/doctrine/gazeta012400.htm

Federação Russa. (2000b*). Information security doctrine of the Russian Federation* [Aprovada pelo Presidente a 9 de setembro de 2009].(Traduzido pelo International Telecommunication Union, 2008) Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Federação Russa. (2009*). National Security Strategy of the Russian Federation to 2020* [Decreto Presidencial n. º 537, de 12 de maio de 2009]. Disponível em: https://thailand.mid.ru/en/o_rossii/vneshnyaya_politika/strategiya_natsionalnoy_bezopasn

Federação Russa. (2015*). Russian National Security Strategy* [Decreto Presidencial n.º 683, de 31 de dezembro de 2015] Disponível em: https://is.muni.cz/el/fss/jaro2016/POL601/Russian-National-Security-Strategy-31Dec2015.pdf

Federação Russa. (2016). *Doctrine of Information Security of the Russian Federation* [Decreto Presidencial n. º 646, de 5 de dezembro de 2016]. Disponível em: https://mid.ru/en/foreign_policy/fundamental_documents/1539546/

Federação Russa. (2021). *About the strategy of national security of the Russian Federation* [Decreto Presidencial n. º 400, de 2 de julho de 2021]. Disponível em: https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf

Fernandes, A. J. (2012). *Introdução à Ciência Política: teorias, métodos e temáticas.* Porto Editora

Furlong, P., & Marsh, D. (2010). *A skin not a sweater: Ontology and epistemology in political science* (pp. 184-211). na.

Galushkin, A. (2015). Internet in modern Russia: History of development, place and role. *Asian Social Science*, 11(18), 305.

Godzimirski, J. M. (2000). Russian national security concepts 1997 and 2000: A comparative analysis. *European Security*, 9(4), 73–91. https://doi.org/10.1080/09662830008407473

Götz, E., & Staun, J. (2022). Why Russia attacked Ukraine: Strategic culture and radicalized narratives. *Contemporary Security Policy*, 43(3), 482-497.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, 53(4), 1155-1175.

Hermenegildo, G. F. (2020). *Cibersegurança Na União Europeia e Os Desafios Para a sua Eficácia Perspetivas, Panorama Estratégico e Instrumentos Jurídicos* (Tese de Mestrado, Universidade do Porto (Portugal)).

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2), 49-60.

Hyslip, T. S., & Pittman, J. M. (2015). A survey of botnet detection techniques by command and control infrastructure. *Journal of Digital Forensics, Security and Law*, 10(1), 2. Disponível em: https://commons.erau.edu/cgi/viewcontent.cgi?article=1195&context=jdfsl

Kari, M. J. (2019). *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture–a tool to Explain Russia´ s Cyber Threat Perception and Response to Cyber Threats.* JYU dissertations.

Konradova, N. (2020). *The rise of Runet and the main stages of its history. Internet in Russia: A Study of the Runet and Its Impact on Social Life*, 39-61.

Lara, António de Sousa (2015). *Ciência Política: Estudo da Ordem e da Subversão.* ISCSP

Martins, M. (2012). Ciberespaço: uma nova realidade para a segurança internacional. *Nação e defesa.*

McFaul, M. (2020). Putin, Putinism, and the domestic determinants of Russian Foreign policy. *International Security*, 45(2), 95-139.

Ministério da Defesa da Federação Russa. (2011). *Conceptual views regarding the*

activities of the Armed Forces of the Russian Federation in the information space. Ministério da Defesa da Federação Russa. Traduzido pelo CCDCOE da NATO. Disponível em: https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf

NATO. (1949). *The North Atlantic Treaty*, Washington D.C., 4 April 1949. Disponível em: http://www.nato.int/cps/en/natolive/official_texts_17120.htm

NATO. (2003). *Prague Summit 2002. Selected Documents and Statements*. Disponível em: https://www.nato.int/docu/0211prague/speeches-e.pdf

NATO. (2016). *Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw.* Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2024, 30 de julho). *Cyber defence*. Acedido a 1 de Setembro, 2024, Disponível em: https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, 7, 61-73.

Parsons, C. (2010). Constructivism and interpretive theory. *Theory and methods in political science*, 3, 80-98

Parlamento Europeu, & Conselho da União Europeia. (2022). *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas para um elevado nível comum de cibersegurança em toda a União* (Diretiva NIS2). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555

Prodanov, C. C., & De Freitas, E. C. (2013). *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico* 2ª Edição. Editora Feevale.

Putin, V. (2021, 7 de dezembro). *'On the historical unity of Russians and Ukrainians*'. Kremlin. Disponível em: http://en.kremlin.ru/events/president/news/66181

Ramich, M. S., & Piskunov, D. A. (2022). The securitization of cyberspace: from rulemaking to establishing legal regimes. *Vestnik RUDN. International Relations*, 22(2), 238-255.

Renz, B. (2018). Russia and 'hybrid warfare'. In *Russia, the West, and the Ukraine Crisis* (pp. 35-52). Routledge.

Ribeiro, António Silva (2009). Teoria Geral da Estratégia. Coimbra: Almedina.

Roberts, K. (2017). Understanding Putin: The politics of identity and geopolitics in Russian foreign policy discourse. *International Journal: Canada's Journal Of Global Policy Analysis*, 72(1), 28-55. doi: 10.1177/0020702017692609

Romana, H. B. (2016). Da cultura estratégica: uma abordagem sistêmica e interdisciplinar. *Revista da EGN*, 22(1), 13-32.

Schmidt, A. (2013). *The Estonian Cyberattacks. The fierce domain–conflicts in cyberspace,* 2012, 1986-2012. Disponível em: https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks

Schröder, H. (2009). Russia's National Security Strategy to 2020. *Russian Analytical Digest*, 62(9), 10. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RAD-62-6-10.pdf

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know.* Oxford University Press.

Stoltenberg, J. (2019). *NATO will defend itself*. Acedido a de 1 de setembro de 2024 Disponível em: https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en ´

Tiirmaa-Klaar, H. (2021). *The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body*. Hague Centre for Strategic Studies. Acedido a 1 de setembro 2024. Disponível em: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf

Trenin, D. (2019). *Russia*. Polity.

Tzu, Sun (2015). *A Arte da Guerra*. Leya.

União Europeia. (2007). *Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que estabelece a Comunidade Europeia*. Disponível em: https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:C2007/306/01

União Europeia. (2023, 28 de novembro). *Convenção sobre a cibercriminalidade*. Eur-Lex. https://eur-lex.europa.eu/PT/legal-content/summary/convention-on-cybercrime.htm

Wang, P., Sparks, S., & Zou, C. C. (2008). An advanced hybrid peer-to-peer botnet IEEE *Transactions on Dependable and Secure Computing*, 7(2), 113-127. Disponível em: https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/wang/wang.pdf

Wirtz, J. J. (2015). Cyber war and strategic culture: The Russian integration of cyber power into grand strategy. *Cyber war in perspective: Russian aggression against Ukraine*, 29-36