idn cadernos

X SEMINÁRIO IDN JOVEM

AHNHELINA BYKOVA, BRUNO OLIVEIRA, CRISTOVÃO RIBEIRO, ESTER SANTOS, GABRIELA PENA, JOÃO GERALDES, JULIANA BRITO, MÁRIO SANTOS, MARISA NOGUEIRA, MIGUEL PACHECO, TIAGO RAMALHO

PORTO, 8 E 9 DE ABRIL DE 2025

idn Instituto da Defesa Nacional

Abril
2026
N.º 58

X Seminário IDN Jovem

Porto, 8 e 9 de Abril, Instituto da Defesa Nacional
e Universidade Portucalense - Infante D. Henrique

Os Cadernos do IDN resultam do trabalho de investigação residente e não residente promovido pelo Instituto da Defesa Nacional. Os temas abordados contribuem para o enriquecimento do debate sobre questões nacionais e internacionais.
As opiniões livremente expressas nas publicações do Instituto da Defesa Nacional vinculam apenas os seus autores, não podendo ser vistas como refletindo uma posição oficial do Instituto da Defesa Nacional ou do Ministério da Defesa Nacional de Portugal.

Diretora
Isabel Ferreira Nunes

Editor
Luís Cunha

Núcleo de Edições
Assistente Editorial: Filipa Teles

Capa
Nuno Fonseca/nfdesign

Propriedade, Edição e Design Gráfico
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Pré-Impressão, Impressão e Acabamento
Europress - Indústria Gráfica
Rua João Saraiva, 10-A – 1700-249 Lisboa – Portugal
Tel.: 218 444 340 Fax.: 218 492 061 E-mail: geral@europress.pt www.europress.pt

ISSN 1647-9068
Depósito Legal 344513/12

Índice

PROGRAMA

X SEMINÁRIO IDN JOVEM

UNIVERSIDADE PORTUCALENSE – INFANTE D.HENRIQUE

PORTO, 8 E 9 DE ABRIL DE 2025

TERÇA-FEIRA, 8 DE ABRIL DE 2025

9h30 **Receção dos Participantes**

10h00 **Sessão de Abertura** (Salão Nobre da UPT)

Prof. Doutor Fernando dos Santos Ramos, Reitor da Universidade Portucalense - Infante D. Henrique

Prof.ª Doutora Fernanda Neves Rebelo, Diretora do Departamento de Direito, Universidade Portucalense - Infante D. Henrique

Prof.ª Doutora Isabel Ferreira Nunes, Diretora do IDN

Juliana Brito, Presidente do NEDRI

10h30 **Keynote Speech:** A "Era da Inteligência" e a Vingança da Geopolítica

Tenente-Coronel Jorge Rodrigues

11h00 ***Intervalo***

11h15 **Painel 1 - Defesa Nacional e o Espaço Euro-Atlântico** (Auditório 201)

Comentador: Prof. Doutor Pedro Ponte e Sousa

Papers:

A importância do Sea Denial enquanto Estratégia Naval de Portugal no Atlântico

***Hugo Mota**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade da Beira Interior*
***Rui Fernandes**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade da Beira Interior*
***Matilde Pereira**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade da Beira Interior*
***Matilde Marques**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade da Beira Interior*

A Resposta da União Europeia à Invasão Russa da Ucrânia: Uma Perspetiva Realista Neoclássica

***António Sanches**, Mestrando em Relações Internacionais, Universidade da Beira Interior*

Poder, Querer e Dever na Segurança Europeia: A Fragilidade da UE e da NATO na Gestão da Ameaça Russa até 2014

***Aniel Martins**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade Lusófona*
***Francisco Raposo**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade Lusófona*
***Luís Rocha**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade Lusófona*
***Sebastiano Cá**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade Lusófona*
***Sofia Ribeiro**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Universidade Lusófona*

12h45 ***Almoço***

14h15 **Painel 2 - Política Externa e Defesa** (Auditório 201)

Comentador: Prof.ª Doutora Suhayla Castro

Papers:

A Política da Cibersegurança da União Europeia e os Impactos da Invasão Russa da Ucrânia de 2022: O caso da Diretiva NIS e NIS 2.0

***Miguel Pacheco,** Mestrando em Relações Internacionais, Escola de Economia, Gestão e Ciência Política, Universidade do Minho*

A União Europeia, a Guerra Híbrida e a Cibersegurança: A Reconfiguração da Segurança Regional Após os Ataques à Rede Elétrica Ucraniana (2015-2024)

***Gabriela Pena**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***Juliana Brito**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***Marisa Nogueira**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*

O reconhecimento do governo espanhol da Palestina como um Estado independente - Perspetiva construtivista

***Luís Silva**, Mestrando em Estratégia, Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa*

O Acordo Nuclear do Irão: Uma vitória ou um falhanço?

***Renata Silva**, estudante de Licenciatura em Relações Internacionais, Escola de Economia, Gestão e Ciência Política, Universidade do Minho*
***Pedro Azevedo**, estudante de Licenciatura em Relações Internacionais, Escola de Economia, Gestão e Ciência Política, Universidade do Minho*

A Organização das Nações Unidas como ator no cenário de segurança internacional- MINUSMA: United Nations Multidimensional Integrated Stabilization Mission in Mali vs UNMIK: United Nations Mission in Kosovo: Uma análise comparativa

***Rita Cartaxo**, Mestranda em Ciência Política e Relações Internacionais, Faculdade de Ciências Sociais e Humanas, Universidade NOVA de Lisboa*

O papel da Comissão Europeia no avanço da coordenação da política energética da UE: Uma perspetiva liberal institucional (2014–2023)

***André Freitas**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***Pedro Alves**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***Rúben Coelho**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***Tiago Salazar**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*

14h15

Painel 3 - Ameaças, Riscos e Soluções Transnacionais (Sala 202)

Comentador: Prof. Doutor Rui Garrido

Papers:

Globalisation of climate change, ocean and Arctic: security nexus in the 21st century

***Céline Rodrigues**, Doutoranda em Relações Internacionais, Faculdade de Ciências Sociais e Humanas, Universidade NOVA de Lisboa*

Desinformação e Manipulação Política: As Novas Armas dos Conflitos Híbridos

***Joana Mesquita**, Mestranda em Políticas Públicas, ISCTE - Instituto Universitário de Lisboa*
***Joana Santos**, Mestranda em Ação Humanitária, ISCTE - Instituto Universitário de Lisboa*
***Francisco Mira**, Mestrando em Estudos Internacionais, ISCTE – Instituto Universitário de Lisboa*

Literature review on the concept of "regional digital transformation"

***Anhelina Bykova**, Doutoranda em Ciências Económicas e Empresariais, Universidade dos Açores*

Água como in/segurança: evolução discursiva no contexto Israel-Palestina

***Ana Sofia Pires**, Mestranda em Ciência Política e Relações Internacionais, Faculdade de Ciências Sociais e Humanas, Universidade NOVA de Lisboa*

O Repressive Regime Lobbying na União Europeia

***Bruno Oliveira**, estudante de Licenciatura em Ciência Política e Relações Internacionais, Faculdade de Ciências Sociais e Humanas, Universidade NOVA de Lisboa*

As Crises da Ordem Internacional: Contradições e Ameaças

***Mário Santos**, Mestrando em Ciência Política e Relações Internacionais, Faculdade de Ciências Sociais e Humanas, Universidade NOVA de Lisboa*

15h45 ***Intervalo***

16h00 **Painel 4 - Segurança Internacional e Direito Internacional (1)** (Auditório 201)

Comentador: Prof. Doutor Pascoal Pereira

Papers:

Multiculturalism in France: Structural Peace or Social Disclaimer?

***Tiago Ramalho**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***Cristovão Ribeiro**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***João Geraldes**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*

A crise dos refugiados de 2015-2016 e o seu impacto nas políticas de segurança da Grécia e da UE

***Afonso Oliveira**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***José Júnior**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*
***Mara Pinho**, estudante de Licenciatura em Relações Internacionais, Universidade Portucalense Infante D. Henrique*

A Violação Sexual como Arma de Guerra: Desafios à Resolução de Conflito

***Inês Domingues**, Mestranda em Relações Internacionais e Diplomacia, Universidade Portucalense Infante D. Henrique*

O Tratado CEDAW e a Questão Teológica: Os casos do Irão e do Vaticano

***Pedro de Carvalho**, Mestrando em Relações Internacionais e Diplomacia, Universidade Portucalense Infante D. Henrique*

17h30 ***Fim do primeiro dia do Seminário***

QUARTA-FEIRA, 9 DE ABRIL DE 2025

10h00 **Painel 5 - Segurança Internacional e Direito Internacional (2)** (Auditório 201)

Comentador: Prof.ª Doutora Raquel Fernandes

Papers:

Bio-Humanitarismo: O Novo Paradigma da Ação Humanitária e a Gestão da Vida Não-Segurada

***Diogo Almeida**, Mestrando em Relações Internacionais – Estudos da Paz, Segurança e Desenvolvimento, Faculdade de Economia, Universidade de Coimbra*

Enhancing the Effectiveness of Humanitarian Aid in Conflict Zones through Strategic Management Approaches

***Ester Santos**, Mestranda em Relações Internacionais e Diplomacia, Universidade Portucalense Infante D. Henrique*

As Políticas da OTAN no Âmbito da Proteção de Civis: Análise da Intervenção da OTAN na Líbia em 2011

***Tatiana Ramos**, Mestranda em Relações Internacionais e Diplomacia, Universidade Portucalense Infante D. Henrique*

11h30 ***Intervalo***

11h45 **Sessão de Encerramento:** Entrega de Diplomas, Tuna Académica e Foto

Prof.ª Doutora Fernanda Neves Rebelo, Diretora do Departamento de Direito, Universidade Portucalense - Infante D. Henrique

Prof.ª Doutora Isabel Ferreira Nunes, Diretora do IDN

Juliana Brito, Presidente do NEDRI

12h30 ***Fim do Seminário***

Capítulo I

POLÍTICA EXTERNA E DEFESA

A Política de Cibersegurança da União Europeia e os Efeitos da Invasão Russa da Ucrânia de 2022: O caso da Diretiva NIS e NIS 2.0

Miguel Pacheco
Mestrado em Relações Internacionais, Universidade do Minho

Resumo

Este artigo examina a política de cibersegurança da União Europeia, focando-se nos efeitos da invasão russa da Ucrânia em 2022 sobre a formulação dessas políticas. Analisa-se a Diretiva NIS e a nova Diretiva NIS 2.0, usando um quadro teórico-analítico que distingue entre uma abordagem de risco e ameaça. A revisão de literatura sobre ciberespaço e cibersegurança destaca a crescente importância da segurança no ciberespaço. A pesquisa revela uma transição na NIS 2.0 para uma postura mais proativa e defensiva em resposta às novas ameaças cibernéticas, refletindo as mudanças no contexto geopolítico. Conclui-se que a NIS 2.0 representa uma evolução significativa na política de cibersegurança da UE, onde os paradigmas de *threat e risk* estão presentes e complementam-se.

Palavras-chave: União Europeia; Ciberespaço; Cibersegurança; Diretiva NIS; Diretiva NIS 2.0.

Abstract

This article examines the cybersecurity policy of the European Union, focussing on the effects of the Russian invasion of Ukraine in 2022 on the formulation of these policies. It analyses the NIS Directive and the new NIS 2.0 Directive, using a theoretical-analytical framework that distinguishes between a risk and threat approach. The literature review on cyberspace and cybersecurity highlights the growing importance of security in cyberspace. The research reveals a transition in NIS 2.0 towards a more proactive and defensive posture in response to new cyber threats, reflecting changes in the geopolitical context. It concludes that NIS 2.0 represents a significant evolution in EU cybersecurity policy, where the threat and risk paradigms are present and complement each other.

Key words: *European Union; Cyberspace; Cybersecurity; NIS Directive; NIS 2.0 Directive.*

Introdução

A cibersegurança no ciberespaço é essencial para os seus utilizadores poderem confiar, usar e tirar proveito das suas vantagens. Mas desde cedo a União Europeia percebeu que seria necessário salvaguardar os direitos e as liberdades fundamentais, de entre os quais se destacam e, importam para questões de cibersegurança, o direito à privacidade, direito à proteção das informações pessoais e as liberdades/direitos à expressão e informação (Sciacca, 2022). Deste modo, hoje a cibersegurança é um domínio político de *policy-making* emergente e cada vez mais significativo (Carrapiço e Barrinha, 2018). Como nota Sciacca (2022), o quadro legislativo, de políticas e estratégias da UE em matéria de cibersegurança é, no entanto, de difícil análise. Diferentes áreas de *policymaking* estão envolvidas em matéria de cibersegurança, nomeadamente a Justiça e Assuntos Internos e o Mercado Interno, entre outras (Sciacca, 2022).

Apesar de não ser totalmente consensual, grande parte da literatura aponta que a discussão sobre a cibersegurança, a nível da União Europeia começou por volta da década de noventa do século XX, quando os primeiros atos legislativos não vinculativos foram adotados para regular a segurança no ciberespaço (Radoniewicz, 2022). Contudo, foi apenas no início do milénio que a UE tomou a decisão de tomar uma abordagem plena à cibersegurança. Com a crescente atividade no ciberespaço, a diversificação e aumento exponencial de utilizadores, os riscos associados ao ciberespaço começaram a tornar-se um risco de segurança que tinha de ser abordado pela UE rapidamente (Carrapiço e Barrinha, 2018). Dadas as já mencionadas características do ciberespaço, que colocam desafios à soberania e capacidade de "policiamento" por parte dos Estados "a UE apresentou-se como a solução lógica e eficaz para o desafio que os Estados-membros enfrentam no que respeita à melhor forma de combater as ameaças à cibersegurança" (Carrapiço e Barrinha, 2018, p. 299). Tomada esta posição da UE, como solução para os desafios dos Estados-membros seguiu-se a adoção de (vários) atos legislativos, documentos estratégicos para o ciberespaço e a criação de instituições europeias para o ciberespaço, nomeadamente a Agência Europeia para a Segurança das Redes e da Informação (ENISA), em 2004, e o Centro Europeu para o Cibercrime da EUROPOL, em 2013 (Ruohonen et al., 2016; Carrapiço e Barrinha, 2018; Geraldes, 2019).

O primeiro programa "*eEurope 2002 – An Information Society for All*", seria adotado em sede de Conselho Europeu, no ano de 2000, quando da presidência portuguesa do Conselho. Este programa conheceu vários desenvolvimento e "versões atualizadas", sublinhando-se as de 2005 e 2010 (Radoniewicz, 2022). Até aqui, denota-se o paradigma dominante da perceção do ciberespaço e das suas vulnerabilidades a nível da (des)informação, sendo o designação da ENISA ("*Information Security*") próprio reflexo disso. Em 2008, uma diretiva do Conselho da UE compelia os Estados-membros e as instituições da UE a identificarem e designarem infraestruturas críticas, cujos níveis de proteção precisassem de melhorias (Radoniewicz, 2022). Esta diretiva, de 2008, é um exemplo claro daquilo a que Eriksson e Giacomello (2007) apelidam de *politics of protection*. Cavelty (2018) argumenta que, até 2007, a cibersegurança foi sempre um *side issue*

ou uma subcategoria, isto porque, precisamente em 2007, a Estónia foi alvo de fortes e significativos ciberataques, tornando a questão da cibersegurança mais presente na agenda política europeia.

A primeira estratégia da União Europeia para a segurança no ciberespaço foi adotada em 2013. Este documento marca o momento em que a UE passa a olhar para o ciberespaço com teor securitário como matéria de segurança (Cavelty, 2018). A estratégia clarificou os princípios que deveriam ser tidos em conta quando se formulassem políticas em matéria de cibersegurança e definiu cinco prioridades: alcançar a resiliência cibernética, reduzindo riscos e ameaças; combater drasticamente o cibercrime; desenvolver políticas e capacidades de ciberdefesa com coordenação civil e militar; fortalecer recursos industriais e tecnológicos para garantir a segurança de *hardware* e *software* críticos; e estabelecer uma política internacional coerente para proteger os direitos dos cidadãos no ciberespaço. (Comissão Europeia, 2013; Carrapiço e Barrinha, 2018; Radoniewicz, 2022; Sciacca, 2022)

Ainda em 2013, o Parlamento Europeu e o Conselho passaram uma diretiva que tinha como objeto os ataques aos sistemas de informação, substituindo a decisão do Conselho de 2005. As provisões da decisão de 2005 manteram-se na sua grande maioria, contudo, a grande transformação e desenvolvimento foi ao nível das soluções apresentadas. Passaram ainda a ser consideradas novas atividades cibercriminosas (Radoniewicz, 2022). Em 2014, com o documento "*The Continuation of Work on a Comprehensive Approach to Cybersecurity and Cybercrime*", a União Europeia passou a reconhecer o ciberespaço, como um espaço propício às atividades criminais e fraudulentas, reforçando-se deste modo a necessidade de garantir seguranças aos cidadãos da UE no ciberespaço. Por isso, em 2015, a União adotaria a "*Digital Single Market Strategy*" de forma a garantir o desenvolvimento de um quadro legislativo uniforme para a dimensão digital do mercado interno da UE (Radoniewicz, 2022).

Cavelty (2018) refere que desde 2014 a UE tem trabalhado um outro ciberpilar,[1] o da ciberdefesa, sob o Quadro Estratégico da UE para a Ciberdefesa, que aborda mais as questões militares do ciberespaço (ex: ciberguerra). Contudo, Geraldes (2019), argumenta que, "ao contrário dos outros dois pilares, a ciberdefesa é o pilar menos desenvolvido, e diz respeito à proteção de sistemas de comunicação e informação que estão na base da defesa nacional" (Geraldes, 2019, p. 104).

Em 2016, adotou-se uma das diretivas centrais entre as políticas da UE para a cibersegurança. O Conselho da UE e o Parlamento Europeu passaram a diretiva com medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, mais conhecida pela sua abreviatura NIS. A diretiva NIS introduziu obrigações aos setores privados de reportar todo e qualquer ciberincidente, criou uma equipa de resposta a incidentes de segurança informática (CSIRT) para garantir a cooperação entre os Estados-membros, desbloqueou fundos para incentivar a inovação e investigação no âmbito da cibersegurança e estabeleceu parcerias público-

1 De acordo com Cavelty (2018) e Geraldes (2019) são três os ciberpilares da UE: a Proteção de Infraestruturas Críticas; o Cibercrime e, por último, a Ciberdefesa.

-privadas, para viabilizar o mercado único digital (Parlamento Europeu e Conselho, 2016; Carrapiço e Barrinha, 2018; Markopoulou et al., 2019; Radoniewicz, 2022; Sciacca, 2022).

Em 2017, o Conselho Europeu asseverou continuar os esforços na implementação da ciberestratégia da UE. Entre as formas de materializar o compromisso do Conselho, mencionou-se a renomeação da ENISA para Agência Europeia da Cibersegurança, com vista a alargar o escopo e as competências sob o mandato da agência e demonstrou-se a vontade de se estabelecer um sistema de certificação de cibersegurança para produtos, serviços e outros. Ambos os quesitos materializaram-se apenas em 2019 pela regulação 2019/881 do Parlamento Europeu e do Conselho, mais conhecido como *Cybersecurity Act* (Carrapiço e Barrinha, 2018; Radoniewicz, 2022; Sciacca, 2022). Como menciona Chiara (2022), é a primeira vez que um ato legislativo da União define claramente o que se entende por cibersegurança (Art. 2.º, n.º1): "todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas" (Parlamento Europeu e Conselho, 2019). Chiara (2022) nota um alargamento claro da definição e conceito de cibersegurança, em relação à da Estratégia para a Cibersegurança de 2013.

Um último ato legislativo que importa abordar, no que diz respeito ao *policy-making* de cibersegurança na União Europeia é o Regulamento Geral da Proteção de Dados (RGPD). Este regulamento foi adotado em 2018 e estabelece obrigações para todos os privados e públicos que atuem como controladores ou processadores de dados pessoais (Markopoulou et al., 2019; Sciacca, 2022). De acordo com Sciacca (2022), o RGPD adota uma abordagem baseada no risco, ou seja, quanto maior o risco, mais estritas devem ser as medidas de proteção desses dados. Backman (2023), com o seu quadro teórico, que será usado mais à frente na análise, explica perfeitamente a abordagem do RGPD. Contudo, no modelo de Eriksson e Giacomello (2007), o regulamento seria entendido e explicado, como *politics of protection*.

Outros atos legislativos têm vindo a ser adotados nos últimos anos, o que reflete a clara necessidade de readaptação da União Europeia ao contexto das relações internacionais, bem como aos mais recentes desenvolvimentos tecnológicos e do ciberespaço. A evolução contínua da legislação demonstra o compromisso da União Europeia em elevar os padrões de cibersegurança de forma abrangente, garantindo a proteção dos direitos dos cidadãos e a integridade do mercado digital. A criação de novas instituições e a adaptação de políticas existentes evidenciam a abordagem proativa da UE na resposta às ameaças emergentes e à rápida evolução tecnológica, ao mesmo tempo que sublinha a importância da cooperação entre os Estados-membros, a nível interno, e outros parceiros internacionais, a nível externo.

Deste modo, considerando a problemática que foi apresentada, coloca-se a seguinte questão de investigação: de que forma a invasão russa da Ucrânia em 2022 influenciou a transformação da política de cibersegurança da União Europeia, movendo-a de uma abordagem predominantemente orientada para o risco e a vulnerabilidade para uma que enfatiza as ameaças? Para melhor poder responder à questão, foram adotadas duas hipóteses iniciais que poderão ser refutadas ou validadas de acordo com os resultados do processo investigativo, de acordo com as propostas que se seguem.

Para abordar de forma abrangente e sistemática a questão de pesquisa, o artigo está estruturado para iniciar com uma revisão de literatura. Esta secção providenciará ao leitor uma compreensão abrangente e geral do que é o ciberespaço e o porquê da sua crescente securitização. São explorados os conceitos essenciais para a compreensão da investigação empírica deste artigo. Na metodologia, é exposta a base teórica do trabalho. São debatidas as duas possibilidades de análise, através de dois quadros teórico analíticos distintos: o primeiro, de Eriksson e Giacomello (2007), e o segundo, de Sarah Backman (2023). É explicada a escolha de um em detrimento do outro, através de uma breve análise das potencialidades e fragilidades de cada um dos modelos teóricos.

Na secção seguinte, é aplicado diretamente às diretivas NIS e NIS 2.0 o quadro teórico-analítico de Sarah Backman (2023). Estas são analisadas numa primeira fase de modo separado quanto ao seu conteúdo. Posteriormente, numa perspetiva comparada, as duas diretivas são analisadas, explicando-se a proximidade e as diferenças entre as ambas. Também nesta secção, são discutidos, debatidos e explicados os resultados obtidos mediante a aplicação do modelo de Backman (2023) às duas diretivas. Por último e, em modo conclusivo, expõem-se os desenvolvimentos que o presente artigo atingiu, assim como os pontos que poderiam ser melhor trabalhados e que podem servir para futuros trabalhos académico-científicos de investigação.

1. Revisão de Literatura: O Ciberespaço e a Cibersegurança

Vivemos num mundo cada vez mais digital, no qual se observa uma transformação clara dos conceitos de espaço e tempo, transformando o mundo naquilo a que Herbert MacLuhan chamou de "aldeia global". Grande parte desta interdependência e interconectividade que hoje se observa em muito se deve às tecnologias da informação e comunicação. As características do ciberespaço levantam fortes desafios à segurança (inter)nacional, às tradicionais conceções de soberania e estruturas do sistema internacional (Eriksson e Giacomello, 2007). Como refere Cavelty (2015): "a cibersegurança tem a ver com a insegurança criada por e através deste novo lugar/espaço e com as práticas ou processos para o tornar (mais) seguro" (Cavelty, 2015, p. 401).

As tecnologias da informação e comunicação conheceram desenvolvimentos impressionantes em poucas décadas. Do surgimento da internet, aos primeiros *websites* e às comunicações de satélite passaram pouco mais de três décadas. As tecnologias espalharam-se pelo mundo e são cada vez mais acessíveis. O crescente número de utilizadores que estas tecnologias têm, para além de uma conquista, em alguns casos traduzem-se em riscos ou ameaças. A revolução da informação, como apelidam os autores Eriksson e Giacomello (2007), o período de rápida evolução das TIC, tornam a segurança um aspeto cada vez mais importante na grande parte dos setores da sociedade. Arnold Wolfers (citado em Eriksson e Giacomello, 2007) acredita que a segurança nacional consiste na ausência de qualquer ameaça aos valores fundamentais de qualquer sociedade. Deste modo, pode assumir-se que, no atual contexto de "sociedade de informação", uma

ameaça à(s) informação(ões) pode constituir uma ameaça aos valores fundamentais das sociedades (Eriksson e Giacomello, 2007).

O controlo dos fluxos de informação e, da informação propriamente dita, já há muito tem sido identificado como função crítica para a manutenção da soberania e segurança nacional. O ciberespaço, termo cuja origem é atribuída a William Gibson, dada a sua natureza, não conhece fronteiras, não tem limites e encontra-se em constante expansão (Nikitakos e Mavropoulos, 2014; Ruohonen et al., 2016; Zdzikot, 2022), o que dificulta a tarefa dos Estados em garantir a sua segurança e "policiamento", representando deste modo desafios ao tradicional conceito de soberania e capacidade coerciva do Estado (Eriksson e Giacomello, 2007). Exemplos disso, a presença, cada vez mais significativa e crescente, de outros atores (internacionais) na informação, que não os Estados – como os media, ONGs e indivíduos – constitutem informações alternativas e não governamentais. Ao crescente número de atores, junta-se ainda os níveis "saturantes" de informação existente, que exaurem a capacidade do Estado de verificar que informações entram e saem do seu território. (Eriksson e Giacomello, 2007)

1.1. A Crescente Importância e Relevância da Segurança no Ciberespaço

A internet, uma das dimensões mais relevantes e central do ciberespaço, é resultado de uma evolução do ARPANET (*Advanced Research Projects Agency Network*), cuja construção tinha como objetivo a melhoria das comunicações entre universidade e laboratórios de pesquisa envolvidos em projetos do *United States Department of Defence*, não havendo, à partida, necessidades de segurança, uma vez que se tratava de um sistema de rede fechado e com poucos utilizadores (Cavelty, 2015; Kremling e Parker, 2018; Puyvelde e Brantly, 2019). À medida que os utilizadores foram aumentando a rede, que não tinha sido construída com a "segurança em mente" (Cavelty, 2015, p. 401), a problemática começou a emergir. O cenário tornou-se ainda mais difícil quando, na década de noventa, a comercialização da internet teve início com a invenção da World Wide Web (WWW). Muitas vezes renunciou-se à segurança para garantir que esta não dificultaria o seu funcionamento. (Cavelty, 2015; Puyvelde e Brantly, 2019)

O mundo digital (ciberespaço) de hoje, não pode ser tomado como um espaço estável e seguro. Como Nikitakos e Mavropoulos (2014) e Zdzikot (2022) referem, o ciberespaço, graças às suas características que dificultam o "policiamento" por parte dos Estados, é hoje procurado por redes de crime organizado que utilizam este (ciber)espaço e as suas ferramenteas de modo criativo para satisfazer as suas atividades, criando por vezes "categorias de crimes completamente novas" (Zdzikot, 2022, p. 10). Além disso, como também refere Zdzikot (2022):

> "em termos geopolíticos e intitucionais, é um local atrativo para muitos países prosseguirem os seus objetivos políticos, tarefas de *intelligence* ou manifestação de poder. As ações no ciberespaço podem também servir de preparação para operações militares ou ser elemento das que já estão em curso." (Zdzikot, 2022, pp. 10-11)

Diante da globalização, a cibersegurança tornou-se uma prioridade nas políticas internas de cada país, com impactos também para a segurança internacional. Qualquer interrupção séria no ciberespaço afeta a sensação de segurança dos cidadãos e outras, como a segurança das transações comerciais e a eficiência das instituições públicas, comprometendo a segurança em geral. Desta forma é incontornável a necessidade de se regular o ciberespaço, de modo a que se consiga "policiar" e proteger este espaço e as ciberinformações das entidades públicas, dos cidadãos e das empresas (Zdzikot, 2022).

O ciberespaço é difícil de definir. No entanto, é uma realidade. Uma realidade que se introduziu no quotidiano de forma gradual. Os níveis de interconectividade e dependência do ciberespaço nos dias de hoje são incomparáveis e é cada vez mais difícil (e quase impossível) reverter o processo (Nikitakos e Mavropoulos, 2014; Kremling e Parker, 2018). Na atualidade, "ninguém consegue viver sem ele (ciberespaço)" (Nikitakos e Mavropoulos, 2014, p. 259). Uma grande parte das atividades (humanas) internacionais é agora conduzida através deste espaço. Governos, cidadãos e empresas estão cada vez mais dependentes, com uma grande parte dos serviços terciários a acrescentarem o prefixo e-, como o e-*learning*, e-*banking*, e-*vote* e algumas infraestruturas físicas, como controlos aéreos dos aeroportos, que dependem em grande medida do ciberespaço para o seu funcionamento. Em alguns países a ciberdimensão é já tão relevante para a economia, que a internet contribui até 8% para o PIB. (Nikitakos e Mavropoulos, 2014; Mbanaso e Dandaura, 2015; Puyvelde e Brantly, 2019)

Como Puyvelde e Brantly (2019) argumentam, a internet (e o ciberespaço) tornaram-se espaços sociais, onde os indivíduos se agregam em função dos seus interesses. O aparecimento de empresas como a LinkedIn, o Facebook e o Twitter, no início deste milénio, tornaram-se plataformas de conexão, ligação e "amizade" entre os que usam estas plataformas (Puyvelde e Brantly, 2019). O ciberespaço é agora uma arena central da vida e sociedade humana do século XXI, como referem Puyvelde e Brantly (2019) "o advento da internet está a transformar as vidas humanas, os laços sociais e a política, e desafia as conceções estatocêntricas tradicionais sobre as interações humanas em todo o mundo" (Puyvelde e Brantly, 2019, p. 32). À medida que a internet e o ciberespaço ganham espaço na vida quotidiana, aumentam também as vulnerabilidades aos ataques através desse mesmo espaço. Deste modo, o emergir das ciberameaças está diretamente relacionado não só com a crescente complexidade mundial da rede de computadores (internet), como também com a crescente presença e diversas atividades humanas na ciberdimensão, com diversos propósitos – sociais, económicos, militares, investigação e pesquisa (Puyvelde e Brantly, 2019).

Apesar de a cibersegurança (e outros ciberconceitos) parecer um termo particularmente recente, o debate acerca da (in)segurança na ciberdimensão começou na década de 1990's. Depois de alguns testes militares de segurança revelarem falhas graves de segurança, as implicações militares dos ciberataques começaram a alertar os *experts*, fazendo emergir os primeiros debates à cerca da ciberguerra (Puyvelde e Brantly, 2019). Contudo, o próprio conceito de ciberguerra e a forma como esta era percebida pelos Estados e pela comunidade académica também foi alterado. Inicialmente, o conceito da guerra no

quinto domínio (ciberespaço) estava apenas diretamente relacionado com "guerras de informação", enquanto que hoje o conceito pode acolher atividades conduzidas por militares que visem perturbar ou destruir sistemas de comunicação ou infraestruturas críticas (*power grids*; barragens; sinalização luminosa, etc.) (Puyvelde e Brantly, 2019). Neste sentido, as ciberoperações que ocorrem na ciberdimensão, em contexto de ciberguerra, podem ultrapassar a fronteira digital e causar danos graves e irreversíveis na vida real, como mortes (Eriksson e Giacomello, 2007).

Nenhum Estado ou ator internacional está (nos tempos que correm) livre de ciberataques. Ataques através do ciberespaço conseguem perturbar os serviços públicos, cadeias de produção e distribuição de bens essenciais – com impactos severamente negativos para a economia – e roubar propriedades intelectuais, informações pessoais que podem em última instância comprometer a segurança nacional. Esta reflexão de Nikitakos e Mavropoulos (2014) ecoa de Eriksson e Giacomello (2007), autores que acreditam que "o terrorista de amanhã poderá ser capaz de fazer mais com um teclado do que com uma bomba" (Eriksson e Giacomello, 2007, p. 28). A crescente preocupação com as vulnerabilidades do ciberespaço faz com que deixe de ser visto como "um mero assunto técnico e passa a ser considerado simultaneamente como uma matéria de segurança" (Geraldes, 2019, p. 94).

2. Abordagem Baseada no Risco (*politics of protection*) e Abordagem Baseada na Ameaça (*politics of threat*): Quadro de Análise

Após a contextualização providenciada pela revisão de literatura sobre o ciberespaço, a crescente securitização que o caracteriza e a forma como a UE tem respondido a esta necessidade com as suas políticas, é agora exposto o modelo com que nos propomos analisar as duas diretivas NIS. O modelo teórico de Eriksson e Giacomello (2007) divide-se em duas formas de percecionar a analisar o ciberespaço e contruir políticas para este – *politics of threats* vs. *politics of protection*. As *politics of threats* têm uma visão alarmista e securitária do ciberespaço, sendo dominada por conceitos como, Pearl Harbor eletrónico, ciberameaça, ciberguerra, ciberataque e ciberterrorismo. Por outro lado, as *politics of protection* são essencialmente de uma lógica protecionista, prevencionista e preempetiva, onde dominam os conceitos de cibercrime, ciberresiliência, proteção de infraestruturas críticas (PIC), regulamentação de fluxos de dados e cooperação público privada. A dualidade entre as duas visões é clara, especialmente na forma como percecionam o ciberespaço. Apesar do trabalho dos autores Eriksson e Giacomello (2007) providenciar uma sólida base teórica para proceder à análise das políticas, não existe um modelo claro e pré-concebido que possa ser diretamente aplicado às diretivas NIS.

Sarah Backman (2023) também desenvolveu trabalho neste sentido através de um quadro teórico analítico (figura 1) que pode ser diretamente utilizado para a análise qualitativa das diretivas NIS, o que se pretende fazer neste artigo. Para além de ser um trabalho académico mais recente do que o de Eriksson e Giacomello (2007), possui

também a vantagem de ter sido elaborado e já aplicado no contexto da cibersegurança na União Europeia. Enquanto que a abordagem baseada em ameaças preocupa-se essencialmente com a intenção e ação de partes conflituantes, ameaças externas a um determinado objeto e políticas fundamentadas na defesa contra causas diretas de danos, a abordagem alicerçada no risco preocupa-se em ter como foco as vulnerabilidades sistémicas e a (ciber)resiliência de determinados objetos, sem identificar propriamente uma ameaça ou risco concreto (Backman, 2023). Ao passo que a primeira está mais direcionada para ameaças concretas e graves (curto prazo), nas quais existe um "outro" ameaçador, a última trata de questões a longo prazo, ameaças permanentes ou futuras, que possam emergir, sem a necessidade de se ter identificado um "outro" ameaçador (Backman, 2023).

Figura 1
Quadro Teórico-Analítico (Backman, 2023, p. 91).

	Threat-based security logic	Risk-based security logic
Problem Emphasis	Focus: Agency and intent of conflicting parties.	Focus: Systemic characteristics, vulnerability of societies.
Proposed Response	*Defend* against direct causes of harm (antagonistic threats) **Coded words:** • Threat • Attacks	*Govern* the constitutive causes of harm. **Coded words:** • Risk • Vulnerabilities
Policy prescription	Focus: Defend and deter. Plan of action for defence against threat, that is external to referent object. **Coded words:** • Deterrence • Defense • Diplomacy	Focus: Manage and mitigate. Plan of action to increase governance and resilience of referent object. **Coded words:** • Prevention • Awareness • Resilience

Inicialmente, a metodologia adotada por este trabalho consiste numa análise qualitativa das diretivas NIS, onde será aplicado o quadro teórico-analítico de Backman (2023), para qualificar as duas diretivas quanto ao seu conteúdo e concluir que paradigma(s) domina(m) a política. Posteriormente, fazendo uso do método comparado, as duas diretivas serão comparadas numa tentativa de encontrar variáveis que possam explicar o(s) paradigma(s) que as diretivas apresentam. A escolha específica das diretivas NIS é explicada pela centralidade que assumem na governança do ciberespaço ao nível da União Europeia e pelos dois períodos em que ambas foram celebradas e adotadas. A primeira, em 2016, antes do conflito, e a segunda em 2022, depois do conflito. Grande parte da literatura, considera que as diretivas são a espinha dorsal da cibersegurança na UE. Coloca-se deste modo, a questão de partida que guiará a investigação: de que forma a invasão russa da Ucrânia em 2022 influenciou a transformação da política de cibersegurança da União Europeia, movendo-a de uma abordagem predominantemente orientada para o risco e a vulnerabilidade para uma que enfatiza as ameaças?

Além disso, e tendo em conta o propósito deste artigo, o de analisar a evolução das políticas da UE e a mudança do seu paradigma em função da invasão da Ucrânia por

parte da Rússia, um conflito que, a literatura demonstra ter uma ciberdimensão, com potenciais efeitos *spillover* para a União. Exposta a metodologia, colocam-se as seguintes hipóteses: 1. O conflito russo-ucraniano (2022) alterou o paradigma das políticas da UE de *risk* para *threat*; 2. A diretiva NIS (2016) é dominada por um paradigma de *risk*, enquanto que a diretiva NIS 2.0 (2022) é dominada por um paradigma de *threat*.

3. Os Efeitos da Invasão Russa da Ucrânia sob a Formulação de Políticas de Cibersegurança na UE: O Caso da Diretiva NIS e NIS 2.0

Foi com grande surpresa que no dia 24 de fevereiro de 2022 a Europa acordou com uma guerra às suas portas, que para Barichella (2022) é uma das "crises geopolíticas mais significantes desde a II Guerra Mundial" (Barichella, 2022, p. 1). A Europa não esperava que a Rússia fosse realizar uma invasão a toda a escala, um conflito que, como Willett (2022) refere, tem em grande medida uma ciberdimensão, joga-se também no ciberespaço, algo que foi sendo revelado gradualmente. Poucas horas antes do início da invasão, a Rússia lançaria um ciberataque contra a rede de satélites Viasat, que deixou sem rede ou comunicações os clientes ucranianos, entre os quais muitas autoridades e serviços públicos e empresas ucranianas, tendo também afetado (com menor gravidade) alguns utilizadores na Europa Central (Willett, 2022; Barichella, 2022). Willett (2022) destaca que o ataque tinha um alvo claro, o governo e administração pública da Ucrânia, que dependiam em grande medida da rede de satélites para as suas comunicações.

São vários os relatórios que apontam para uma grande presença do conflito na ciberdimensão, como o CISCO, da Google ou da ESET, contudo, destaca-se um relatório da Microsoft que aponta que a Federação Russa tem integrado a ciberdimensão nas suas operações militares contra a Ucrânia (Willett, 2022; Duguin e Pavlova, 2023). Dois exemplos práticos são identificados por esse relatório: os ciberataques coordenados com ataques de mísseis aos media baseados em Kiev, e a infiltração russa nas redes de uma companhia ucraniana de energia nuclear, que coincidiu com a ocupação russa da central de Zaporizhzhia (Willett, 2022). Assiste-se, portanto, a uma combinação entre ataques militares tradicionais e ciberataques que complementam os primeiros (Monsees, 2023; Duguin e Pavlova, 2023). Contudo, muitos argumentam que as ciberoperações que a Rússia tem levado a cabo contra a Ucrânia têm duas problemáticas: 1) má coordenação com os meios físicos-militares; 2) e o impacto dos ciberataques foi sempre muito menor do que o esperado pela Rússia (má eficiência, em grande medida graças às cibercapacidades e ciberresiliência da Ucrânia) (Willett, 2022; Barichella, 2022; Mueller et al., 2023).

Os receios europeus de um *spill over* do ciberconflito russo-ucraniano, rapidamente se confirmaram. O ciberespaço não conhece fronteiras e, por isso, mesmo que, acidentalmente, alguns ciberataques russos à Ucrânia alastraram não só à Europa, mas a outros países do globo, no geral (Barichella, 2022; Radu, 2023; Duguin e Pavlova, 2023). O melhor exemplo disso foram os já referidos ataques à rede de satélites Viasat, que na

Europa deixou vários milhares de utilizadores, empresas e governos sem comunicações. Na Alemanha, por exemplo, duas mil eólicas ficaram inutilizáveis (Barichella, 2022).

O apoio manifesto e materializado do Ocidente à Ucrânia fez aumentar exponencialmente as ciberretaliações por parte da Rússia. Os ciberataques são mais presentes no leste da União Europeia e da NATO, e mais pronunciados nos países fronteiriços com a Ucrânia, isto porque países como a Polónia ou a Roménia têm estado na linha frente do apoio militar, político e humanitário à Ucrânia. É por estes países que grande maioria dos refugiados entra na Europa. Sabendo disso, a Rússia dirigiu ataques constantes aos postos romenos e polacos de controlo de fronteiras. Não são só os Estados a ser ciberatacados, mas também, por exemplo, ONG, organizações de caridade, ajuda e apoio alimentar, médico, entre outros apoios necessários, foram alvos e vítimas de ciberataques às suas plataformas *on-line*, com vista a impedir a continuidade do apoio (Barichella, 2022).

Depois da fase inicial do conflito russo-ucraniano, o regime de Putin tem focado as suas ciberoperações na exploração das cibervulnerabilidades da União Europeia e dos seus Estados-membros. As ações russas no âmbito da desinformação não são novas, contudo, aumentaram exponencialmente após o início do conflito. A União Europeia ainda não recuperou da crise económica gerada pela pandemia de Covid-19 e Moscovo soube bem aproveitar esse contexto, para explorar os custos que o apoio à Ucrânia acarretaria para o contribuinte europeu, como, por exemplo, a inflação e os custos da energia.

As ações russas não têm, portanto, diretamente como alvos os Estados-membros da União e a sua administração pública. Não se constitui, por isso, uma "ciberguerra" contra estes países. Ao invés disso, "o conflito cibernético entre a Rússia e a Ucrânia tem sido a batalha *on-line* por mentes e corações" (Willett, 2022, p. 19). A Rússia tenta, assim, descontinuar o apoio europeu à Ucrânia, e fá-lo a partir de dentro dos Estados-membros da UE, influenciando a perceção das suas sociedades sobre o conflito, que, por sua vez, deixam de apoiar as ações dos seus Estados em favor da Ucrânia (Willett, 2022; Barichella, 2022). Mais recentemente, investigações têm apontado para a possível interferência russa nos vários atos eleitorais – situação, de resto, "tradicional" por parte da Rússia, de acordo com a literatura – e, em particular, nas eleições europeias de 2024. Apoiando, financiando e fazendo crescer no seio político da UE partidos que bloqueiam decisões e minam as posições conjuntas, resultando, provavelmente, num bloqueio das medidas e legislações de apoio à Ucrânia (Reuters, 2024; *Politico*, 2024).

O conflito levanta, assim, vários desafios à União Europeia, que tem procurado adaptar e transformar as suas políticas para responderem aos novos desafios postos pela guerra russo-ucraniana (Saalman et al., 2023). A diretiva NIS, sendo central na cibersegurança na União Europeia, foi alvo de reformas para garantir uma maior abrangência de áreas de atuação e altos níveis padronizados de cibersegurança. Esta mudança, como refere a literatura, foi em grande medida pressionada pelo aparecimento do conflito às portas da Europa (Liedekerke e Laudrain, 2022; Saalman et al., 2023).

3.1. A Diretiva NIS (análise qualitativa)

A Diretiva NIS (Diretiva de Segurança das Redes e da Informação) foi estabelecida em 2016 pela União Europeia, com o objetivo de alcançar um nível elevado comum de segurança para redes e sistemas de informação em toda a União. A diretiva exige que os Estados-membros adotem uma estratégia nacional de segurança para as suas redes e sistemas de informação. A NIS cria um grupo de cooperação para facilitar a colaboração estratégica e a troca de informações entre os Estados-membros, promovendo a confiança entre eles. Também estabelece uma rede de equipas de resposta a incidentes de segurança informática (CSIRT) para promover a cooperação operacional rápida e eficaz. (Parlamento Europeu e Conselho, 2016; Carrapiço e Barrinha, 2018; Markopoulou et al., 2019; Radoniewicz, 2022; Sciacca, 2022)

Analisando e aplicando à Diretiva NIS o quadro teórico-analítico de Backman (2023), a lógica dominante é a lógica de segurança baseada em riscos. A diretiva enfatiza a importância de entender e mitigar as vulnerabilidades intrínsecas aos sistemas de informação e redes. Em vez de se concentrar ou identificar apenas ameaças específicas e as suas intenções, a NIS promove a análise de riscos e a identificação de vulnerabilidades para criar uma postura de segurança mais robusta e preventiva. Quanto às *coded words* que Backman (2023) define para se verificar que lógica é a dominante, conceitos e palavras como "risco", "vulnerabilidades", "prevenção", "conscientização" e "resiliência" são centrais na diretiva. Conclui-se, deste modo, que a lógica dominante da Diretiva NIS é claramente a de segurança baseada em riscos, focada na gestão e mitigação de riscos através da governança aprimorada e do aumento da resiliência das infraestruturas críticas.

3.2. A Diretiva NIS 2.0 (análise qualitativa)

A Diretiva NIS 2 (2022/2555) foi adotada como reforma à anterior Diretiva NIS de 2016. A principal distinção que precisa de ser feita entre as duas diretivas é que a primeira tem foco essencialmente na "segurança de redes e sistemas de informação", enquanto que a Diretiva NIS 2.0 adota uma visão mais alargada da cibersegurança, adereçando não apenas as redes e os sistemas de informação (diretiva NIS), mas também os seus usuários e qualquer outro ator que possa ser afetado por ciberataques. A diretiva NIS 2.0, no fundo, atualiza e expande a Diretiva NIS de 2016, enquadrando as crescentes ameaças e a evolução do ciberespaço. A NIS 2.0 passa a abranger novos setores essenciais e importantes, como fornecedores de serviços digitais, administração pública e setores de saúde e pesquisa. A nova diretiva introduz requisitos mais rigorosos de segurança e obrigações de notificação de incidentes para as entidades abrangidas. As autoridades nacionais de cibersegurança têm agora mais poderes para impor sanções e garantir a conformidade. (Parlamento Europeu e Conselho, 2022; Galdón e Urien, 2023; Vandezande, 2024)

Entre os pontos-chave da NIS 2, destaca-se a harmonização das estratégias de cibersegurança nos Estados-membros da UE, promovendo uma colaboração mais estreita entre as autoridades nacionais e a Agência da União Europeia para a Cibersegurança (ENISA). A diretiva também estabelece a realização de avaliações pelos pares para

melhorar a confiança mútua e a capacidade de resposta a incidentes. A ENISA é responsável por publicar relatórios bienais sobre o estado da cibersegurança na União, incluindo avaliações de riscos e recomendações políticas para preencher lacunas na segurança. (Parlamento Europeu e Conselho, 2022; Galdón e Urien, 2023; Vandezande, 2024)

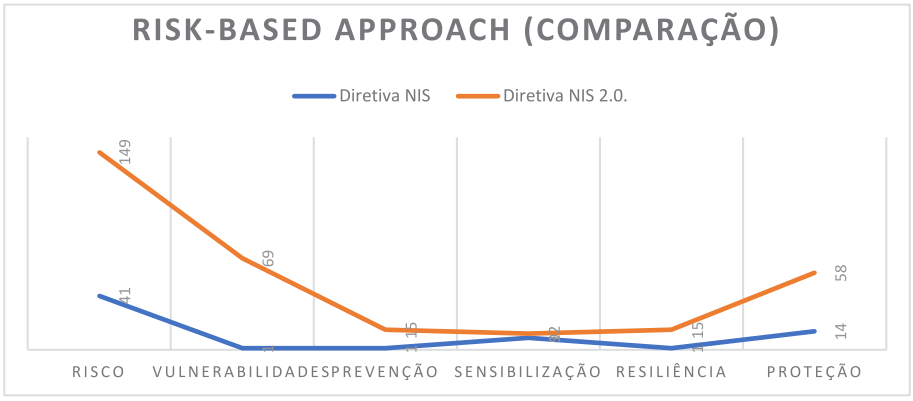
Analisando a Diretiva NIS 2 à luz do quadro teórico-analítico de Backman (2023), a lógica dominante é a lógica de segurança baseada em ameaças, embora a lógica de segurança baseada em riscos ainda esteja bastante presente e mantendo uma forte correlação. A diretiva enfatiza a defesa contra causas diretas de danos, como ameaças e ataques antagonistas. Ao contrário da primeira, a diretiva NIS 2.0 não se foca apenas na gestão de vulnerabilidades, promove também a defesa ativa contra ameaças específicas, reforçando a postura de segurança para dissuadir e mitigar ataques diretamente.

A diretiva exige ainda que os Estados-membros adotem estratégias nacionais de segurança cibernética focadas na defesa e dissuasão de ameaças. Considerando as *coded words* que Backman (2023) estabelece para se fazer a análise qualitativa, dominam os conceitos de "ameaça", "ataque", "dissuasão", "defesa" e "diplomacia", centrais na diretiva.

3.3. As Diretivas em Perspetiva Comparada: Mudança de Paradigma?

Aplicado o quadro de análise Backman (2023) às duas diretivas e analisadas e revistas as suas diferentes componentes, serão agora apresentados, analisados, discutidos e justificados os resultados da análise, considerando as hipóteses inicialmente formuladas e a apresentadas na metodologia.

Figura 2
Dados próprios com base na aplicação do modelo de risk-based approach de Backman (2023) à Diretiva NIS e NIS 2.0

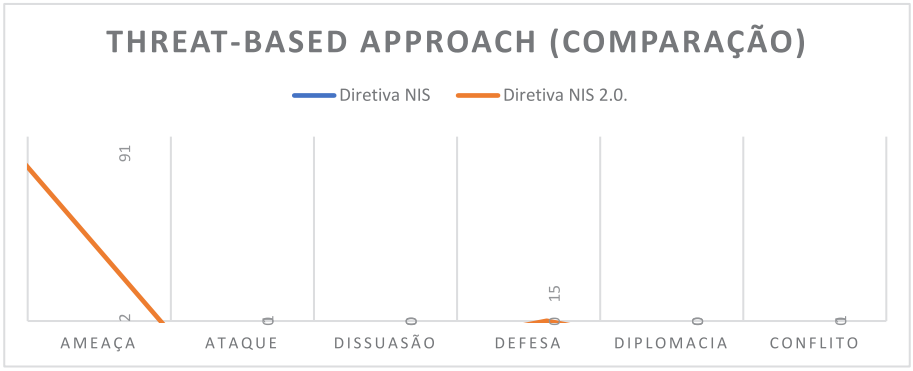


Olhando-se primeiramente sobre o modelo de *risk-based approach* da autora Sarah Backman (2023), com base no número de menções das *coded words* fornecidas pelo

modelo teórico-analítico da mesma (figura 2), é percetível a forte correlação entre o modelo e as duas diretivas, com uma particular correlação sobre a diretiva NIS 2.0. Existe, no entanto, uma explicação para este fenómeno. A diretiva NIS 2.0 é uma reforma, recuperação e transformação da diretiva NIS, alargando a sua área de atuação e aplicação (Galdón e Urien, 2023; Vandezande, 2024), o que faz com que a lógica dominante na diretiva NIS passe a enquadrar também a diretiva NIS 2.0. Além disso, outro fator pode explicar este fenómeno. As ações russas no ciberespaço, como refere a literatura (Willett, 2022; Barichella, 2022) têm seguido mais uma lógica de desinformação e não essencialmente de ataque direto (isto porque a maioria dos danos das ciberoperações russas na Europa foram com base num efeito *spill over* do conflito russo-ucraniano), ações que, segundo a análise de Eriksson e Giacomello (2007), se encontram numa lógica de *politics of protection* e não de *politics of threats*. A lógica de *politics of protection*, por sua vez, equipara-se à *risk-based approach* de Backman (2023). Estas deverão ser as razões por detrás da particular correlação da diretiva NIS 2.0 com a *risk-based approach*.

Aplicando-se o modelo de *threat-based approach* de Backman (2023) pode concluir-se, pela leitura e observação da figura 3, que a diretiva NIS 2.0 tem uma forte correlação com a lógica do modelo de *threat-based approach* quando comparada com a diretiva NIS, em que a correlação é quase nula. Deste modo, a segunda hipótese, que foi colocada no início da investigação; encontra-se, deste modo, parcialmente validada. No entanto, o paradigma de *threat* não é dominante, uma vez que a diretiva também tem uma forte correlação com o paradigma de *risk*, como se verifica em cima.

Figura 3
Dados próprios com base na aplicação do modelo de threat-based approach de Backman (2023) à Diretiva NIS e NIS 2.0



A primeira hipótese seguiu a mesma trajetória, uma vez que se encontra também parcialmente validada. O conflito não alterou totalmente o paradigma da diretiva; no entanto, pode concluir-se pela análise dos dados que, antes do conflito, a *threat-based approach* era inexistente (diretiva NIS) e, após o início do conflito (diretiva NIS 2.0),

verifica-se um aumento significativo da perceção de ameaça no ciberespaço pela União Europeia. Se, por exemplo, se aplicar este modelo à estratégia de cibersegurança da UE adotada também em 2022, as conclusões são diferentes. A *threat-based approach* é de longe dominante, enquanto que a *risk-based approach*, em nenhuma das suas *coded words* ultrapassa as 25 menções. O período (2022) e o contexto (guerra russo-ucraniana) da formulação das políticas e documentos estratégicos da União influenciou claramente os paradigmas que dominaram as mesmas.

Conclusão

A invasão russa da Ucrânia em fevereiro de 2022 foi um evento catalisador significativo que teve implicações na formulação de políticas de cibersegurança na União Europeia, evidenciado pela reforma de diretivas NIS (NIS 2.0). Este conflito, descrito como uma das crises geopolíticas mais significativas desde a Segunda Guerra Mundial (Barichella, 2022), expôs a ciberdimensão que uma guerra moderna pode assumir. Os ciberataques russos, como o incidente com a rede de satélites Viasat, demonstraram a interconexão e a vulnerabilidade das infraestruturas digitais, não só na Ucrânia, mas também na Europa e em outros países.

A resposta da União Europeia incluiu a revisão e atualização das suas políticas de cibersegurança, em particular, a Diretiva NIS de 2016, que inicialmente se focava na segurança de redes e sistemas de informação; evoluiu depois para a NIS 2.0 em 2022, refletindo uma abordagem mais abrangente e rigorosa. A NIS 2.0 não só amplia o escopo para incluir setores adicionais, como também fortalece os requisitos de segurança e as obrigações de notificação, além de conferir maiores poderes às autoridades nacionais para garantir a conformidade.

A conclusão a que esta análise empírica permite chegar é clara. Assim como em 2007, com os ciberataques russos à Estónia (Cavelty, 2018), as políticas de cibersegurança da União Europeia foram impulsionadas pelo conflito. Verifica-se, mais uma vez, a famosa "pedagogia das crises". A União Europeia tem demonstrado uma forte capacidade de aprender com os erros, durante períodos exigentes que põem à prova o projeto europeu de paz. Pela primeira vez desde a Segunda Guerra Mundial, a Europa presenciou um conflito direto. Desde 1945, a Europa manteve-se em paz, em grande medida graças ao projeto europeu. O conflito russo-ucraniano impulsionou a reforma da diretiva NIS, desejada desde 2020. Dois anos volvidos, em 2022, a nova diretiva foi adotada (NIS 2.0) após o início da invasão.

Ao aplicar o quadro teórico-analítico de Backman (2023), percebe-se uma mudança paradigmática nas diretivas. Enquanto a NIS operacionalizou uma lógica de segurança baseada nos riscos, a NIS 2.0 integra uma abordagem de segurança baseada em ameaças, sem abandonar o anterior paradigma de que é "herdeira" – *risk-based approach*. Esta transição reflete a adaptação às novas realidades do ciberespaço, onde as ameaças são mais complexas e diversificadas.

A análise comparada das diretivas revela que, embora a guerra tenha intensificado a perceção de ameaças no ciberespaço, levando à incorporação de estratégias de defesa ativa e dissuasão na NIS 2.0, a abordagem baseada em riscos permanece relevante. Esta coexistência de paradigmas sublinha a necessidade de uma postura de segurança cibernética robusta, capaz de enfrentar tanto as vulnerabilidades intrínsecas e sistemáticas como as ameaças específicas. A guerra russo-ucraniana catalisou uma revisão profunda das políticas de cibersegurança da UE, resultando numa diretiva mais abrangente e proativa. Esta evolução é crucial para enfrentar os desafios de cibersegurança contemporâneos, garantir a resiliência das infraestruturas críticas e proteger a sociedade europeia num ambiente de ameaça crescente e complexa.

Para futuras investigações, o quadro teórico-analítico de Sarah Backman (2023) poderia ser aplicado a documentos estratégicos da União Europeia, como a Bússula Estratégica ou a Estratégia de Cibersegurança da UE. Poderia ainda ser aplicado a uma análise mais aprofundada dos conceitos estratégicos nacionais e dos seus documentos oficiais para o ciberespaço e a cibersegurança, verificando, deste modo, se existe uma visão partilhada do ciberespaço entre os Estados-membros e, entre estes e a própria União Europeia.

Referências

Backman, S. (2023). Risk *vs.* Threat-based cybersecurity: the case of the EU. *European Security, 32*(1), 85-103.

Barichella, A. (2022). "Cyberattacks in Russia's Hybrid War Against Ukraine and Its Ramifications for Europe". *Europe in the World Policy Paper, No. 281*, 20. Jacques Delors Institute.

Carrapiço, H., e Barrinha, A. (2018). "European Union cyber security as an emerging research and policy field". *European Politics and Society, 19*(3), pp. 299-303.

Cavelty, M. D. (2015). "Cyber-security". In A. Collins, *Contemporary Security Studies* (pp. 400-416). Oxford University Press.

Cavelty, M. D. (2018). "Europe's Cyber Power". *European Politics and Society*, pp. 304-320.

Chiara, P. G. (2022). The IoT and the New EU Cybersecurity Regulatory Landscape. *International Review of Law, Computers & Technology, 36*(2), 118–137.

Comissão Europeia. (2013). Joint Communication of the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Bruxelas: Comissão Europeia.

Duguin, S., e Pavlova, P. (2023). *The Role of Cyber in the Russian War Against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict*. Bruxelas: Parlamento Europeu.

Eriksson, J., e Giacomello, G. (2007). *International Relations and Security in the Digital Age*. Londres: Routledge.

Galdón, J., e Urien, J. (2023). "Directiva NIS 2.0 para la Ciberseguridad de la UE: Respuesta Europea Conjunta Ante un Contexto de Ciberguerra". *SIC – Revista Ciberseguridad, seguridad de la información y privacidad* (153), pp. 110-113.

Geraldes, S. M. (2019). A Estratégia de Cibersegurança da UE: Catastrofista, Realista e/ou Otimista? *Nação e Defesa* (154), pp. 91-108.

Herrmann, D., e Pridöhl, H. (2020). Basic Concepts and Models of Cybersecurity. In M. Christen, B. Gordijn, e M. Loi (eds.) , *The Ethics of Cybersecurity*. Springer, pp. 11-44.

Kremling, J., e Parker, A. M. (2018). *Cyberspace, Cybersecurity and Cybercrime*. Sage Publications.

Liedekerke, A. d., e Laudrain, A. (2022, março 30). *Council on Foreign Relations*. Retrieved from "Russia's Cyber War: What's Next and What the European Union Should Do" *Council on Foreign Relations*, 30 de março: Disponível em: https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do (Acedido em 1 de agosto de 2025)

Markopoulou, D., Papakonstantinou, V., e Hert, P. d. (2019). "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation", *Computer Law & Security Review, 6*(35).

Mbanaso, U. M., e Dandaura, E. (2015). "The Cyberspace: Redefining A New World", *IOSR Journal of Computer Engineering, 17*(3), pp. 17-24.

Monsees, L. (2023). *The Cybersecurity Implications of Russia's War on Ukraine*. Praga: Institute of International Relations Prague.

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., e Macias, J. M. (2023). "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures", *On Future War*, 25.

Nikitakos, N., e Mavropoulos, P. (2014). "Cyberspace as a State's Element of Power". In E. G. Carayannis, D. F. Campbell, e M. P. Efthymiopoulos, *Cyber-Development, Cyber-Democracy and Cyber--Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*. Springer, pp. 259-278.

Parlamento Europeu e Conselho. (2016, julho 19). Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho – Relativa a Medidas Destinadas a Garantir um Elevado Nível Comum de Segurança das Redes e da Informação em toda a União.

Parlamento Europeu e Conselho. (2022, dezembro 27). Diretiva (UE) 2022/2555 – Relativa a Medidas Destinadas a Garantir um Elevado Nível Comum de Cibersegurança na União que Altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e Revoga a Diretiva (UE) 2016/1148.

Parlamento Europeu e Conselho. (2019, abril 17). Regulamento (UE) 2019/881 – Relativo à ENISA e à Certificação da Cibersegurança das Tecnologias da Informação e Comunicação e que Revoga o Regulamento (UE) n.º 526/2013.

Politico. (2024). *How Russia is Targeting the European Election*. Disponível em: https://www.politico.eu/newsletter/eu-election-playbook/how-russia-is-targeting-the-european-election/ (Acedido em: 27 de fevereiro de 2026).

Puyvelde, D. V., e Brantly, A. F. (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Londres: Polity Press.

Radoniewicz, F. (2022). "Cybersecurity in the European Union Law". In K. Chałubińska-Jentkiewicz, F. Radoniewicz, e T. Zieliński (eds.), *Cybersecurity in Poland: Legal Aspects*. Springer, pp. 73-92.

Radu, C.-C. (2023). The Russian-Ukrainian War and It's Impact on Cyber Security in NATO and the EU. *Romanian Military Thinking,* (4), pp. 38-53.

Reuters (2024). "European Election: How the EU says Russia is spreading Disinformation". Disponível em: https://www.reuters.com/world/europe/european-election-how-eu-says-russia-is-spreading-disinformation-2024-06-03/ (Acedido em: 1 de agosto de 2025)

Ruohonen, J., Hyrynsalmi, S., e Leppänen, V. (2016). "An Outlook on the Institutional Evolution of the European Union Cyber Security Apparatus". *Government Information Quarterly*, pp. 746--756.

Saalman, L., Su, F., e Dovgal, L. S. (2023). "Cyber Crossover and It's Escalaroty Risks for Europe". *SIPRI – Insights on Peace and Security,* (9), 24.

Sciacca, G. (2022). *Cybersecurity in the EU: An Introduction*. 25.

Vandezande, N. (2024). "Cybersecurity in the EU: How the NIS2-Directive Stacks Up Against its Predecessor". *Computer Law & Security Review,* (52).

Willett, M. (2022). "The Cyber Dimension of the Russia-Ukraine War. *Survival – Global Politics and Strategy", 64*(5), pp. 7-26.

Zdzikot, T. (2022). "Cyberspace and Cybersecurity". In K. Chałubińska-Jentkiewicz, F. Radoniewicz, e T. Zieliński (eds.), *Cybersecurity in Poland: Legal Aspects*. Springer, pp. 9-22.

A União Europeia, a Guerra Híbrida e a Cibersegurança: A Reconfiguração da Segurança Regional Após os Ataques à Rede Elétrica Ucraniana (2015-2024)

Gabriela Ribeiro Pena
Juliana Martins Magno de Brito
Marisa Filipa de Sousa Nogueira

Licenciadas em Relações Internacionais, Especialização em Diplomacia e Estudos de Área pela Universidade Portucalense Infante D. Henrique.

Resumo

Este artigo examina a correlação entre a guerra híbrida, a cibersegurança e a segurança europeia através de uma análise construtivista dos ataques à rede elétrica ucraniana em 2015 e 2016. Estes incidentes, emblemáticos das ameaças híbridas, ilustram a complexidade crescente das operações cibernéticas e as suas implicações geopolíticas.

O estudo avalia a resposta da União Europeia (UE) a essas ameaças, com especial atenção aos seus enquadramentos institucionais e iniciativas estratégicas para reforçar a cibersegurança coletiva. Do ponto de vista metodológico, a investigação adota uma abordagem qualitativa, combinando a análise documental com os conhecimentos teóricos do construtivismo para analisar a forma como as identidades e as narrativas partilhadas moldam as políticas de segurança da UE.

Ao contextualizar os desafios colocados pela guerra híbrida, o artigo sublinha a necessidade de estratégias coerentes e prospetivas para reduzir vulnerabilidades e salvaguardar a estabilidade europeia. As considerações finais contribuem para o debate mais vasto sobre a evolução das ameaças híbridas e as suas implicações para a governação da segurança internacional, destacando ainda a dimensão normativa da ação externa da UE (Manners, 2002).

Palavras-chave: Proteção das infraestruturas críticas; cibersegurança; União Europeia; guerra híbrida.

Abstract

This article examines the correlation between hybrid warfare, cybersecurity, and European security through a constructivist analysis of the cyberattacks on Ukraine's power grid in 2015 and 2016. These

incidents, emblematic of hybrid threats, illustrate the growing complexity of cyber operations and their geopolitical implications.

The study assesses the European Union's (EU) response to these threats, with particular attention to its institutional frameworks and strategic initiatives aimed at strengthening collective cybersecurity. Methodologically, the research adopts a qualitative approach, combining document analysis with constructivist theoretical insights to explore how shared identities and narratives shape EU security policies.

By contextualizing the challenges posed by hybrid warfare, this paper underscores the necessity for coherent and forward-looking strategies to mitigate vulnerabilities and ensure European stability. The concluding remarks contribute to the broader discourse on the evolution of hybrid threats and their implications for international security governance. Additionally, it underscores the EU's transformative role in shaping global cybersecurity norms in response to hybrid threats (Manners, 2002).

Keywords: *Protection of critical infrastructure; cybersecurity; European Union; hybrid war.*

Introdução

A digitalização das infraestruturas críticas ampliou vulnerabilidades, elevando a cibersegurança[1] a um pilar central da segurança regional e internacional. Os ciberataques[2], como os que visaram a rede elétrica da Ucrânia em 2015 e 2016, representam um ponto de viragem na compreensão das ameaças híbridas[3]. Atribuídas ao grupo Sandworm[4], ligado à Rússia, estas operações interromperam o fornecimento de eletricidade a milhares de pessoas, demonstrando a capacidade do ciberespaço[5] produzir efeitos físicos e sociais, com relevância estratégica e simbólica (Lee et al., 2016) (Greenberg, 2019) (ENISA, 2015-2024). Para além do seu impacto imediato, estes incidentes intensificaram o debate europeu sobre riscos sistémicos e potenciais efeitos em cascata nas infraestruturas no espaço da UE (FireEye, 2016) (NATO, 2016).

1 No contexto das políticas de segurança, a cibersegurança é entendida como a proteção das redes e sistemas de informação contra incidentes que afetem a continuidade de serviços essenciais e a estabilidade institucional (NATO, 2016) (ENISA, 2015-2024).

2 Os ciberataques consistem em ações deliberadas no ciberespaço destinadas a comprometer, degradar ou interromper o funcionamento de sistemas de informação, redes ou infraestruturas críticas, podendo assumir uma dimensão estratégica quando integrados em dinâmicas de conflito e coerção política (Cavelty, 2007).

3 As ameaças híbridas referem-se à combinação coordenada de instrumentos convencionais e não convencionais – incluindo meios militares, cibernéticos, informacionais, económicos e políticos – empregadas por atores estatais ou não estatais com o objetivo de explorar vulnerabilidades e gerar instabilidade sem ultrapassar claramente o limiar do conflito armado tradicional (Hoffman, 2007) (NATO, 2016) (Cavelty, 2007).

4 Sandworm é um grupo de *hackers* associado ao serviço de inteligência militar russo (GRU). Conhecido por ataques destrutivos como o NotPetya (2017), o grupo tem um histórico de operações cibernéticas contra infraestruturas críticas na Ucrânia e no Ocidente. O nome "Sandworm" foi dado por analistas de segurança devido a referências ao universo de ficção científica 'Duna' encontradas no código dos seus *malwares*.

5 O ciberespaço pode ser entendido como o domínio global constituído por redes interligadas de sistemas de informação e comunicação, incluindo infraestruturas digitais, dados e utilizadores, que assumiu crescente relevância estratégica nas dinâmicas contemporâneas de segurança e conflito (Nye, 2011) (Kramer et al., 2009).

A UE, profundamente interligada através de infraestruturas partilhadas, posiciona-se cada vez mais quer como um ator central em matéria de cibersegurança, quer como um interveniente estabilizador em cenários de conflitos híbridos[6]. A sua resposta aos ciberataques ucranianos reflete esta evolução, ilustrada por quadros políticos como a Diretiva SRI[7] (Diretiva (UE) 2016/1148) e o Regulamento da Cibersegurança[8] (Regulamento (UE) 2019/881), com uma narrativa política assente na resiliência, solidariedade e proteção de valores democráticos no espaço digital (Commission, 2020) (Conselho, 2019). Deste modo, a resposta europeia ultrapassa o plano estritamente técnico, contribuindo para a construção e consolidação da identidade da UE enquanto ator de segurança regional e potência normativa (Manners, 2002).

A teoria construtivista das Relações Internacionais fornece uma lente valiosa para analisar esta dinâmica, centrando-se na forma como as narrativas partilhadas e as perceções de ameaça influenciam o comportamento institucional e moldam as identidades políticas (Wendt, 1999) (Adler, 1997). A natureza cada vez mais digitalizada das infraestruturas globais amplifica a importância estratégica da cibersegurança no contexto da guerra híbrida[9]. Estas tendências exigem uma perspetiva teórica que capte a interação entre as ameaças materiais e as construções ideacionais, como a evolução da identidade da UE enquanto ator de segurança (Finnemore e Sikkink, 2005).

Este artigo tem como objetivo responder à seguinte questão de investigação: *Como é que a resposta da União Europeia aos ataques à rede elétrica ucraniana moldou a sua identidade enquanto ator de segurança regional e a sua abordagem à guerra híbrida e à cibersegurança?* A investigação examina a forma como as ciberameaças foram enquadradas como desafios existenciais, empregando para tais metodologias qualitativas, baseada em: *(i)* análise documental de políticas; e *(ii)* análise do discurso de declarações políticas e mediáticas, no período 2015-2024. Este enquadramento tem servido de base à adoção de normas e políticas de cibersegurança alinhadas com os objetivos da UE em matéria de cooperação, resiliência e estabilidade regional.

---

6 O termo *conflitos híbridos* refere-se a situações de confrontação caracterizadas pela utilização combinada e prolongada de instrumentos militares e não militares – incluindo meios cibernéticos, informacionais, económicos e políticos – frequentemente abaixo do limiar da guerra declarada, dificultando a sua atribuição e enquadramento jurídico, sendo amplamente adotado pela União Europeia e pela NATO (Hoffman, 2007) (NATO, 2016) (Europeu, 2020).

7 A diretiva SRI (NIS Directive) foi a primeira legislação da UE focada na cibersegurança. Ela impôs obrigações para operadores de infraestruturas críticas e criou requisitos mínimos de segurança para empresas estratégicas. Em 2023, a UE reforçou essa legislação com a Diretiva SRI 2, ampliando a abrangência e endurecendo as exigências de segurança para novas áreas.

8 O regulamento (UE) 2019/881, conhecido como Ato da Cibersegurança, reforçou o mandato permanente da Agência da União Europeia para a Cibersegurança (ENISA) e instituiu um quadro europeu de certificação em cibersegurança, com o objetivo de harmonizar padrões de segurança e aumentar a confiança no mercado digital europeu.

9 A guerra híbrida combina operações convencionais com táticas assimétricas, como desinformação, sabotagem cibernética e guerra económica. Um exemplo clássico é a anexação da Crimeia pela Rússia em 2014, onde forças não identificadas ("homens verdes") foram utilizadas ao lado de ataques cibernéticos e propaganda.

O artigo está estruturado do seguinte modo: a primeira secção descreve o quadro teórico, centrando-se no construtivismo e na sua relevância para a cibersegurança e a guerra híbrida. A segunda secção examina os ataques à rede elétrica ucraniana, entendidos como um estudo de caso, descrevendo em pormenor as suas caraterísticas híbridas e o seu significado geopolítico. A terceira secção analisa a resposta política da UE, destacando as suas medidas técnicas e narrativas normativas. Por último, a consideração final reflete sobre os resultados e as suas implicações para o papel da UE na governação da segurança global.

Quadro Teórico

A natureza evolutiva da guerra híbrida, em particular a sua intersecção com a cibersegurança, exige um quadro teórico sólido capaz de compreender e abordar a resposta da UE a essas ameaças. A guerra híbrida, tal como descrita por Hoffman (2007), envolve a "utilização simultânea e adaptativa de meios convencionais e irregulares para atingir fins políticos". Esta estratégia tira partido das vulnerabilidades em vários domínios, combinando táticas militares convencionais com métodos não convencionais, como ciberataques, campanhas de desinformação e coerção económica. Um exemplo desta abordagem são os ataques à rede elétrica ucraniana em 2015 e 2016. Como mencionaremos mais adiante, estes incidentes, que utilizaram ferramentas cibernéticas para perturbar infraestruturas críticas, criaram uma instabilidade social e económica significativa, enquanto promoviam objetivos geopolíticos. Estes casos sublinham uma transformação mais ampla dos conflitos modernos, em que o ciberespaço emerge como um campo de batalha fundamental, corroendo as fronteiras tradicionais entre a guerra e a paz (NATO, 2016).

A cibersegurança tornou-se, por conseguinte, um componente central da gestão das ameaças híbridas, abordando as vulnerabilidades em infraestruturas críticas interligadas, como a energia, as finanças e os cuidados de saúde. A crescente dependência dos sistemas digitais tornou-os alvos privilegiados para os adversários que pretendem desestabilizar Estados ou regiões. Os ataques ucranianos, por exemplo, exploraram as fraquezas dos sistemas de controlo de supervisão e aquisição de dados (SCADA)[10], demonstrando como as operações cibernéticas podem desencadear uma perturbação generalizada.

O construtivismo nas Relações Internacionais dá ênfase à construção social de ameaças, identidades e normas, desafiando os paradigmas materialistas que dão prioridade às capacidades materiais em detrimento dos fatores ideacionais. Wendt (1999)

10 SCADA (Supervisory Control and Data Acquisition) é um sistema utilizado para monitorar e controlar infraestruturas industriais, como redes elétricas, usinas de tratamento de água e sistemas de transporte. Estes sistemas são alvos frequentes de ataques cibernéticos devido à sua importância crítica e à sua interconectividade com redes digitais. No ataque de 2015 à Ucrânia, os *hackers* comprometeram os sistemas SCADA para manipular remotamente os disjuntores e interromper o fornecimento de energia.

argumentou que o sistema internacional é moldado por entendimentos partilhados e significados intersubjetivos, tornando o construtivismo particularmente adequado para analisar a forma como a UE enquadra e aborda as ameaças híbridas. A resposta da UE aos ciberataques, por exemplo, não é apenas um esforço técnico; está profundamente moldada pela sua identidade enquanto promotora da paz e segurança regionais. O construtivismo revela como as narrativas de solidariedade e segurança coletiva da UE sustentam as suas estratégias de cibersegurança, moldando tanto as escolhas políticas como o comportamento institucional (Adler, 1997) (Manners, 2002).

Neste enquadramento, o construtivismo permite compreender como as narrativas de solidariedade e segurança coletiva sustentam as estratégias europeias de cibersegurança, moldando tanto as escolhas políticas como o comportamento institucional. Aprofundando esta perspetiva, Finnemore e Sikkink (2005) oferecem um contributo central ao demonstrar como as normas internacionais, uma vez socialmente legitimadas, podem desencadear mudanças políticas e institucionais duradouras. A sua abordagem permite analisar a forma como determinadas interpretações partilhadas de ameaça e vulnerabilidade favorecem a consolidação de novas normas, posteriormente internalizadas em quadros jurídicos e práticas institucionais, reforçando a identidade da UE enquanto ator de segurança regional e potência normativa no domínio digital.

Esta perspetiva contrasta com as abordagens realistas tradicionais, que interpretariam as ações da UE principalmente através da lente do poder material e dos ganhos relativos (Waltz, 2010) (Mearsheimer, 2014). Embora o realismo ofereça informações valiosas sobre a dinâmica do poder, não tem em conta as dimensões normativas e ideacionais da resposta da UE às ameaças híbridas (Wendt, 1999). O construtivismo, por sua vez, destaca a forma como a UE aproveita as ciberameaças como oportunidades para reforçar a sua identidade como ator da segurança global, alinhando as suas medidas técnicas com objetivos normativos mais amplos (Manners, 2002) (Finnemore e Sikkink, 2005).

Ao combinar os conceitos de guerra híbrida, cibersegurança e construtivismo, este quadro teórico fornece uma lente abrangente através da qual se analisa a resposta da UE aos ataques à rede elétrica ucraniana. Esta abordagem capta as dimensões técnica e normativa da estratégia da UE, oferecendo uma compreensão matizada da forma como a União navega na complexa intersecção de ameaças digitais e imperativos de segurança regional. A título de exemplo, o facto de a UE enquadrar as ciberameaças não só como desafios técnicos mas também como ameaças existenciais à estabilidade coletiva realça o papel das construções ideacionais na definição das políticas (Wendt, 1999) (Adler, 1997).

Estudos de Caso: Ataques à Rede Elétrica da Ucrânia

Para observar empiricamente a lógica da guerra híbrida no domínio cibernético, esta secção analisa os ataques de 2015 e 2016 à rede elétrica ucraniana como eventos com forte impacto operacional e elevado significado político, dada a centralidade da energia enquanto infraestrutura crítica e elemento de resiliência societal.

Em 23 de dezembro de 2015, a Ucrânia sofreu um dos primeiros ciberataques amplamente documentados com impacto direto no fornecimento de energia elétrica. Este ataque afetou principalmente a empresa de distribuição de energia "Prikarpattyaoblenergo"[11], cujas 30 subestações foram desligadas, deixando cerca de 225 000 pessoas sem eletricidade durante seis horas (Lee et al., 2016). A literatura e relatórios técnicos subsequentes destacam a relevância do caso pela demonstração de uma cadeia de ataque capaz de atravessar fronteiras entre tecnologias de informação e sistemas industriais, com efeitos físicos (Lee et al., 2016) (Greenberg, 2019)

A atribuição de responsabilidades em operações híbridas tende a ser politicamente sensível e tecnicamente complexa. Embora, mais tarde, o grupo hacktivista CyberBerkut[12] tenha reivindicado a autoria inicial, a sofisticação da operação sugeriu a peritos um apoio estatal robusto, associando-se o arsenal digital do *cluster* Sandworm vinculado aos serviços de inteligência russos, devido às tensões geopolíticas persistentes entre a Rússia e a Ucrânia (Streltsov, 2017) (Greenberg, 2019).

Ao visarem infraestruturas críticas, exemplificaram a forma como a guerra híbrida explora domínios não militares para atingir objetivos políticos e psicológicos (FireEye, 2016) (NATO, 2016). Estes incidentes reforçam as preocupações existentes, ao evidenciar *malware* orientado para ambientes industriais (frequentemente referidos na literatura técnica como "Industroyer/CrashOverride"), sublinhando a escalada de sofisticação e a possibilidade de replicação em diferentes sistemas energéticos (Dragos, Inc. and Electricity Information Sharing and Analysis Center (EISAC), 2017). No conjunto, estes incidentes revelaram a falta de quadros legislativos e teóricos eficazes para enfrentar essas ameaças de forma abrangente (Streltsov, 2017), contribuindo para consolidar, no debate europeu, a perceção de que infraestruturas críticas interdependentes exigem coordenação supranacional e mecanismos comuns de preparação e resposta (ENISA, 2015-2024) (Commission, 2020).

A nível mundial, os incidentes alimentaram o debate sobre o modo como as nações se poderiam proteger destas operações avançadas e encobertas, podendo responsabilizar os seus autores (Streltsov, 2017). A União Europeia, em particular, implementou muitos regulamentos novos para evitar estes ataques, como a Diretiva (UE) 2016/1148 relativa à segurança das redes e da informação (Diretiva SRI), adotada em 2016 (SRI, 2016), como um dos primeiros passos significativos da UE para reforçar a cibersegurança nos Estados-membros. A diretiva exigia que os países da UE identificassem e protegessem as infraestruturas críticas, como os sistemas de energia, saúde e transportes, e obrigava à

11 A Prikarpattyaoblenergo é uma empresa regional de distribuição de energia elétrica na Ucrânia. Em 23 de dezembro de 2015, foi alvo de um ataque cibernético sofisticado que resultou no desligamento de subestações e na interrupção do fornecimento de energia para milhares de consumidores. O ataque foi realizado por meio de acesso remoto aos sistemas SCADA da companhia.

12 CyberBerkut era um grupo hacktivista pró-Rússia que surgiu em 2014, durante a crise da Crimeia. O grupo alegava combater o que designava de "interferência ocidental" na Ucrânia e estava ligado a diversas campanhas de desinformação, ataques DDoS e vazamentos de dados contra governos e instituições ucranianas e ocidentais.

criação de equipas de resposta a incidentes de segurança informática (CSIRT)[13] e ao reforço da cooperação transfronteiriça para fazer face a incidentes cibernéticos de grande escala. Na UE, o desafio é particularmente grave devido à natureza supranacional das suas infraestruturas interligadas, o que exigiu respostas coordenadas entre os Estados-membros (Conselho, 2016).

A dimensão construtivista assume nesta análise um papel preponderante, uma vez que a relevância dos ataques à rede elétrica ucraniana transcende a mera disrupção técnica para se consolidar como um precedente estratégico fundamental. Este caso de estudo ilustra a transição das operações cibernéticas para instrumentos de coerção política e de manipulação psicológica, sublinhando que a atribuição de responsabilidades em conflitos híbridos acarreta consequências diplomáticas tão profundas quanto o próprio dano material (Cavelty, 2007). Ao evidenciar as fronteiras cada vez mais ténues entre atores estatais e não estatais, estes incidentes revelam os imperativos ideacionais que impulsionam a dinâmica dos conflitos na era digital. Sob esta ótica, a interpretação destes eventos como um sinal de vulnerabilidade coletiva europeia funcionou como o catalisador necessário para reforçar o impulso político em torno da harmonização regulatória e das narrativas de solidariedade na proteção do espaço digital comum. A secção seguinte analisa detalhadamente essa resposta institucional e normativa.

A Resposta Política da UE

A resposta da UE aos ataques à rede elétrica ucraniana sublinha a evolução do seu papel no quadro de segurança regional, combinando medidas técnicas com iniciativas normativas para fazer face a ameaças híbridas. Estes ataques expuseram vulnerabilidades em infraestruturas críticas em toda a Europa, catalisando ações políticas destinadas a reforçar a resiliência da cibersegurança, ao mesmo tempo que moldam a identidade da UE como promotora da segurança coletiva e da paz.

Uma pedra angular da resposta técnica da UE foi a adoção da Diretiva relativa às redes e aos sistemas de informação (SRI, 2016). Implementada em 2016, esta Diretiva é a primeira legislação à escala da UE destinada a reforçar a cibersegurança nos Estados-membros, estabelecendo requisitos mínimos de segurança para os operadores de serviços essenciais, incluindo energia, cuidados de saúde e transportes (Conselho, 2016). A Diretiva SRI também introduziu obrigações de cooperação transfronteiras, promovendo a partilha de informações e a comunicação de incidentes entre os Estados-membros. Estas medidas procuraram atenuar a fragmentação das estratégias nacionais de cibersegurança, dando resposta a um desafio fundamental colocado pelas infraestruturas interligadas da UE.

13 As CSIRT (Computer Security Incident Response Teams) são equipas especializadas responsáveis por monitorizar, prevenir e responder a incidentes de segurança cibernética. Estas equipas desempenham um papel crucial na proteção das infraestruturas críticas, fornecendo suporte técnico, investigando ameaças e coordenando respostas a ataques cibernéticos em nível nacional e internacional.

Complementando a Diretiva SRI, a UE adotou o Regulamento da Cibersegurança em 2019 (Regulamento (UE) 2019/881), que reforçou o mandato da Agência da União Europeia para a Cibersegurança (ENISA) (2015-2024). O ato reforçou o papel da ENISA enquanto plataforma central de conhecimentos especializados, permitindo-lhe fornecer aos Estados-membros orientações, formação e apoio para a aplicação de quadros sólidos de cibersegurança. Além disso, o ato introduziu um quadro de certificação para produtos e serviços de tecnologias da informação e da comunicação (TIC), com o objetivo de promover a confiança e a transparência em todo o ecossistema digital (Conselho, 2019). Em conjunto, estas iniciativas refletem o empenho da UE em criar um panorama de cibersegurança unificado e resiliente, capaz de enfrentar os desafios multifacetados das ameaças híbridas (Commission, 2020).

Para além da dimensão regulatória, a resposta da UE também foi fundamental para a construção da sua identidade enquanto ator de segurança regional. Na sequência dos ataques ucranianos, os líderes da UE e as instituições enquadraram a cibersegurança como um desafio partilhado que exige uma ação coletiva. Os discursos dos funcionários da UE sublinharam frequentemente os princípios da solidariedade e da ajuda mútua, reforçando o papel da União como garante da paz e da estabilidade. Nomeadamente, as conclusões do Conselho Europeu de 2017 sobre cibersegurança salientaram a necessidade de "uma abordagem coordenada e abrangente para enfrentar as ciberameaças", reafirmando simultaneamente o compromisso da UE de proteger os seus cidadãos da guerra híbrida (2017).

Para além das suas medidas técnicas, a UE aproveitou os ataques ucranianos para reforçar a sua identidade como líder mundial em matéria de cibersegurança. Esta narrativa, frequentemente articulada via discursos oficiais e documentos políticos, enquadra a UE como uma potência normativa empenhada no multilateralismo e na proteção dos valores democráticos na era digital (Manners, 2002).

Esta construção de narrativa vai para além da retórica, moldando a forma como a UE se apresenta na cena internacional. Ao posicionar-se como uma potência normativa empenhada na defesa dos valores democráticos e na proteção das infraestruturas críticas, a UE tem procurado projetar a sua liderança na arena global da cibersegurança (Manners, 2002) (Commission, 2020). Esta identidade é reforçada pelo seu envolvimento com parceiros externos, em particular com a NATO, com a qual tem aprofundado a cooperação política e técnica no domínio cibernético, nomeadamente através do diálogo estruturado UE–NATO, da partilha de informação e da coordenação em matéria de resiliência e resposta a incidentes cibernéticos (EEAS, 2016) (Europeia, 2024). Esta interação reflete uma lógica de complementaridade, na qual a UE privilegia instrumentos regulatórios e normativos, enquanto a NATO mantém uma abordagem mais centrada na defesa coletiva e na dissuasão (NATO, 2016).

Apesar dos progressos alcançados, a resposta da UE não está isenta de limitações. A implementação das medidas de cibersegurança continua a variar entre os Estados-membros, refletindo disparidades significativas em termos de recursos, capacidades técnicas e vontade política (ENISA, 2015-2024). Estas assimetrias dificultam a obtenção de um nível homogéneo de resiliência digital e sublinham a necessidade de uma

coordenação mais eficaz, tanto no plano interno da UE como no quadro da cooperação com parceiros estratégicos externos (Commission, 2020).

Neste contexto, a interação entre a UE e a NATO evidencia diferenças institucionais relevantes. Enquanto a UE tende a basear a sua ação em mecanismos regulatórios, cooperação civil e cumprimento predominantemente voluntário, a NATO adota uma abordagem mais centralizada e militarizada no enfrentamento das ameaças híbridas, incluindo no ciberespaço (NATO, 2016) (Europeia, 2024). Esta divergência não constitui necessariamente um obstáculo, mas antes revela a complementaridade funcional entre as duas organizações, permitindo uma resposta mais abrangente às ameaças híbridas, que combina dissuasão, resiliência e governação normativa (Sarcià, 2024).

Ao combinar ações políticas concretas com narrativas de construção de identidade e ao articular a sua atuação com a NATO, a UE demonstrou capacidade de adaptação às ameaças híbridas emergentes, reforçando simultaneamente o seu papel enquanto ator de segurança regional. Estes esforços sublinham a dupla tónica da UE na resposta a vulnerabilidades imediatas e na promoção de uma visão de longo prazo assente na resiliência, na cooperação multilateral e na proteção da estabilidade regional, alinhando as respostas técnicas com o seu compromisso mais amplo com a paz e a segurança internacionais (Manners, 2002) (Finnemore e Sikkink, 2005).

Análise e Discussão

A resposta da UE aos ataques à rede elétrica ucraniana revela o modo como a guerra híbrida e a cibersegurança passaram a ocupar um lugar central na formulação das políticas de segurança regional. Os incidentes de 2015 e 2016 revelaram vulnerabilidades significativas nas infraestruturas críticas interligadas do espaço europeu, reforçando a perceção de que ameaças cibernéticas, mesmo quando ocorridas fora das fronteiras da UE, podem ter impactos diretos na estabilidade política, económica e social do continente. Esta perceção contribuiu para a consolidação de uma abordagem mais coordenada e institucionalizada à cibersegurança no seio da União.

Como discutido anteriormente, a internalização da Diretiva SRI exemplifica um marco fundamental onde a cibersegurança deixa de ser entendida exclusivamente como uma competência nacional para se afirmar como um pilar da segurança coletiva europeia. À luz do modelo de Finnemore e Sikkink (2005), esta transição demonstra como as normas de resiliência digital foram absorvidas pelas instituições da UE, reconfigurando o modo como a mesma enquadra institucionalmente as ameaças híbridas.

Este processo é operacionalizado, em grande medida, através do fortalecimento do mandato da ENISA (2015-2024) , que passou a desempenhar um papel central na coordenação técnica, na produção de conhecimento especializado e no apoio à implementação das políticas europeias de cibersegurança.

Contudo, avaliações institucionais indicam que o impacto destas diretivas tem sido desigual. Relatórios do Parlamento Europeu sublinham que, embora a Diretiva SRI tenha

contribuído para elevar os níveis gerais de preparação e para melhorar a cooperação transfronteiriça, persistem diferenças significativas na sua implementação entre os Estados-membros, refletindo assimetrias em termos de capacidades técnicas, recursos administrativos e prioridades políticas (Europeu, 2020) (Commission, 2023). Estas limitações evidenciam os desafios estruturais inerentes à governação da cibersegurança num contexto multinível, no qual a harmonização normativa nem sempre se traduz automaticamente em práticas homogéneas.

Neste enquadramento, a interação entre a UE e a NATO assume particular relevância. Enquanto a UE tende a privilegiar instrumentos regulatórios, mecanismos civis de cooperação e uma abordagem normativa à segurança cibernética, a NATO adota uma postura mais centralizada e orientada para a dissuasão e a defesa coletiva. Longe de constituírem abordagens concorrentes, estas diferenças revelam uma lógica de complementaridade funcional, permitindo uma resposta mais abrangente às ameaças híbridas, que combina capacidades militares, resiliência civil e governação normativa (NATO, 2016) (Conselho, 2024).

Paralelamente, o papel emergente da Inteligência Artificial[14] (IA) acrescenta uma nova camada de complexidade à análise da guerra híbrida e da cibersegurança. Ferramentas baseadas em IA têm vindo a ser utilizadas para melhorar a deteção precoce de ameaças, automatizar respostas a incidentes e reforçar a proteção de infraestruturas críticas. No entanto, estas mesmas tecnologias podem ser exploradas por agentes hostis para potenciar ataques mais sofisticados, incluindo campanhas de desinformação em larga escala, *deepfakes* e manipulação cognitiva, ampliando os riscos associados aos conflitos híbridos.

A UE tem procurado responder a estes desafios através da adoção do Regulamento Europeu da Inteligência Artificial[15], que estabelece princípios e requisitos para o uso seguro e responsável da IA, particularmente em domínios sensíveis e estratégicos (Conselho, 2024) . Embora este enquadramento regulatório ainda se encontre numa fase inicial de implementação, a sua articulação com as políticas de cibersegurança revela uma crescente consciência de que a resiliência europeia face à guerra híbrida depende da capacidade de antecipar e governar os impactos das tecnologias emergentes.

No seu conjunto, estes desenvolvimentos reforçam a leitura construtivista adotada neste artigo. A resposta da UE às ameaças híbridas não resulta apenas de cálculos materiais ou técnicos, mas de processos contínuos de construção de significados partilhados,

14 A Inteligência Artificial pode ser explorada tanto para defesa quanto para ataque na guerra híbrida. Ferramentas de IA são usadas para automatizar a deteção de ameaças, mas também para criar desinformação avançada, como *deepfakes*. Em 2023, um relatório da NATO alertou que a IA generativa pode aumentar a dificuldade de identificar ataques híbridos em tempo real.

15 Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial. Este diploma estabelece princípios e requisitos para o uso seguro e responsável da IA, particularmente em domínios sensíveis e estratégicos, posicionando a União Europeia como uma empreendedora normativa capaz de antecipar e governar os impactos das tecnologias emergentes na segurança regional.

aprendizagem institucional e afirmação identitária. A cibersegurança, agora indissociável da governação da IA, emerge como um domínio no qual a UE procura consolidar o seu papel enquanto empreendedora normativa, articulando instrumentos regulatórios, cooperação internacional e valores fundacionais numa visão de segurança orientada para a resiliência e a estabilidade a longo prazo.

Considerações Finais

A resposta da UE aos ataques à rede elétrica ucraniana demonstra a forma como construiu a sua identidade enquanto ator de segurança regional, ao mesmo tempo que aborda as complexidades das ameaças híbridas e da cibersegurança. Estes ataques expuseram as vulnerabilidades das infraestruturas interligadas, catalisando uma série de medidas técnicas e normativas que evidenciam a evolução do papel da UE na governação da segurança global. Ao implementar iniciativas como a Diretiva SRI e a Lei da Cibersegurança, a UE demonstrou a sua capacidade para reforçar a resiliência e promover a cooperação transfronteiriça entre os Estados-membros.

Para além das respostas técnicas, o foco da União na solidariedade e em princípios comuns fortaleceu a sua imagem como garante da paz, destacando o seu papel de empreendedora normativa na construção de um espaço digital seguro.

A análise construtivista realizada neste artigo revela que a resposta da UE foi moldada não apenas por considerações materiais, mas por narrativas e perceções partilhadas de segurança coletiva, ao responder à pergunta *"Como é que a resposta da União Europeia aos ataques à rede elétrica ucraniana moldou a sua identidade enquanto ator de segurança regional e a sua abordagem à guerra híbrida e à cibersegurança?"*. Ao enquadrar as ameaças híbridas como desafios existenciais à estabilidade regional, a UE mobilizou narrativas que legitimaram a sua liderança, alinhando as decisões políticas com a sua identidade mais alargada enquanto poder normativo.

No entanto, a análise também destaca desafios persistentes. A aplicação desigual das medidas de cibersegurança nos Estados-membros e a rápida evolução das ciberameaças sublinham a necessidade de uma adaptação contínua e de uma maior coordenação. A capacidade da UE para manter a sua liderança neste domínio dependerá do seu empenho em colmatar estas lacunas, mantendo simultaneamente um equilíbrio entre as suas respostas técnicas e os seus objetivos.

Olhando para o futuro, a UE deve aprofundar os seus investimentos na cibersegurança, centrando-se em desafios emergentes como a IA, a computação quântica e o papel dos intervenientes não estatais na guerra híbrida. A investigação futura poderá explorar como os quadros da UE se adaptarão a estes desenvolvimentos, bem como a forma como as suas parcerias com a NATO e outros intervenientes mundiais evoluirão em resposta a uma paisagem geopolítica em mutação.

Ao integrar medidas técnicas com liderança normativa, a UE respondeu com êxito às vulnerabilidades imediatas, ao mesmo tempo que construiu uma visão para a

resiliência a longo prazo. Esta dupla abordagem não só dá resposta às complexidades da guerra híbrida, como também solidifica a identidade da UE enquanto ator proativo e cooperante no domínio da segurança, num mundo cada vez mais interligado e imprevisível. À medida que a UE continua a navegar pelas complexidades da guerra híbrida, a sua capacidade de liderar pelo exemplo será fundamental. Ao equilibrar a inovação técnica com a governança normativa, a UE tem potencial não só para salvaguardar a sua própria estabilidade, mas também para moldar as normas mundiais em matéria de cibersegurança e de gestão de ameaças híbridas.

Referências

Adler, E. (1997) "Seizing the Middle Ground: Constructivism in World Politics". *European Journal of International Relations,* 3, pp. 319-363.

Cavelty, M. D. (2007) *Cyber-Security and Threat Politics US Efforts to Secure the Information Age*. London: Routledge.

Commission, E., 2020. *The EU Cybersecurity Strategy for the Digital Decade*. [Online] Available at: https://digital-strategy.ec.europa.eu/en

Commission, S.-G. o. t. E., 2023. *Proposal for a COUNCIL RECOMMENDATION on a Blueprint tocoordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance,* Bruxelas: European Commission.

Conselho, P. E. &., 2016. *European Union*. [Online] Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Conselho, P. E. &., 2019. *European Union, EUR-Lex*. [Online] Disponível em: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Conselho, P. E. &., 2024. *European Union, EUR-LEX*. [Online] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L_202401689

Dragos, Inc. and Electricity Information Sharing and Analysis Center (EISAC) (2017) *CrashOverride: Analysis of the Threat to Electric Grid Operations,* s.l.: s.n.

EEAS (2016) *Technical Arrangement on Cyber Defence between the European Union and the North Atlantic Treaty Organization,* Bruxelas: European External Action Service.

ENISA (2015-2024) *ENISA – European Union Agency for Cybersecurity*. [Online] Disponível em: https://www.enisa.europa.eu/publications#contentList

Europeia, C. d. U., 2017. *European Concil, Concil of the European Union*. [Online] Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/

Conselho Europeu (2024). *UE-OTAN: 9.º relatório intercalar salienta a importância de uma cooperação cada vez mais estreita num momento decisivo para a segurança euro-atlântica,* Bruxelas: Conselho da União Europeia.https://www.consilium.europa.eu/pt/press/press-releases/2024/06/13/eu-nato-9th-progress-report-stresses-the-importance-of-ever-closer-cooperation-at-a-key-juncture-for-euro-atlantic-security/

Europeu, P., 2020. *Directive on security of network and information systems (NIS Directive) EU cybersecurity policy,* Bruxelas: Parlamento Europeu.

Finnemore, M. e Sikkink, K. (2005) "International Norm Dynamics and Political Change*", International Organization,* 52(4), pp. 887-917 DOI: 10.1162/002081898550789.

FireEye (2016) *Sandworm: History of Cyber Espionage and Disruption.* [Online] Disponível em: https://www.mandiant.com/

Greenberg, A. (2019) *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin´s Most Dangerous Hackers.* Nova Iorque: Doubleday.

Hoffman, F. G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies.

Kramer, F., Starr, S. H. e Wentz, L. (2009) *Cyberpower and National Security.* Lincoln: Potomac Books.

Lee, R. M., Assante, M. J. e Conway, T. (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid.* [Online] Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Manners, I. (2002) "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies,* 40(2), pp. 235-258.

Mearsheimer, J. J. (2014) *The Tragedy of Great Power Politics.* Nova Iorque: W. W. Norton & Company.

NATO (2016a) *Hybrid Threats: Implications for NATO's Defence and Deterrence.*

NATO (2016b) *Warsaw Summit Communiqué: Hybrid Threats and Cyber Defence,* Bruxelas: North Atlantic Treaty Organization. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

Nye, J. S. (2011) *The Future of Power.*Nova Iorque: PublicAffairs.

Sarcià, S. A., 2024. "Why and How the EU and NATO Should Combine Their Efforts to Build Common Capabilities in the Cyber Domain", *International Cybersecurity Law Review*, 5, pp. 373-386.

SRI (2016) *Europeam Union, Eur-Lex.* [Online] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

Streltsov, L. (2017) "The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments", *European Journal for Security Research,* 2(2), pp. 147-184.

Waltz, K. N. (2010) *Theory of International Politics.* Long Grove: Waveland Press.

Wendt, A. (1999) *Social Theory of International Politics.* Cambridge: Cambridge University Press.

Capítulo II

AMEAÇAS, RISCOS E SOLUÇÕES TRANSNACIONAIS

Literature review on the concept of "regional digital transformation"

Anhelina Bykova
Doctoral Student in Business and Economics, University of Azores

Resumo

Com o presente estudo tenta-se procurar as evidências do conceito "transformação digital regional", já que o mesmo revela-se de extrema importância no atual contexto económico e político, porque pode contribuir muito para melhor formulação das políticas, bem como nas abordagens dos conceitos económicos e da defesa. Para tal efetuou-se levantamento de dados das bases de dados como Science Direct, Web of Science, ProQuest e EBSCO com intuito de encontrar as evidências necessárias.

Após análise detalhada, confirmou-se a presença do conceito "transformação digital regional" e verificou-se que este é muito recente, em uso crescente, bem como amplamente utilizado em países geograficamente amplos e com acentuada diversificação das regiões.

Palavras-chave: Digital; regiões; conceptualização; região digital; transformação regional.

Abstract

The main objective of this review is to find evidence for the use of the concept of "regional digital transformation" and to provide a clear definition of it. To this end, we conducted a systematic literature search of 35 papers in which this term was used. Our findings provided us with important insights, such as that this concept is still quite new but is gaining traction among researchers working in the field and is applied to the process of digital transformation in geographical areas with particular characteristics. It is also used as a unit of measurement and to denote the initiatives, the group, and the centers.

Keywords: *Digital, regions, conceptualization, digital region, regional transformation.*

Introduction

With this article, we aim to outline the concept of regional digital transformation and present a clear definition through a detailed systematic review of the selected articles.

Defining the problem and presenting all relevant concepts that integrate the solution is essential. Through extensive consultation of diverse literature, we can verify sporadic mentions of "regional digital transformation" appearing here and there, but nothing specific that clarifies and explains what it entails. This is why we wish to conduct a comprehensive analysis to understand where it has been used, when, why, and whether any further reference exists to the concept or a definition. In the absence of a clear concept like "regional digital transformation", we would like to propose a potential definition that arises from our review.

To achieve this aim, we will carry out a systematic literature review in accordance with the PRISMA 2020 guidelines. The articles will be retrieved from primary scientific databases and filtered using this specific terminology within the body of the articles. Based on the evidence gathered from the data, we will be able to demonstrate not only the existence and utilisation of such a concept but also how these usages manifest, thereby facilitating their understanding and definition.

This research is particularly significant for national security, given the strategic importance of peripheral regions, such as the Azores and Madeira, in global geopolitics. Understanding digital transformation in these contexts provides valuable insights for regional resilience and theoretical advancement.

Literature review

It is well-known that conceptualization is critical in academic research (Gong and Ribiere, 2021). In the first step of explaining and exploring the problem, difficulties may arise in researching a specific issue (Onen, 2016). However, sometimes, after a thorough literature review, the answer is not readily available. As new information emerges, the results should be presented as a conceptual article (Reese, 2022). This is also true in this case, as our study focuses on digital transformation in a regional context. Nevertheless, there is not enough information on this topic. Therefore, we decided to investigate it by conducting a systematic literature analysis for a holistic overview.

At this stage, it is relatively easy to start with the concept of digital transformation, as many theorists have already dealt with this definition and often mention in their approaches that it is a process of technological integration in organizations (Gong and Ribiere, 2021; Hanelt et al., 2021; North et al., 2020; Vial, 2019). The digital transformation can be seen as a radical institutional change that requires good leadership (AlNuaimi et al., 2022). This extreme change is frequently underlined (Mahboub and Sadok, 2022) and sometimes together with the specific context of each organization (Hanelt et al., 2021; Remane et al., 2017). Vial, in his study, states that digital transformation is not organization-centric; even though most definitions are centred on organizations, there are still other entities to which it may apply, such as industry and society. Whatever entities they are, the four important dimensions (Matt et al., 2015) should be present: use of technologies, changes in value creation, structural changes, and financial aspects. And it

is why digital transformation is seen as multidisciplinary by its nature (Verhoef et al., 2021), as it concerns a diverse range of changes.

One definition goes beyond by presenting digital transformation as a convergence of hard (technological) and soft (human) powers (Ebert and Duarte, 2018), affecting industries, people and organizations (Reis and Melão, 2023). Chowdhury et al. (2023) emphasise the importance of inclusive digital transformation through regionally adaptive, resident-centric, and knowledge-based policies. Also, one can't forget that digital transformation includes such aspects as cybersecurity, data protection, and infrastructure security risks. This is critical for regional resilience and should always be emphasised. Digital growth in regions is a topic that frequently arises in big countries with diversified areas, such as Australia, where regional digital growth is important (Knight, 2015), so that regional communities can contribute to regional development and the digital economy. In one other study (Nosova et al., 2021), there is a reference to the "regional digital transformation centers" as an answer to the dynamics of digital transformation in the states, so these centers could accelerate, reduce the cost and risks, and improve the quality of digital transformation.

To be successful in the transition (McAfee and Brynjolfsson, n.d.), five key areas have been highlighted: leadership with clear goals and understanding of the challenge, talent management with employees having the right skills, technology, decision-making, and organisational culture. Yet, it is also important to consider that digital transformation is moving in some industries/areas faster than in others, which can be explained by digital maturity (Westerman et al., 2014).

The performance of companies depends on their geographical location (Risal et al., 2024), starting with which continent they are located on, in the southern or northern hemisphere of the planet, or the southern or northern part of the country. And when different countries approach each other, different perspectives emerge. For instance, the Pandemic of COVID-19 influenced the creation of new forms of economic integration (Nosova et al., 2021), highlighting regional economic zones. Depending on the size of the country, a closer look is often important to better understand the performance of the industry in that country or the performance of that region, because the regional stakeholders must see and act to get the regional digital transformation (Chen et al., 2024). We focus on regional digital transformation because we want to know how regions, not countries, perform.

In an initial literature search, we were unable to find any reference to the clear concept of the regional digital transformation, but we had a reference to it (Chen et al., 2024) as a process of transition from traditional local economic and social systems towards digitisation and informatisation.

Methods

When we consulted ProQuest, where we conducted our search using three available databases (Coronavirus Research Database, Ebook Central, and Publicly Available

Content Database), we obtained twenty results, of which eighteen articles were from scientific journals, and two were conference papers.

Next, we searched for Science Direct, which returned fifteen results, all of which were research articles.

By searching the Web of Science (in all databases available there, including all collections), we obtained seven results, all of which were articles.

Finally, we searched EBSCOhost, including the following available databases: Academic Search Complete, Business Source Complete, ERIC, and Library, Information Science & Technology Abstracts. We obtained eleven results.

In total, we found forty-two articles, of which three were duplicates, one was retracted, and one was a private company report; therefore, we decided not to include it, leaving us with thirty-seven. Since our main goal was to try to find evidence and explain the concept of "regional digital transformation," we decided to exclude articles in which this expression does not occur, as mentioned. In this case, we identified two articles that dealt with the topic of regional digital transformation but did not use the concept in the texts. In the first case, we had a reference to "in the terms of regional heterogeneity, digital transformation" (Wang et al., 2024), and in the second case, we have a reference to "the project "Smart specialization in the agro-industrial complex of the region: digital transformation and convergent technologies" (Kulik et al., 2021). As a result of this first scan, we were left with thirty-five articles for review and analysis.

Even though the bias assessment does not apply to this systematic review as the investigation covers qualitative evidence (Whiting et al., 2003), we verified several scales to maintain the rigour of this analysis, among which we also adjusted the AMSTAR-2 (Shea et al., 2017) to our study.

To make our research more complete, we decided to use bibliometric analysis as the primary focus of this study which is on the concept, though we can observe through keywords and abstract terms overview in which context and what relation exists with "regional digital transformation". For this reason, we used VOSviewer to offer a more visual approach to our sample. This software is a free tool for bibliometric analyses of databases.

Results

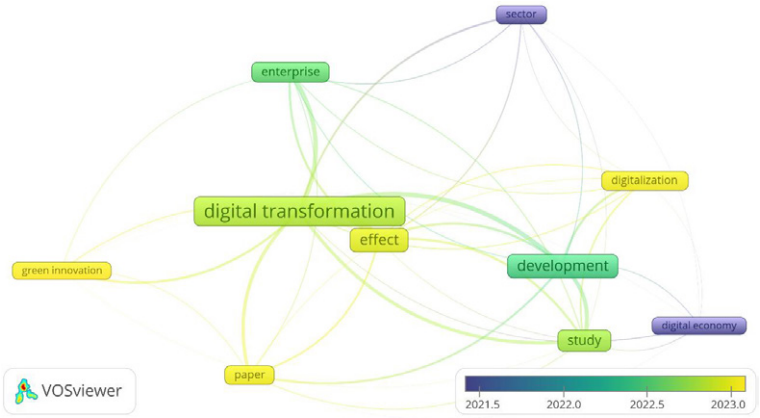
Bibliometric findings

In characterising all the articles, we have created two maps to understand the correlation of the main terms better. The first map was created based on textual data with the co-occurrence of terms based on the abstract, and the second was based on bibliographic data with the co-occurrence of keywords, highlighting the main terms, the year of publication, and the correlations among them.

Based on the analysis of the term co-occurrence created on the abstract, we saw that the most recent terms used were "green innovation," "paper," "digitalization," and

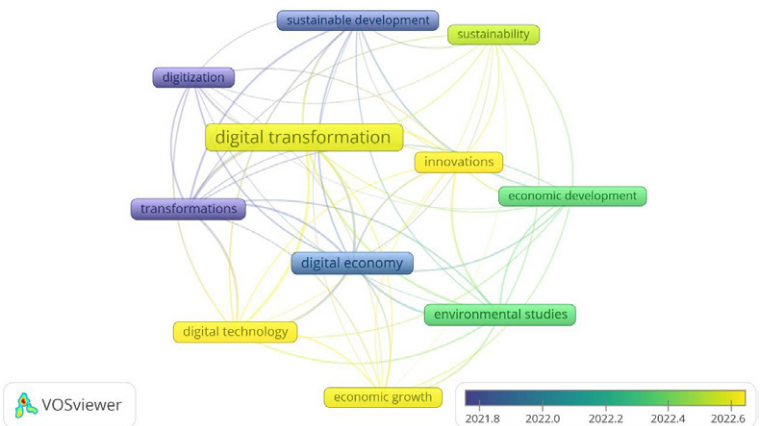
"effect." The articles published before were "digital economy" and "sector." The "digital transformation" has the biggest occurrence between the articles and a strong interconnection between all the other terms.

Figure 1
Terms co-occurrence map based on the abstract.



When the analysis of the map of keywords co-occurrence based on bibliographic data showed that the "digital transformation" keyword is the most frequently used in the second half of 2022, together with "innovation", "digital technology", and "economic growth". On the other hand, keywords like "digitization," "transformation," "sustainable development," and "digital economy" were the terms occurring with more frequency in 2021.

Figure 2
Keywords co-occurrence map based on bibliographic data.

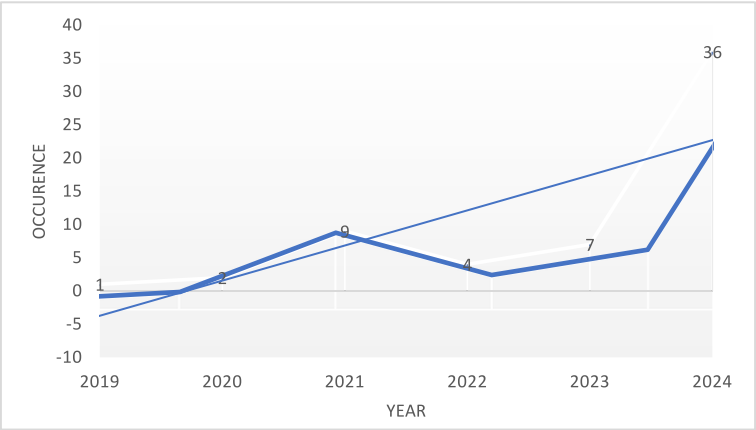


In both maps, the term "digital transformation" is predominant, correlating with all other terms in the analysis and of late use, while the term "digital economy" was of earlier appearance. The correlation is stronger with the terms "enterprise" and "development" in the first map and with "transformation", "digital economy", and "digitization" in the second map.

Concept occurrence

Once we started the analysis of the articles, we observed two relevant and representative pieces of information: increasing growth over time in the use of the concept of regional digital transformation and major contributions to its use by the country in which the study was done. After a close look at the results related to the "regional digital transformation", we can say that it appeared for the first time in the article *Logistic methodology of development of the regional digital economy* by Vilken et al., Kalinina, O., and Zotova, E. in 2019.

Figure 3
Term occurrence by year of publication of articles.



Our analysis results indicated that the term "regional digital transformation" was originally used by Russian researchers and by the Chinese in 2020, increasing over time. Besides these two main contributors, Russia, with 5 contributions, and China, with 26 of 35, other researchers writing on the matter were from Spain and the UK. Also, it is important to underline that there were 4 research cooperations in this field between Chinese researchers and colleagues from Lebanon, Taiwan, Australia, Japan, and Singapore in 2024. There was also one collaboration between South American and European researchers from Austria, Argentina, Brazil, Chile, and the United Kingdom.

After a thorough analysis of thirty-five articles in which the term "regional digital transformation" was used, we observed that in most cases, it was used uniquely and as a

reference to the process of digital transformation at the regional level. In three cases, it was part of the name, such as the "Regional Digital Transformation Group" in Brazil or the "Regional Digital Transformation Programme" and the "Regional Digital Transformation Centers" in the Russian Federation.

Next is a table with the results of our systematic literature review on the use of the concept of "regional digital transformation", as suggested by PRISMA 2020 guidelines, where not only the articles but also the number of occurrences of the concept and characteristics of its usage can be observed.

On two occasions, we noted the reference to regional digital transformation as a measure of macro-level digital transformation (Sun and Guo, 2022) between the national and industrial levels. In the study on neighbourhood green technology innovation (Du et al., 2024), the "regional digital transformation" measures collecting data on the digital transformation of individual enterprises and processing using provincial and municipal standards. Another study analysed the statement that regional digital transformation can influence the debt structure of companies (Lee et al., 2024). In the article *Digital Policy Quality and Enterprise Innovation*, the authors emphasise that digital policy aims to regulate and guide the development of regional digital transformation (Zhao and Fan, 2024).

The article *Digital transformation, productive services agglomeration and innovation performance* by Ding, Y., Shi, Z., Xi, R., Diao, Y., and Hu, Y. (2024) presented us with valuable insights into regional digital transformation as it explores the relationship between digital transformation and innovation performance at the regional level. The authors attempt to explain regional digital transformation from a single perspective (e.g., scale of digital technology adoption, digital industry output) and develop a regional digital transformation index for China. They also reaffirm the relationship between regional digital transformation and the digital economy.

The last and the most important study in this systematic review was *From riches to digitalization: The role of AMC in overcoming challenges of digital transformation in resource-rich regions* by Chen, Y., Wang, Y., and Zhao, C. (2024), as the main objective of it is to promote regional digital transformation. Authors, along with their paper, answered several questions, such as What (is regional digital transformation), When (does it happen), and How (can it be achieved). Starting by presenting their understanding of regional digital transformation as "**the process of transitioning from traditional local economic and social systems towards digitisation and informatisation**" (Chen et al., 2024). It will happen when regional governments, enterprises, and other important stakeholders recognise the potential that this process can bring to regional economies and social development and act accordingly. For this to happen, existing economic and social structures need to be adjusted, and modern technologies and business models introduced.

Discussion

After finishing our analysis, we may conclude that the term "regional digital transformation" is recent and is only slightly used in scientific research. From the evidence, it is easy to affirm that the term is more applicable to territories with specific characterizations (Chen et al., 2024) that differ significantly from one another.

From the bibliometrics results on terms co-occurrence from abstracts, we may conclude that amongst 35 articles relevant to this systematic literature review on the concept of the "regional digital transformation" in the period from 2019 to 2024, the most occurring terms at the beginning were "digital economy" and "sector", and by the end were "sustainability". All of them were connected to the term "digital transformation", which was in the middle of the map and more commonly used together with "effect" and "development", showing the evolution and expansion of the concept of "digital transformation". While looking for the co-occurrence of the terms between the keywords, it is possible to conclude that between the first articles, the most frequent keywords were "transformation", "digitalization", and "sustainable development" when by the end followed by "digital technology" and "innovation" and strongly interconnected by the terms of "digital transformation" and "digital economy", confirming our initial conclusion of the evolution of the concept and its expansion.

Also, we can deduce that the concept of "regional digital transformation" is related through bibliometric analysis to "digital transformation", as well as to the "development", "transformation", "digital economy", "digitization", and less strong, but important onnection to the "economic growth", "economic development", and "sustainable development".

The second and main part of our analysis results indicates that the term "regional digital transformation" is recent. According to the established parameters of this systematic literature review, the first evidence of it is related to the article of 2019, but it is increasingly used, as can be seen in Figure 3. For instance, in 2024, the number of uses grew to 36, indicating a certain urgency in defining and framing this concept.

Furthermore, we concluded that almost all articles were produced in geographically large countries and with regions that are quite diverse from one another. At first, the concept was used more by Russian authors and, lately, it has been used more by the Chinese, mostly because of their massive territories as countries with many regions and significant differences among them.

Primarily, the term "regional digital transformation" appeared to name some changes related to digital transformation, but on a smaller scale, as regions in countries with vast territories. It came to be used as a measure of the process of digital transformation on a smaller scale for the big state of China. In the last couple of years, the concept has become an essential measure for a state like China in such a way that even the proposed initial definition.

These results led us to define the regional digital transformation as a digital transformation on a regional scale, which could be characterized by several factors, such as the region's position, its digitalization level, its resources, regional economy, and other cultural and social aspects.

References

AlNuaimi, B. K., Kumar Singh, S., Ren, S., Budhwar, P., and Vorobyev, D., (2022). "Mastering digital transformation: The nexus between leadership, agility, and digital strategy". *Journal of Business Research*, *145*, pp. 636-648. https://doi.org/10.1016/j.jbusres.2022.03.038

Chen, Y., Wang, Y., and Zhao, C., (2024). "From riches to digitalization: The role of AMC in overcoming challenges of digital transformation in resource-rich regions". *Technological Forecasting and Social Change*, *200*, 123153. DOI: 10.1016/j.techfore.2023.123153

Du, G., Zhou, C., and Zhang, M. (2024). "Does digital transformation promote local-neighborhood green technology innovation? Based on the panel data of Chinese A-share listed companies from 2011 to 2021". *Journal of Cleaner Production*, *466*, 142809. https://doi.org/10.1016/j.jclepro.2024.142809

Ebert, C., and Duarte, C. H. C. (2018). "Digital Transformation". *IEEE Software*, *35*(4), pp. 16-21. https://doi.org/10.1109/MS.2018.2801537

Gong, C., and Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation*, *102*, 102217. https://doi.org/10.1016/j.technovation.2020.102217

Hanelt, A., Bohnsack, R., Marz, D., and Antunes Marante, C. (2021). "A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change". *Journal of Management Studies*, *58*(5), pp. 1159–1197. https://doi.org/10.1111/joms.12639

Knight, S. (2015). "Delivering the digital region: Leveraging digital connectivity to deliver regional digital growth". *Australian Planner*, *52*(1), pp. 4-15. https://doi.org/10.1080/07293682.2015.1019750

Kulik, A., Lavrinenko, E., Lyshchikova, J., and Stryabkova, E. (2021). Smart-Specialization of The Agro-Industrial Complex in The Context of Digital Transformation of Regional Economic Systems. *ETIKONOMI*, *20*(2), pp. 309-318. https://doi.org/10.15408/etk.v20i2.22015

Lee, C.-C., Wang, C.-W., Purnama, M. Y. I., and Sharma, S. S. (2024). "Digitalization and firms' debt maturity: Do financial constraints and uncertainty matter?", *Pacific-Basin Finance Journal*, *85*, 102399. https://doi.org/10.1016/j.pacfin.2024.102399

Mahboub, H., and Sadok, H. (2022). "Towards a Better Digital Transformation: Learning from the Experience of a Digital Transformation Project". In M. A. Bach Tobji, R. Jallouli, V. A. Strat, A. M. Soares, and A. A. Davidescu (eds.), *Digital Economy. Emerging Technologies and Business Innovation,* (Vol. 461) Springer International Publishing, Springer International Publishing, pp. 203-214. https://doi.org/10.1007/978-3-031-17037-9_15

Matt, C., Hess, T., and Benlian, A. (2015). "Digital Transformation Strategies". *Business & Information Systems Engineering*, *57*(5), pp. 339–343. https://doi.org/10.1007/s12599-015-0401-5

McAfee, A., and Brynjolfsson, E. (n.d.). *Big Data: The Management Revolution*, Harvard Business Review, 90(10), pp. 60-68.

North, K., Hermann, A., Ramos, I., Aramburu, N., and Gudoniene, D. (2020). The VOIL Digital Transformation Competence Framework. Evaluation and Design of Higher Education Curricula. In A. Lopata, R. Butkienė, D. Gudonienė, and V. Sukackė (eds.), *Information and Software Technologies* (Vol. 1283). Springer International Publishing, pp. 283-296. https://doi.org/10.1007/978-3-030-59506-7_23

Nosova, S., Norkina, A., Makar, S., and Fadeicheva, G. (2021). "Digital transformation as a new paradigm of economic policy". *2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society*, *190*, pp. 657-665. https://doi.org/10.1016/j.procs.2021.06.077

Onen, D., 2016. *Appropriate Conceptualisation: The Foundation of Any Solid Quantitative Research*.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D., (2021). "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews". *BMJ*, *372*, n71.

Reese, S., 2022. "Writing the Conceptual Article: A Practical Guide". *Digital Journalism*, *11*, pp. 1-16. https://doi.org/10.1080/21670811.2021.2009353

Reis, J., and Melão, N., 2023. "Digital transformation: A meta-review and guidelines for future research". *Heliyon*, *9*(1), e12834. https://doi.org/10.1016/j.heliyon.2023.e12834

Remane, G., Hanelt, A., Wiesböck, F., and Kolbe, L., 2017. Digital maturity in Traditional Industries – An Exploratory Analysis.

Risal, R., Giriati, G., Wendy, W., and Malini, H., (2024). Firm Size, Profitability, and ESG Disclosure in Indonesia: Geographical Location As Moderating Variable. *International Journal of Economics Development Research (IJEDR)*, *5*(2), Article 2.

Shea, B. J., Reeves, B. C., Wells, G., Thuku, M., Hamel, C., Moran, J., Moher, D., Tugwell, P., Welch, V., Kristjansson, E., and Henry, D. A., (2017). AMSTAR 2: A critical appraisal tool for systematic reviews that include randomised or non-randomised studies of healthcare interventions, or both. *BMJ*, j4008. https://doi.org/10.1136/bmj.j4008

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., and Haenlein, M., (2021). "Digital transformation: A multidisciplinary reflection and research agenda". *Journal of Business Research*, 122, pp. 889-901. https://doi.org/10.1016/j.jbusres.2019.09.022

Vial, G., 2019. "Understanding digital transformation: A review and a research agenda". *The Journal of Strategic Information Systems*, *28*(2), pp. 118-144.

Vilken, V., Kalinina, O., Barykin, S., and Zotova, E., 2019. Logistic methodology of development of the regional digital economy. *IOP Conference Series. Materials Science and Engineering*, 497(1). https://doi.org/10.1088/1757-899X/497/1/012037

Wang, S., Song, Y., and Zhang, W., 2024. "A Study on the Impact of Digital Transformation on Green Resilience in China". *Sustainability*, *16*(5), 2189. https://doi.org/10.3390/su16052189

Westerman, G., Bonnet, D., and McAfee, A., (2014). *Leading digital: Turning technology into business transformation*. Harvard Business Review Press.

Whiting, P., Rutjes, A., Reitsma, J., Bossuyt, P., and Kleijnen, J., (2003). The development of QUADAS: a tool for the quality assessment of studies of diagnostic accuracy included in systematic reviews. *BMC Medical Research Methodology*, 3, 25.

Zhao, R., and Fan, J., 2024. "Digital Policy Quality and Enterprise Innovation: The Case of China's Big Data Comprehensive Pilot Zone". *Sustainability*, *16*(12), 5032. https://doi.org/10.3390/su161250

O *Repressive Regime Lobbying* na União Europeia

Bruno Miguel Manuel Oliveira

Segundo Ano do Curso de Licenciatura em Ciência Política e Relações Internacionais, Universidade Nova de Lisboa

Introdução

São vários os desafios geopolíticos e geoeconómicos que a União Europeia (UE) enfrenta. Por um lado, a nível externo, a UE depara-se com um conflito armado prolongado na sua vizinhança oriental, dificuldades geoeconómicas face a outras potências económicas, nomeadamente a China e os Estados Unidos da América (EUA), e ainda tensões com o seu principal aliado atlântico, os EUA. Por outro lado, as questões internas, como o crescimento do euroceticismo da extrema-direita, a falta de competitividade económica ou a crise de legitimidade democrática, também dificultam a atuação externa da União Europeia.

No entanto, existe um problema cujo nível de perceção é muito reduzido fora dos corredores de Bruxelas: o *repressive regime lobbying* (RRL). Este tipo de *lobbying* não só tem implicações em termos securitários, como também coloca em risco a democracia e transparência institucional da própria União Europeia, uma vez que é praticado por países terceiros cujos regimes políticos são caracterizados pelo autoritarismo e pelo desrespeito pelos direitos humanos.

O caso do Qatargate revelou, em 2022, pela primeira vez, as brechas e as falhas do sistema europeu relativamente à regulação do *lobbying* e como diversos Estados terceiros utilizavam essa fragilidade para alcançarem os seus objetivos, fossem eles de caráter político, económico ou militar[1].

Tendo em conta este conceito, o objetivo deste trabalho consiste numa análise às implicações decorrentes do RRL existente na UE, mais concretamente no âmbito das políticas de segurança e defesa da organização e ao nível da própria democracia europeia.

O primeiro capítulo abordará as principais problemáticas e teorias relacionadas com o *lobbying* e grupos de interesse na sua generalidade, bem como a importância do RRL enquanto vertente do mesmo. O segundo capítulo analisará os caso de estudo de maior

1 O "Qatargate" resultou de uma investigação da Justiça belga a alegadas ofertas do Qatar e de Marrocos a eurodeputados e assistentes de grupos do PE para influenciar decisões em Bruxelas, numa operação que resultou na apreensão de malas de dinheiro com um total de 1,5 milhões de euros. Ver: https://expresso.pt/internacional/2023-01-11-Qatargate-Eurodeputada-demite-se-da-presidencia-de-subcomissao-do-Parlamento-Europeu-01ba11d0

impacto dentro da área e o impacto do RRL na União Europeia e nas suas instituições, com especial ênfase para o Parlamento Europeu (PE), abordando ainda as estratégias predominantes de *lobbying* conduzidas por países externos à comunidade europeia, cujos governos são marcadamente antidemocráticos e avessos à defesa dos direitos humanos, tal como a Rússia e a China, para promover os seus interesses nacionais e divisões no seio da UE. O terceiro e último capítulo terá como foco as implicações e os riscos deste tipo de *lobbying* na política securitária da União Europeia, seja a nível político-militar, seja em termos de segurança económica, bem como abordará as implicações do RRL, mas a partir de uma perspetiva direcionada para a legitimidade e transparência das instituições da UE.

1. Enquadramento teórico e conceitual

1.1. Grupos de Interesse, *Lobbying* e Influência

Para melhor se entender o conceito de *repressive regime lobbying* (RRL) é imprescindível conhecer e analisar primeiro os conceitos-base subjacentes a este: grupos de interesse, *lobbying* e influência.

Começando pelo primeiro, a definição de grupo de interesse é uma tarefa complexa e depende, em grande medida, do paradigma e da perspetiva teorética utilizados nessa mesma definição. Existem três modelos teóricos principais na literatura: pluralismo, corporativismo e neopluralismo. Se, por um lado, o pluralismo defende a existência de numerosos e pequenos grupos formados, essencialmente, por indivíduos, que influenciam as políticas públicas, por outro lado, o corporativismo traduz-se na existência de poucos e monopolísticos grupos, nomeadamente sindicatos e organizações patronais, que trabalham diretamente com o Estado, para permitir uma harmonização de interesses (Lisi et al., 2022). O neopluralismo funciona como uma terceira via entre as suas abordagens teóricas supracitadas, focando-se noutras formas de atuação como os "triângulos de ferro", isto é, grupos de interesse, comissões parlamentares e burocracias governativas, ou redes temáticas (*issue networks*) entre os diversos atores relativamente a áreas específicas (Heclo, 1978).

Neste sentido, não é possível integrar os atores-chave do RRL (Estados e respetivas empresas) numa categorização teórica, não obstante a existência de diversos aspetos comuns com o modelo pluralista. No seu conjunto, estes constituem um grupo de interesse *de facto*, visto que, mesmo atuando de forma individual e sem cooperação, os Estados têm objetivos similares e as suas ações têm influência e impacto no processo de tomada de decisão no seio da UE.

No que toca ao *lobbying* (ou lóbi de base), a sua definição também é complexa, mas pode ser considerado como uma das estratégias predominantes de tentativa de influência nos processos de tomada de decisão, especialmente à luz da teoria pluralista (Lisi et al., 2022). Para este trabalho será utilizada a definição de *lobbying* proposta por Lester Milbrath (1963): "Lobbying is the stimulation and transmission of a communication, by

someone other than a citizen acting on his own behalf, directed to a governmental decision-maker with the hope of influencing his decision". Simultaneamente, Milbrath apresenta três elementos constitutivos para esta definição, que serão tidos em conta na definição de *lobbying* utilizada neste trabalho. Em primeiro lugar, o *lobbying* deve envolver decisões governamentais e não de caráter privado. Em segundo lugar, deve existir uma intenção de influenciar essas mesmas decisões governamentais. Em último lugar, o *lobbying* só existe quando é realizado através de um intermediário, como, por exemplo, uma empresa.

Para além do *lobbying*, existem outras técnicas utilizadas pelos grupos de interesse ou outros atores que exercem influência e pressão nos processos decisórios. Uma delas é o contacto direto e recorrente com os decisores políticos, principalmente através da prática da porta giratória (*revolving door*). Esta prática consiste no recrutamento, por parte de organizações privadas, na sua maioria, de políticos e outros funcionários públicos. Desta forma, as empresas e outras organizações privadas (ou mesmo estatais) têm acesso a informações e contactos dentro da organização onde a pessoa recrutada exercia funções. Simultaneamente, esta prática também procura influenciar o rumo da definição de agenda (*agenda-setting*) dos governantes.

Estas estratégias podem ser divididas em dois tipos: estratégias diretas ou indiretas. Por um lado, as estratégias diretas têm por base o contacto direto entre o interesse organizado e os decisores políticos, estabelecido por um intermediário entre as duas partes, permitindo assim uma maior proximidade entre o grupo e os governantes. Esta é a estratégia preferencial no RRL. Por outro lado, as estratégias indiretas têm como objetivo principal a consciencialização da opinião pública para certos temas, motivando a sua mobilização nesse sentido, para levar à ação dos governantes (Weiler, 2015). A escolha do tipo de estratégia a adotar passa, em grande medida, pela posição do grupo. Estes podem ser caracterizados como *insider* ou *outsider*. Um grupo que seja *insider* tem uma rede de contactos individuais com os governantes e, portanto, maior facilidade em adotar estratégias diretas. Os grupos de caráter *outsider*, contrariamente aos *insiders*, não têm contacto direto com os decisores políticos, o que faz com que seja mais fácil usar estratégias indiretas (Weiler, 2015).

Intimamente relacionadas com os conceitos de grupo de interesse e de *lobbying*, existem outras questões pertinentes que podem ser levantadas: O que é a influência? Como podemos medir a influência?

Uma vez mais, não existe uma definição universal do que é influência. Por ser extremamente difícil encontrar e avaliar casos empíricos, devido à discrição deste tipo de atividades, existem duas correntes principais na literatura relativamente à medição de influência. Uma primeira corrente defende que a influência não pode ser medida, em primeiro lugar, porque os modelos de medição são incompletos, e, em segundo lugar, porque o estudo do *lobbying* ocorre, maioritariamente, na fase final do processo de tomada de decisão, onde a influência existe em menor escala (Baumgartner, 1998). Outra corrente é da opinião de que é possível levar a cabo essa medição da influência, apesar da extrema dificuldade da tarefa (Dür, 2008).

1.2. O que é o Repressive Regime Lobbying (RRL)?

O RRL constitui uma noção que surgiu pela primeira vez em 2022, em decorrência do escândalo do Qatargate, introduzida pelo centro de pesquisa independente Corporate Europe Observatory (CEO), por meio de um artigo intitulado "Qatargate: Time to close the door on repressive regime lobbying".

A característica essencial do RRL é que este é praticado por regimes políticos de caráter autoritário/autocrático ou híbrido, através das mais variadas estratégias e táticas supracitadas, de forma a alcançar os seus objetivos e interesses. No processo de categorização da natureza do regime será utilizado para este trabalho o Índice de Democracia do ano de 2023 publicado pelo *Economist Intelligence Unit* da revista *The Economist*. Neste índice é utilizada uma escala de medição de 0,00 a 10,00, constituindo 0 o regime mais autoritário e 10 o regime mais democrático. Nesse sentido, existem quatro categorias principais: regimes autoritários (de 0,00 a 4,00), regimes híbridos (de 4,01 a 6,00), democracias imperfeitas (de 6,01 a 8,00) e democracias plenas (de 8,01 a 10,00).

Importa também notar que o RRL, tal como o *lobbying* em termos gerais, ocorre necessariamente através de um intermediário, seja ele uma empresa privada ou estatal (empresas de consultoria ou de relações públicas, por exemplo), uma organização nãogovernamental (ONG) ou um *think tank*.

2. O *Repressive Regime Lobbying* em ação

Neste capítulo serão apresentados os casos de estudo dos Estados mais pertinentes para a análise do RRL na União Europeia, nomeadamente a Rússia e a China.

2.1. Rússia

Começando por um dos mais ativos Estados lobistas, a Rússia tem um longo historial de *lobbying* dentro da UE, sendo que o país encontra-se na 144.ª posição do Índice de Democracia do *The Economist*, com uma pontuação de 2,22.

De acordo com um estudo publicado em 2015 pelo Corporate Europe Observatory (CEO), um dos primeiros registos de atividade russa ocorreu em 2006, ano em que a Rússia contratou a empresa europeia de relações públicas GPlus para trabalhar de perto com o gabinete de imprensa do presidente. Um ano depois, a maior empresa de energia da Rússia, a Gazprom, também aderiu aos serviços da GPlus. Através desta empresa o governo russo e a Gazprom aplicavam uma estratégia direta através do fenómeno da porta giratória, o que permitia a ambas as entidades russas ter contacto direto com antigos funcionários da UE que eram contratados pela GPlus. Entre eles encontravam-se os próprios fundadores da GPlus, Peter Guildford e Nigel Gardner, ambos antigos porta-vozes de instituições da UE, ou Bruno Dethomas, antigo porta-voz da Comissão Europeia, responsável pelas relações com os países vizinhos da UE da Europa de Leste e embaixador da UE no Brasil, Polónia e Marrocos.

Durante os anos em que a Rússia usufruiu dos serviços da GPlus, os seus objetivos principais foram a suavização da perceção no seio europeu relativamente ao desrespeito pelos direitos humanos e repressão interna, uma vez que a Rússia assumiu a presidência do grupo G8 em 2006, bem como a perseguição dos seus interesses económicos no setor energético, mais concretamente a construção do gasoduto *Nord Stream*, onde o antigo chanceler alemão Gerhard Schröder fez parte do conselho de administração imediatamente após a sua saída de funções.

Em 2014, com a anexação da Crimeia pela Rússia, houve uma ligeira inversão de política por parte da UE, marcada também por um certo grau de ambiguidade. Por um lado, o primeiro pacote de sanções à Rússia foi aplicado a 17 de março do mesmo ano (com a aplicação progressivamente de mais sanções) e o projeto de construção do gasoduto *South Stream* (entre a Rússia e a Europa através do Mar Negro) não avançou por decisão europeia. Por outro lado, no ano seguinte, a Alemanha celebrou um contrato com a Rússia, dando início à construção do gasoduto *Nord Stream 2* e colocando em evidência mais uma vitória dos esforços russos (Karlsen, 2019).

Entre 2015 e 2022, a Rússia prosseguiu com as suas práticas de *lobbying*, desta vez orientadas para a atenuação das sanções impostas pela União Europeia. Durante estes anos, a Rússia aumentou o número de organizações lobistas presentes na UE. Segundo o Registo de Transparência da UE, neste período, foram registadas onze das atuais dezasseis organizações que declaram atividades de *lobbying* na UE. Apesar do reduzido número, a ONG Transparency International EU apresenta pelo menos mais 85 organizações com ligações à Rússia e aos seus interesses (Kergueno, 2022). Para além das sanções, o *lobbying* russo também sofreu um processo de diversificação, abordando questões como as relações externas da União Europeia com países terceiros, com destaque para a Turquia, ou as suas dinâmicas internas, como o caso do Brexit (Karlsen, 2019).

O conflito militar originado pela invasão da Ucrânia pela Rússia foi o ponto de inversão total nas relações UE-Rússia, mas isso não implicou uma alteração na estratégia de *lobbying* russo. Tal como ocorreu em 2014, o *lobbying* russo mantém como objetivos elementares a atenuação das sanções na sua economia e a promoção de negócios na área do setor energético, nomeadamente no que toca à exportação de recursos naturais (Khoma, 2024). Recentemente, foram divulgados por diversos órgãos de comunicação europeus, entre eles o *Financial Times* e o *Politico*, vários casos de *lobbying* russo. A 31 de janeiro de 2025, foi relatado pelo *Financial Times* que a maior empresa russa produtora de gás natural liquefeito (GNL), Novatek, tentou recorrer ao *lobbying* com *think tanks* europeus, mais precisamente o Bruegel, o European Policy Center e o Center for Regulation in Europe, contra sanções mais apertadas da UE, num momento em que os líderes europeus discutiam um aumento das restrições à importação de GNL proveniente da Rússia.

Em 2024, antes das eleições europeias, um escândalo de influência russa surgiu no seio do Parlamento Europeu: o Russiangate. Tal como noticiado em março do mesmo ano pelo jornal *Politico*, o caso envolveu o website "Voice of Europe", que era utilizado como canal de propaganda russa por Viktor Medvedchuk, um oligarca ucraniano próximo de Vladimir Putin, três meses antes do decorrer das eleições europeias. Neste caso

estiveram ainda presentes suspeitas de corrupção, tendo o primeiro-ministro belga da altura, Alexander De Croo, declarado que membros do Parlamento Europeu foram contactados e pagos pela Rússia para promover a imagem do país na opinião pública europeia (*Politico*, 2024). Em seguimento deste caso, o Parlamento Europeu adotou a resolução 2024/2696 (RSP), denominada "New allegations of Russian interference in the European Parliament, in the upcoming EU elections and the impact on the European Union", denunciando o caso e outras tentativas de influência russa na UE, com ênfase para os ataques cibernéticos e propaganda na sociedade civil. A resolução também apresentou uma série de outros casos de envolvimento russo, como o do eurodeputado eslovaco Miroslav Radačovský, que trabalhava de perto com o Estado russo, ou do também eurodeputado do partido Alternativa para a Alemanha (Alternativ für Deutschland, AfD) Maximilian Krah, acusado de receber fundos de agentes do Kremlin. O documento também expõe os contactos realizados entre o antigo eurodeputado e atual presidente do partido *Junts per Catalunya*, Carles Puigdemont, e o diplomata russo Nikolai Sadovnikov na véspera do referendo independentista de 2017.

O historial de *lobbying* russo coloca em evidência uma linha de continuidade na sua estratégia de influência. O *lobbying* russo apresenta tanto objetivos de longo prazo como a curto prazo. O principal objetivo a longo prazo assenta numa política de "dividir e conquistar" entre os países da UE, recorrendo a diversas táticas, com um aumento crescente do recurso às novas tecnologias e ao meio digital, quer seja em ciberataques, quer através de estratégia indireta, como a mobilização da opinião pública. A curto prazo encontram-se os interesses económicos, alterando o seu foco de acordo com a conjuntura internacional e com a progressão das sanções europeias. No entanto, independentemente do caráter temporal do objetivo, existem duas finalidades imutáveis: a afirmação do poder e interesses russos e o enfraquecimento dos seus rivais económicos e políticos (UE e EUA) (Karlsen, 2019). Importa ainda notar que no que toca às ligações entre a Rússia e membros do Parlamento Europeu, existe uma forte afinidade entre os partidos políticos de extrema-direita e de extrema-esquerda, tal como demonstram os casos acima referidos e diversas votações de resoluções críticas da Rússia que não foram apoiadas pelo grupo europeu A Esquerda ou o antigo Identidade e Democracia.

2.2. China

Outra potência muito presente no setor do *lobbying* europeu é a China, país com uma pontuação de 2,12 no Índice de Democracia, ocupando a 148.ª posição, muito perto do resultado da Rússia. Segundo o estudo "Chinese Influence Operations" do *Institut de Recherche Stratégique de l'École Militaire* (Charon e Vilmer, 2021), a estratégia chinesa assenta em nove pilares essenciais: a diáspora, os *media*, a diplomacia, a economia, a política, a educação, os *think tanks*, a cultura e a manipulação de informações. Destes nove pilares serão abordados com maior destaque a economia, a diplomacia e a política.

O grande desafio que se coloca à análise da presença de *lobbying* e influência chinesa na União Europeia é o nível de discrição da mesma. Simultaneamente, a literatura

existente na área do RRL é muito voltada para o *lobbying* russo e em muitas ocasiões é difícil fazer a distinção entre *lobbying* e influência chinesa e a realização de negócios e outras transações económicas (Godement e Vasselier, 2017).

No entanto, é possível identificar um elemento comum na literatura: a importância vital da estratégia da Iniciativa do Cinturão e Rota (*Belt and Road Initiative* ou *One Belt, One Road*). Em 2013, o presidente chinês, Xi Jinping, anunciou aquele que seria um dos planos de desenvolvimento económico mais ambiciosos de sempre, consistindo na conexão entre a Ásia aos continentes europeu e africano. Esta ligação seria feita em diversos níveis e setores, com destaque para os investimentos em infraestruturas como portos, estradas, linhas férreas, mas também no setor das telecomunicações. Se para alguns a iniciativa foi vista como o apogeu da globalização económica, para outros, nomeadamente a literatura ocidental, esta não passou de um plano para aumentar as capacidades geopolíticas e económicas e o poder da China (Khanal e Zhang, 2023).

A iniciativa não passou despercebida na Europa e, ainda no próprio ano de lançamento do projeto, tanto a Bielorrússia como a Moldávia aderiram. Dois anos depois começam a aderir mais países europeus, especialmente no Leste Europeu, como a Polónia, a Hungria e a Roménia, entre outros. O processo de expansão europeu continuou até 2019, ano em que a Itália aderiu, tendo o país, entretanto, abandonado a iniciativa em 2023, ano em que se comemorava uma década de existência do programa (McBride, Berman e Chatzky, 2023).

Durante o período de 2013 a 2019/20, a Iniciativa do Cinturão e Rota teve bastante sucesso e impacto na Europa, com a esmagadora maioria dos países europeus a usufruir do investimento direto estrangeiro chinês, fruto dos esforços lobistas e da influência progressiva da China. Contudo, em 2019/20, a pandemia Covid-19 assolou o continente europeu e o resto do mundo, o que provocou consequentemente um afastamento das relações UE-China, que até ao momento viam a interconectividade económica como um ponto positivo nas relações entre ambos.

Depois da pandemia e da subsequente retoma das economias, a interconexão económica voltou a ser o assunto do dia. Se, por um lado, a iniciativa chinesa perdeu vigor na Europa, por outro lado as relações económicas entre ambas as partes permaneceram, o que levou a uma alteração de direção na política lobista, focando-se mais em outros aspetos económicos.

Um desses aspetos remete para um dos principais motores da economia europeia, o mercado automóvel e a produção de veículos elétricos. Sendo este um terreno em que a China começa a apostar cada vez mais, não é surpreendente que os seus esforços de *lobbying* tenham tomado esta nova direção. Quando a União Europeia começou a equacionar a implementação de tarifas aos veículos elétricos produzidos na China, esta utilizou a sua influência de forma a mitigar os efeitos resultantes das tarifas, com o próprio presidente chinês a realizar diversas visitas à Europa, durante as quais reuniu com chefes de Estado e de Governo, entre eles o presidente de França, Emmanuel Macron, o primeiro-ministro espanhol, Pedro Sánchez, ou a presidente da Comissão Europeia, Ursula von der Leyen (Geraci, 2024).

Outra das prioridades da influência da China no continente europeu é a mobilização das massas e a manipulação da opinião pública, muito assentes numa política de estratégia indireta e interligada com o *soft power* chinês. Com esse objetivo em mente, são criadas diversas associações de amizade entre o país oriental e os países da União Europeia, tanto a nível bilateral, a German Chinese Friendship Association, como em termos da organização na totalidade, com destaque para o Grupo de Amizade UE-China, EU-China Friendship Group na designação em língua inglesa. Este grupo, fundado em 2006, tinha como missão o aprofundamento das relações entre a UE e a China, especialmente no que toca ao comércio entre ambas as partes. Na legislatura anterior, o grupo era composto por cerca de quarenta eurodeputados, cujo líder, o checo Jan Zahradil, era vice-presidente do Comité de Comércio Internacional do Parlamento Europeu durante as negociações do Acordo global de Investimento UE-China (EU-China Comprehensive Agreement on Investment) e o Secretário-Geral era o primeiro oficial da UE de nacionalidade chinesa, Gai Lin (Charon e Vilmer, 2021). Desde a sua fundação, o grupo realizou diversas visitas à China, sempre a convite de instituições chinesas e em estreita ligação com outros órgãos do Partido Comunista Chinês (*Politico*, 2020). Após investigações do Comité Especial sobre a Interferência Estrangeira em Todos os Processos Democráticos na EU (INGE) e acusações de proximidade entre este grupo e as autoridades chinesas, atuando simultaneamente fora dos canais oficiais da UE, o Grupo de Amizade UE-China acabou por ser suspenso em janeiro de 2021 (*Politico*, 2021).

As controvérsias com a influência chinesa já haviam sido debatidas aquando da abertura de várias investigações a outros oficiais da UE suspeitos de entregarem informações confidenciais às autoridades chinesas meses antes (*Politico*, 2021), mas permaneceram até ao período das eleições europeias, quando o Parlamento Europeu denunciou, através da já supracitada resolução 2024/2696 (RSP), as suspeitas de espionagem do assistente de Maximilian Krah, eurodeputado alemão da extrema-direita.

Importa ainda referir que a estratégia indireta chinesa passa ainda pelo financiamento de *think tanks* e de organizações não governamentais (ONG), cujas missões estejam em sintonia com os interesses chineses, com destaque para os países da Europa Central e de Leste, uma vez que estes têm uma posição mais endurecida para com a China (Godement e Vasselier, 2017), através do Instituto China-CEE.

3. As Implicações do RRL na segurança e democracia europeias

Os dois casos de estudo analisados no capítulo anterior permitem uma visão geral das fragilidades a que a União Europeia está sujeita no que toca a influências externas de países terceiros. Esta exposição da União Europeia face a influências externas acarreta consequências não só a nível das políticas de segurança e defesa, mas também em termos da própria democracia europeia.

Em primeiro lugar, por um lado, a segurança europeia, ou seja, a segurança dos cidadãos europeus, fica comprometida em diversos níveis. Por um lado, a troca de

informações confidenciais entre eurodeputados, oficiais e outros funcionários da União Europeia e as autoridades desses mesmos países terceiros cria automaticamente brechas na segurança. Com efeito, esta troca de informações permite que estas fiquem na posse Estados autocráticos com uma agenda antieuropeia, que desrespeita os valores europeus. Esses Estados recorrem à respetiva influência para criar divisões no seio europeu (Karlsen, 2019), para além das ligações entre membros de instituições e organizações europeias e os serviços secretos de países externos.

Por outro lado, estes Estados também utilizam a sua influência com o objetivo de aumentar o seu poder geoeconómico e defender intransigentemente os seus interesses económicos vitais, em detrimento da economia europeia. Tanto a Rússia como a China servem-se das relações comerciais com a União Europeia como um instrumento de pressão, explorando a dependência europeia em relação aos recursos energéticos. No caso da Rússia, o gás natural liquefeito permanece um ponto frágil na política energética europeia, colocando a UE numa encruzilhada entre o fornecimento de gás a preços acessíveis ou a colaboração económica com um Estado beligerante (Hockenos, 2025). No caso chinês, as terras-raras assumem um papel preponderante no novo modelo de economia verde, devido à sua centralidade no processo de manufaturação de tecnologias limpas, com destaque para a indústria automóvel com o fabrico de veículos elétricos, área em que a União Europeia e a China são concorrentes, mas onde a primeira está altamente dependente desta última (Patey, 2024).

A interdependência económica entre a UE e a Rússia esteve sempre presente ao longo da história recente de ambas as partes, mas, num primeiro momento com a anexação da Crimeia, e depois com o início do conflito militar entre a Rússia e a Ucrânia, essa interdependência esbateu-se gradualmente. Após 2014, a posição da Rússia foi substituída em grande medida pela da China, que em termos económicos e comerciais ganha gradualmente terreno na União Europeia, apesar da estratégia de *derisking* iniciada pela UE, no seguimento da pandemia de COVID-19 (Kratz, Boullenois e Smith, 2024).

Em segundo lugar, a democracia europeia também fica fragilizada. A perpetuação da existência do RRL é utilizada por uma camada da população eurocética que vê na União Europeia uma crise de legitimidade democrática, como argumento para o seu euroceticismo e reforçando a ideia dessa mesma crise.

Sendo o Parlamento Europeu o coração da democracia europeia, a falta de transparência coloca-se como um entrave para o bom e regular funcionamento das instituições europeias e, consequentemente, torna-as um espaço propício para este tipo de atividades de maior discrição. Como causa desta falta de transparência encontra-se a escassez de regulamentação. Apesar da existência de regulamentos deste tipo de atividade na UE, estes ainda se revelam insuficientes quer em número, quer em substância. Por vezes, são também facilmente contornados, devido ao seu caráter não vinculativo em certos parâmetros. Em 2023, o Parlamento Europeu aprovou uma série de alterações às suas Regras de Procedimento, através da resolução 2023/2095 (REG), entre elas a obrigatoriedade do registo de grupos informais ou um período de seis meses durante o qual os antigos eurodeputados estão interditos de contactar atuais eurodeputados ou de participar noutras ações.

Conclusão

Através da análise destes dois estudos de caso, constata-se o nível de exposição da UE ao RRL. No primeiro caso, a Rússia, foi observada a evolução das suas práticas de *lobbying* ao longo do tempo, marcada por três momentos principais: o início das suas atividades lobistas (2006-2014), a anexação da Crimeia e as suas consequências (2014-2022) e o conflito militar entre a Rússia e Ucrânia como momento decisivo nas relações UE--Rússia (2022-atualidade). Em cada um destes momentos os objetivos do *lobbying* russo também foram sofrendo alterações. Se no primeiro momento, a suavização da imagem da Rússia perante a Europa, principalmente em questões como as violações de direitos humanos, era a prioridade, esta estratégia foi evoluindo, passando o seu foco para a vertente económica. A anexação da Crimeia teve como resposta europeia o primeiro pacote de sanções à Rússia, que desde então viu-se obrigada a utilizar os seus esforços para atenuar o impacto destas, a par da defesa dos seus interesses comerciais, especialmente no setor energético. Hoje em dia, esta continua a ser a orientação geral do *lobbying* russo. O segundo caso, a China, é igualmente um exemplo da extrema importância da defesa dos interesses económicos nas políticas lobistas destes tipos de Estado, com destaque para a Iniciativa Cinturão e Rota, que ocupa um lugar essencial na estratégia de influência chinesa à escala global. Paralelamente, a tentativa de mobilização das massas e da opinião pública permanece um fator significativo da influência chinesa. Esta mobilização foca-se ainda nas elites políticas, mais concretamente com a criação de grupos de amizade que procuram uma agilização nas trocas comerciais entre a China e a UE. Contudo, a China continua a ser um país que divide opiniões, sendo considerada pela União Europeia como um parceiro, competidor e rival.

Estes dois casos apresentam diversas consequências para a UE. A nível da segurança e defesa, o facto de existirem diversas informações sensíveis em mãos dos países em questão, ligações entre funcionários europeus com os serviços secretos destes Estados e a utilização da dependência energética da UE como arma coloca em risco a defesa europeia tal como a conhecemos. No que toca à democracia europeia, esta é fragilizada, reforçando o argumento da crise de legitimidade democrática e demonstrando a falta de transparência no processo de tomada de decisão nas instituições europeias.

Por fim, importa referir dois aspetos relevantes para uma melhor compreensão deste trabalho. O primeiro incide sobre as suas limitações, nomeadamente o grau de parcialidade das fontes utilizadas. Tratando-se maioritariamente de documentos ou de notícias de instituições, organizações e órgãos de comunicação social ocidentais, por vezes, estes revelam-se pouco imparciais. O segundo aspeto está relacionado com as possibilidades futuras deste trabalho. Uma vez que o RRL foi abordado com maior detalhe a nível da União Europeia como um todo, poderá ser conduzida posteriormente uma análise do mesmo em cada Estado europeu a título individual. Além disso, apenas foram analisadas as suas implicações nas áreas da defesa e da democracia, podendo ainda ser exploradas as consequências em termos económicos ou sociais do *repressive regime lobbying*.

Referências

Baumgartner, F. R., e Leech, B. L. (1998) *Basic Interests: The Importance of Groups in Politics and in Political Science*. Princeton, NJ: Princeton University Press.

Berman, N., Chatzky, A., e McBride, J. (2023) "China's Massive Belt and Road Initiative". *Council on Foreign Relations*. Disponível em: China's Massive Belt and Road Initiative | Council on Foreign Relations [Acedido a 17 fevereiro 2025].

Boullenois, C., Kratz, A., e Smith, J. (2024) "Why Isn't Europe Diversifying from China?". *Rhodium Group*. Disponível em: Why Isn't Europe Diversifying from China? – Rhodium Group [Acedido a 25 fevereiro 2025].

Brändli, M., e Weiler, F. (2015) "Inside versus Outside Lobbying: How the Institutional Framework Shapes the Lobbying Behavior of Interest Groups". *European Journal of Political Research*, 54 (4). pp. 745-766.

Cerulus, L. (2020) "Beijing's influence in European Parliament draws fresh scrutiny". *Politico* [online] 26 de novembro. Disponível em: Beijing's influence in European Parliament draws fresh scrutiny – POLITICO [Acedido a 19 fevereiro 2025].

Cerulus, L. (2021) "EU-China 'friendship group' suspended, its chair says". *Politico* [online] 25 em janeiro. Disponível em: EU-China 'friendship group' suspended, its chair says – POLITICO [Acedido a 19 fevereiro 2025].

Charon, P. e Vilmer, J. (2021) *Chinese Influence Operations: A Machiavellian Moment*. Paris: Institut de Recherche Stratégique de l'École Militaire.

Cokeloren, H. e Braun, E. (2024) WRevealed: Russia's best friends in the EU Parliament". *Politico* [online] 6 de junho. Disponível em: Revealed: Russia's best friends in the EU Parliament – POLITICO [Acedido a 12 fevereiro 2025].

Coen, D. e Katsaitis, A. (2024) *Handbook on Lobbying and Public Policy*. Edward Elgar Publishing.

Coen, D. e Richardson, J. (eds.) (2009) *Lobbying the European Union: institutions, actors, and issues*. Oxford: Oxford University Press.

Corporate Europe Observatory (2015) *Spin doctors to the autocrats: how European PR firms whitewash repressive regimes*. Disponível em: European PR firms whitewashing brutal regimes – report | Corporate Europe Observatory [Acedido a 12 fevereiro 2025].

Dür, A. (2008) "Measuring Interest Group Influence in the EU". *European Union Politics*, 9 (4). SAGE Publications.

Geraci, M. (2024) "China's lobbying did not block the EU's new EV tariffs. But it may yet weaken them". *Atlantic Council*. Disponível em: China's lobbying did not block the EU's new EV tariffs. But it may yet weaken them. – Atlantic Council [Acedido a 17 fevereiro 2025].

Godement, F., e Vasselier, A. (2017) "Public diplomacy and lobbying: How influential is China in Europe?. China at the gates: a new power audit of EU-China Relations". *European Council on Foreign Relations*. pp. 75-88.

Heclo, H. (1978) "Issue Networks and the Executive Establishment". In *The New American Political System*, pp 87, 115-124. Edited by Anthony King. Washington, D. C.: American Enterprise Institute.

Hockenos, P. (2025) "Europe Somehow Still Depends on Russia's Energy". *Foreign Policy*. Disponível em: After Years of War, Europe Is Still Dependent on Russia's Energy [Acedido a 10 fevereiro 2025].

Karlsen, G.H. (2019) "Divide and rule: ten lessons about Russian political influence activities in Europe". *Palgrave Communications*, 19 (5). https://doi.org/10.1057/s41599-019-0227-8

Karr, K. (2007) *Democracy and Lobbying in the European Union*. Frankfurt: Campus Verlag.

Kergueno, R. (2017) *From Russia with Lobbying. Transparency International EU*. Disponível em: From Russia with Lobbying – Transparency International EU [Acedido a 29 janeiro 2025].

Khanal, S., e Zhang, H. (2023) "Ten Years of China's Belt and Road Initiative: A Bibliometric Review". *Journal of Chinese Political Science*, 29. pp. 361–395. DOI:10.1007/s11366-023-09873-z

Khoma, S. (2024) How Russia's economic lobby in the European Union works. *Ukrainska Pravda* [online] 13 Junho. Disponível em: How Russia's economic lobby in the European Union works | Ukrainska Pravda [Acedido a 10 fevereiro 2025].

Klüver, H. (2013*) Lobbying in the European Union: Interest Groups, Lobbying Coalitions, and Policy Change*. Oxford: Oxford University Press.

Lisi, M. (coord.) (2022) *Os grupos de interesse no sistema político português*. Lisboa: Fundação Francisco Manuel dos Santos.

Milbrath, L. W. (1963) *The Washington Lobbyists*. Chicago: Rand McNally.

Moury, C. (2016) *A Democracia na Europa*. Lisboa: Fundação Francisco Manuel dos Santos.

Oertel, J. (2020) *The New China Consensus: How Europe is Growing Wary of Beijing*. Londres: European Council on Foreign Relations.

Patey, L. (2024) "The European Union can go green and lower dependencies on China. Danish Institute for International Studies". Disponível em: The European Union can go green and lower dependencies on China | DIIS [Acedido a 25 fevereiro 2025].

Parlamento Europeu (2023) *Resolução 2023/2095 (REG) EP Rules of Procedure: strengthening integrity, independence and accountability*. Disponível em: Document summary | Legislative Observatory | European Parliament [Acedido a 12 fevereiro 2025].

Parlamento Europeu, 2024. *Resolução 2024/2696 (RSP) New allegations of Russian interference in the European Parliament, in the upcoming EU elections and the impact on the European Union*. Disponível em: TA [Acedido a 12 fevereiro 2025].

Voltolini, B. (2015) *Lobbying in EU Foreign Policy-making: The case of the Israeli-Palestinian conflict*. Routledge.

As Crises da Ordem Internacional: Contradições e Ameaças

Mário Alexandre Leiria dos Santos

Mestre em Ciência Política e Relações Internacionais, Faculdade de Ciências Sociais Humanas da Universidade Nova de Lisboa

Resumo

O objetivo deste *paper* é identificar quais são as ameaças à Ordem Internacional Liberal e analisar como surgiram, algo atingível por meio da pergunta de partida: "quais são as principais ameaças à Ordem Internacional Liberal?" Porém, uma reflexão mais profunda permite concluir que a Ordem Internacional Liberal tem sido frequentemente representada como em crise. Mas o que significa esta crise? De onde é que surge? Como afeta Portugal e a Europa? São estas questões que este *paper* responderá. Metodologicamente, pretendemos chegar a estas respostas por meio da revisão da literatura existente, que nos permitiu observar que a crise da Ordem Liberal é, na verdade, uma crise multifacetada, ou seja, diversas crises que se interligam. Entre estas crises e ameaças à Ordem Liberal foi possível denotar: as ações das grandes potências, desde a superpotência hegemónica até às duas grandes potências revisionistas. Ameaças que no pós-Guerra Fria ganharam preponderância com o fenómeno da globalização e as desigualdades resultantes do sistema internacional liberal. Finalmente, encontramos também crises regionais que impactaram o sistema internacional no seu todo e agravaram as outras crises.

Palavras-chave: Ordem Internacional Liberal; Portugal; Europa; Guerra Fria

Abstract

The main purpose of this paper is to identify the key threats to the International Liberal Order and analyze how they have emerged, addressed through the research question: "What are the main threats to the International Liberal Order?" A deeper analysis, however, shows that this Order has long been seen as being in crisis. But what does this crisis involve? Where does it come from, and how does it impact Portugal and Europe? These are the questions this paper aims to answer. Methodologically, we examine them through a review of the existing literature, which indicates that the crisis of the Liberal Order is multifaceted, comprising several interconnected crises. Among these crises and threats to the Order, we highlight: the actions of the great powers, from the hegemonic superpower to the two revisionist great powers; the threats that became prominent in the post-Cold War era due to globalization and the

inequalities resulting from the international liberal order; and, finally, regional crises that have affected the international system and worsened these dynamics.

Keywords: *Liberal International Order; Portugal; Europe; Cold War*

Introdução

A primeira metade da década de 2020 foi um período repleto de desafios para a Ordem Internacional Liberal. A propagação da pandemia de COVID-19 e conflitos armados em diversas partes do mundo, como na Ucrânia ou em Gaza, enfraqueceram as suas instituições e liderança. Além disso, ameaças internas corroeram os seus valores fundamentais, resultando numa crise de legitimidade. No entanto, esta crise multifacetada com que a Ordem Liberal se confronta teve origem ainda no início do século XXI, com as intervenções dos EUA no Médio Oriente a desgastarem a sua imagem internacional, e o colapso dos Lehman Brothers e a invasão russa da Geórgia a marcarem o regresso do revisionismo à agenda internacional. As consequências destes eventos alimentar-se-iam mutuamente e marcariam as décadas seguintes, com, por exemplo, a ocupação do Afeganistão só se resolver em 2021 com uma retirada apressada dos EUA, que desgastou ainda mais a sua imagem. Deste modo, este *paper* pretende investigar estas crises partindo da questão: "Quais as principais ameaças à Ordem Internacional Liberal?"

De modo a responder a esta questão, a metodologia adotada será baseada numa abordagem histórica, com uma revisão de literatura assente tanto em fontes primárias como secundárias. Em termos de estrutura, este *paper* estará dividido em três capítulos: o primeiro capítulo oferecerá uma breve explicação teórica e conceptual, abordando conceitos-chave como liberalismo, globalização e ordem internacional. O segundo capítulo analisará como as características da Ordem Liberal contribuíram para o surgimento destas crises, destacando o papel das grandes potências, tanto hegemónicas quanto revisionistas, a preponderância de ameaças transnacionais, como redes criminosas e terroristas, e o impacto de eventos como a pandemia de COVID-19 e a Guerra na Ucrânia no sistema internacional e na Ordem Liberal. O terceiro capítulo discutirá o impacto destas crises em Portugal. Por fim, a conclusão reunirá os resultados e oferecerá uma resposta à pergunta inicial.

Deste modo, a literatura existente será analisada, com a análise a ser dividida em três capítulos. O primeiro capítulo oferecerá uma breve explicação teórica e conceptual, abordando conceitos-chave como liberalismo, globalização e ordem internacional. O segundo capítulo analisará como as características da Ordem Liberal contribuíram para o surgimento destas crises, destacando o papel das grandes potências, tanto hegemónicas quanto revisionistas, a preponderância de ameaças transnacionais, como redes criminosas e terroristas, e o impacto de eventos como a pandemia de COVID-19 e a Guerra na Ucrânia no sistema internacional e na Ordem Liberal. O terceiro capítulo discutirá o impacto destas crises em Portugal. Por fim, a conclusão reunirá os resultados e oferecerá uma resposta à pergunta inicial.

Enquadramento Teórico e Conceitual – Liberalismo, globalização e Ordem Internacional Liberal

Ao longo deste capítulo iremos enquadrar o que entendemos por liberalismo, ordem internacional liberal e globalização, procurando interligar estes conceitos e destacar o que é essencial para a compreensão deste *paper*.

Começando por um breve enquadramento do que é a teoria liberal nas relações internacionais, observamos que esta teoria se baseia em três pressupostos basilares: primeiro, que os atores políticos fundamentais são os membros da sociedade doméstica, indivíduos e grupos privados que procuram promover os seus interesses, que podem optar por cooperação ou conflito consoante a conciliabilidade dos interesses, escassez ou abundância material e o nível de desigualdade de poder político. O segundo pilar é que todos os governos representam um segmento da sociedade doméstica cujos interesses se refletem nas preferências que o Estado prossegue na política internacional. Finalmente, a teoria liberal assume que a configuração das preferências de Estados interdependentes determina a sua ação (conflito ou cooperação) (Moravcsik, 1997, pp. 516-521). Estes três pressupostos indicam, por sua vez, variáveis que influenciam os níveis internacionais de conflito e cooperação: representatividade das instituições domésticas, nível de coesão e igualdade social e a extensão de interação económica transnacional. Relativamente à primeira variável, a teoria liberal deposita, de forma geral, que quanto mais representativas as instituições são, menos provável é que o governo origine conflito entre Estados; assim, independentemente da vertente liberal (republicana ou pluralista), a centralização de poder num grupo tende a elevar o risco de conflito entre Estados. Além de mais, a interdependência económica é vista por liberais como um impedimento a conflitos entre Estados dado que aumenta o potencial destrutivo que uma guerra pode ter numa economia, e assim, nos interesses materiais das populações, além de que se traduz num maior aumento de comunicação entre sociedades (Moravcsik, 1992, pp. 16-27). Com base nestes pressupostos podemos determinar que para a teoria liberal a construção de instituições que protejam o bem-estar individual, o bloco fundamental para a construção de um sistema político justo, e que limitem o poder político, é essencial para a promoção da paz, sendo esse o objetivo da Ordem Internacional Liberal, conter violência política entre Estados, em particular na Europa pós-Segunda Guerra Mundial (1939-1945) (Meiser, 2018). A teoria da paz democrática é outro ponto importante para a teoria liberal. Esta teoria defende que as democracias raramente entram em guerra entre si, pelo que promover valores democráticos e capitalistas reforça a segurança e o desenvolvimento, algo por instituições internacionais que difundem estes princípios. (Simão, 2019, p. 43). Dada a centralidade da Ordem para este *paper*, é fundamental que se analise o que este conceito em mais detalhe. Uma Ordem, nas Relações Internacionais, pode ser definida como os padrões de atividade que sustentem os objetivos primários da sociedade internacional (Bull, 1977, p. 8).

A Ordem Internacional Liberal surgiu, assim, no contexto do pós-Segunda Grande Guerra numa tentativa de *co-binding* (processo de vinculação através de instituições que

constrangem mutuamente) as potências europeias de modo a ultrapassar as dinâmicas anárquicas e de competição securitária que caracterizaram o continente, a instituição mais importante para este processo seria a Organização do Tratado do Atlântico Norte (NATO), que embora tenha surgido como resposta ao "problema soviético", foi também uma resposta ao problema que uma Alemanha revanchista poderia apresentar. A potência hegemónica americana procurou também, através do Plano Marshall, por exemplo, vincular a Europa através de instituições de interdependência económica e política, de modo a tornar futuras guerras mais custosas (as quais se destaca a Comunidade Europeia do Carvão e do Aço) É importante destacar que esta seria a segunda tentativa de impor uma ordem liberal pelos Estados Unidos, sendo a primeira a ordem wilsoniana, materializada na Sociedade das Nações (1920-1946), e sustentada em ideias de comércio livre, autodeterminação nacional e expectativas de propagação da democracia liberal. Porém, ela falharia dada a falta de arquitetura institucional para a resolução de problemas socioeconómicos ou gestão das relações entre Grandes Potências (Deudney e Ikenberry, 1999, pp. 182-185; Ikenberry, 2018, p. 14).

O sucesso e a afirmação da Ordem Internacional Liberal resultaram, em grande medida, do colapso do bloco soviético (1989-1991), que deixou os Estados Unidos da América (EUA) como a única superpotência global capaz de exercer influência determinante sobre o sistema internacional. Assim, o período pós-Guerra Fria e a consolidação da Ordem Liberal assentaram na unipolaridade e na hegemonia americana, sustentadas pelo consenso das restantes grandes potências em operar dentro desse quadro. Paralelamente, os EUA procuraram não apenas promover os valores liberais mencionados anteriormente, mas também reforçar a sua posição por meio do estabelecimento de alianças defensivas, nomeadamente a NATO no Ocidente e uma rede de acordos bilaterais no Oriente. Além disso, investiram no fortalecimento de laços estratégicos e na limitação da competição securitária com duas potências em particular: a China e a Rússia (Wright, 2014). Assim, com o fim da Guerra Fria a Ordem Internacional Liberal passava de circunscrita a metade do sistema internacional bipolar, à ordem predominante que incluía agora os seus antigos adversários (Ikenberry, 2018, p. 9)

Deudney e Ikenberry (1999) descrevem, assim, a Ordem Internacional Liberal como estando assente em três pilares: instituições internacionais, comércio livre e economias abertas e normas liberais. Em primeiro lugar, o direito internacional e organizações como as Nações Unidas procuram organizar a cooperação e a representação dos Estados para além da mera primazia estatal. Em segundo lugar, a promoção do comércio livre, apoiada por instituições económicas internacionais, visa criar um sistema de mercado aberto que torna a guerra menos provável, pois os custos económicos do conflito seriam elevados. Por fim, a ordem liberal sustenta-se em normas que valorizam direitos humanos, democracia e o Estado de direito, cuja violação pode levar a sanções e à deslegitimação do Estado infrator (Deudney e Ikenberry, 1999; Meiser, 2018).

Estas condições, por sua vez, permitiriam que o próximo conceito, a globalização, surgisse. Este conceito pode ser definido como a crescente interdependência das economias, culturas e populações a nível mundial. Provocada por trocas transfronteiriças de

bens, serviços, tecnologia, investimento, pessoas e informação. Embora algumas destas redes de movimentações já tenham séculos, este termo ganhou popularidade no pós-Guerra Fria dado o impacto no quotidiano, embora a vaga de globalização atual tenha começado em meados de 1940 devido aos esforços norte-americanos de reavivar o comércio e investimento internacional sob regras comuns negociadas (Kolb e Editor, 2018), ou seja, como consequência das instituições da Ordem Internacional Liberal implementada no pós-Guerra pelos Estados Unidos.

Em síntese, a Ordem Internacional Liberal e o processo de globalização estão deste modo interligados, dado que o último surge, em parte, como consequência dos arranjos institucionais, e a ordem internacional afirmou-se devido às interdependências que o processo de globalização originou.

A Ordem Liberal em Crise

A crise da Ordem Liberal é reconhecida tanto no meio académico como no político. Esta crise resulta da constatação de que os benefícios da Ordem Liberal já não exercem apelo suficiente para atrair tanto a potência central da ordem, os Estados Unidos, como as suas rivais, a Federação Russa e a República Popular da China. A narrativa em torno da Ordem Liberal pode ser apresentada de duas formas distintas. Por um lado, sobressai uma visão idealizada da ordem como um compromisso com princípios de cooperação multilateral e valores democráticos, impulsionada pela influência da superpotência americana, que teria promovido uma era de paz e crescimento económico. Por outro lado, existe a perceção de uma ordem imperialista liderada por uma potência hegemónica, marcada por um progresso desigual e profundas injustiças sociais, frequentemente justificada por pretextos de intervenções humanitárias que violam princípios vestefalianos como o da não intervenção e da soberania estatal. A coexistência destas duas narrativas contraditórias evidencia as tensões internas do próprio sistema, nomeadamente a incapacidade de cumprir as promessas de retirar milhões de pessoas da pobreza. Em vez disso, muitos ficaram à margem dos processos de democratização e modernização em regiões como África, Ásia e América Latina (Simão, 2019, pp. 39-41). O final da Guerra Fria, como mencionado acima, alterou fundamentalmente o alcance da ordem liberal: passou de um subsistema no interior da bipolaridade entre Estados relativamente homogéneos em termos de interesses para o único sistema sobrevivente, com Estados fundamentalmente diversos. Os desafios também evoluíram, com temas como alterações climáticas, terrorismo e proliferação de armas a ganharem cada vez maior relevância (Ikenberry, 2018, pp. 18-19).

É importante sublinhar que a liderança americana na Ordem Liberal tem sido questionada e criticada, inclusive por aliados tradicionais, devido à sua política externa, por vezes unilateral e pouco alinhada com as regulações e instituições internacionais que caracterizam esta ordem (Nye, 2004, p. 26; Ikenberry, 2018, pp. 18-19; Simão, 2019, p. 44). Um dos eventos que exemplificam esta tendência intervencionista é a invasão do

Iraque, em 2003. Durante a administração Bush, Washington encarava o Iraque de Saddam Hussein como um Estado pária. (Best et al., 2015d, p. 609). Pós-11 de setembro, a sua deposição foi concebida como meio de maximizar a segurança nacional e, simultaneamente, promover a democratização da região. No entanto, os argumentos relativos ao alegado desenvolvimento de armas de destruição em massa não obtiveram o apoio favorável do Conselho de Segurança das Nações Unidas, nem convenceram aliados tradicionais, como França e Alemanha, que se opuseram à intervenção.

Apesar disso, a invasão teve início em 20 de março de 2003 e, após a ausência de provas de armas de destruição em massa, o foco da intervenção deslocou-se para a democratização do Iraque. Embora a democracia emergente apoiada pelos Estados Unidos parecesse inicialmente progredir, rapidamente eclodiram tensões sectárias, alimentadas tanto pela perceção de imposição externa do novo sistema político como por rivalidades históricas entre xiitas e sunitas. A presença americana não conseguiu estabilizar estas clivagens, e o Iraque transformou-se num terreno fértil para a instalação de grupos associados à Al-Qaeda (Best et al., 2015d, pp. 609-612). Os anos subsequentes foram marcados pelo caos e pela violência, com estimativas de milhares de mortes civis e cerca de 2 milhões de refugiados iraquianos no exterior, além de milhões de deslocados internos, o que agravou a instabilidade regional (Best et al., 2015d, p. 613). Embora Bush tenha optado por enviar mais tropas, o seu sucessor, Barack Obama, terminou formalmente a intervenção em 2011; ainda assim, a violência sectária persistiu, culminando no surgimento do Estado Islâmico do Iraque e do Levante (ISIL), anteriormente Al-Qaeda no Iraque (Best et al., 2015d, pp. 613-614). Esta abordagem unilateral adotada pelos Estados Unidos (aqui exemplificada com a Invasão do Iraque), marcada pela negligência das normas internacionais e pela criação de alianças seletivas, consolidou a sua hegemonia global, mas enfraqueceu os fundamentos da própria Ordem Liberal. Esta contradição tornou o sistema internacional mais vulnerável a disputas, levando outras potências a questionar as normas e instituições estabelecidas. O que, por sua vez, permitiu interpretações divergentes sobre a regulação internacional, a proteção de indivíduos e a própria democracia liberal. Se para uns era "garantia de direitos", para outros consistia numa agenda para fragilizar concorrentes (Simão, 2019, pp. 42-43). Assim, este aspeto da crise liberal é sobretudo de legitimidade e propósito social, dado que o centro da ordem se deslocou do Ocidente e do Japão, mas a liderança ainda se mantém e parece contradizer os próprios princípios da ordem (Ikenberry, 2018, pp. 18-19).

Outro fator importante para a equação da crise da Ordem Liberal é a relação estreita entre a democracia liberal e o desenvolvimento económico capitalista. A intensificação da liberalização e desregulamentação económica após as crises do petróleo da década de 70 tem enfraquecido pilares fundamentais da Ordem Internacional, especialmente no quadro interno. As principais forças opositoras a uma regulamentação do sistema financeiro alinham-se em muitos casos com forças populistas e nacionalistas que procuram culpar elementos externos pelas falhas sistémicas da ordem como desigualdades económicas e pressões da globalização e da automatização sobre a classe média. A isto acrescenta-se também uma crise identitária ocidental, neste contexto cosmopolita e

multi-identitário, para a qual expressões de violência religiosa como o 11 de Setembro ou os ataques do Estado Islâmico em território europeu têm contribuído. A crise do Banco Lehman demonstrou as limitações desta interligação, que procurava equilibrar as forças de mercado e a garantia de direitos sociais. Enquanto isso, as economias de maior sucesso apresentavam uma mistura de mercado livre com gestão estatal (Ikenberry, 2018, pp. 17-18, 19-20; Simão, 2019, pp. 40-44), colocando em dúvida o modelo económico globalizado da ordem internacional (Wright, 2014, pp. 19-20). De certa forma, este desmantelamento progressivo das regulações financeiras e económicas contrariava um dos pressupostos da ordem liberal do pós-Segunda Grande Guerra: o comércio deveria ser conciliado com a estabilidade económica e a proteção do trabalho, e a "social and economic security" deveria estar alinhada com a segurança nacional. Desta perspetiva podemos encarar a crise da ordem liberal como também sendo do seu carácter social (Ikenberry, 2018, pp. 16, 20-21).

O perigo que forças populistas apresentam à Ordem Internacional pode ser encontrado com a eleição da primeira administração Trump (2016-2021); a política externa norte-americana assumiu uma orientação mais isolacionista, centrada na defesa dos interesses nacionais e menos comprometida com a promoção de valores liberais. Paralelamente, a crescente polarização do sistema político interno dificultou o envolvimento global dos Estados Unidos, limitando, por exemplo, a capacidade de firmar novos compromissos multilaterais. Um dos aspetos mais marcantes desta administração foi a instrumentalização da política externa para denunciar o multilateralismo e contestar acordos considerados contrários aos interesses dos seus apoiantes, tanto domésticos quanto internacionais, entre os quais se incluíam figuras como Vladimir Putin (Simão, 2019, pp. 46-47). Entre estas denúncias da primeira administração Trump encontramos a saída do Acordo de Paris sobre as alterações climáticas (*Público*, 2017); a saída do acordo nuclear com o Irão em 2018 (Louro e Gomes Ferreira, 2018); e a saída da Organização Mundial de Saúde em 2020, durante a pandemia de COVID-19 (Lusa, 2020). Estas aproximações a líderes iliberais tiveram impactos significativos na Ordem Liberal, não apenas no plano material, mas também no simbólico. Além disso, a hegemonia e a liderança americana têm sido alvo de contestação por múltiplos atores: desde o radicalismo islâmico, que desde a década de 1990 se mobiliza contra os Estados Unidos e os seus aliados europeus, até às potências revisionistas, como a Rússia e a China, que contestam a atual Ordem Liberal (Simão, 2019, pp. 46-47; Leandro, 2025b, p. 448).

Assim, a crise atual da ordem liberal conjuga múltiplas dimensões: a competição entre modelos de poder, a erosão das instituições multilaterais, o declínio da confiança na democracia liberal e o fortalecimento de discursos nacionalistas e antiliberais. O resultado é um sistema internacional mais fragmentado, onde a liderança americana se vê desafiada e os fundamentos da cooperação global se tornam cada vez mais contestados.

Grandes Potências e a Ordem Internacional

A crise da Ordem Internacional Liberal tem trazido a discussão do papel das grandes potências na sua sustentação, em particular os Estados Unidos. A ordem do pós-Segunda Guerra tinha em conta as lições aprendidas do falhanço da ordem wilsoniana, com um sistema mais institucionalizado e hierarquizado e grandes potências a assumirem um papel determinante na condução do sistema internacional, enquanto os Estados Unidos assumiriam progressivamente um papel de liderança. Porém, embora a base do sistema seja multilateral, os Estados Unidos reservariam um papel mais seletivo no seu envolvimento e comprometimento com o sistema multilateral. A política externa americana, e por consequência a Ordem Liberal, assenta tanto numa lógica impositiva, mais intervencionista, como numa lógica moderada, mais moderada e focada em lógicas cooperativas. Quer duma perspetiva realista, quer institucionalista liberal, a liderança e a forma como os Estados Unidos se comportam são determinantes para a sustentação da Ordem Liberal (Simão, 2019, pp. 44-45). Porém, é de notar o papel que dois dos competidores têm no destino da ordem internacional, a Federação Russa e a República Popular da China. Assim, ao longo deste capítulo iremos explorar como as interações entre estas três potências impactaram a ordem internacional liberal. Assim, ao longo deste capítulo iremos analisar como estas potências se comportaram no sistema internacional individualmente desde a queda da União Soviética (1991) até 2008, ano de dois eventos fundamentais para a perceção da crise da ordem liberal.

Rússia

A década de 1990 caracterizou-se por um desequilíbrio de poder sem precedentes, com os Estados Unidos a afirmarem-se como a única superpotência global, enquanto a Rússia mergulhava em profundas crises políticas e económicas resultantes, sobretudo, da reforma liberal de Boris Yeltsin e de movimentos separatistas como na Chechénia (Best et al., 2015c, pp. 545-546). As expectativas de integração e cooperação com o Ocidente, alimentadas pelo fim da Guerra Fria, rapidamente deram lugar a sentimentos de desilusão e traição, levando Moscovo a abandonar a sua orientação pró-ocidental em favor de uma política externa "multivetorial" (Lo, 2008, p. 29). A renúncia de Yeltsin, em 1999, levou à ascensão de Vladimir Putin, que se apresentou como o garante da estabilidade e do controlo sobre os oligarcas. Internacionalmente, registou-se um processo de socialização entre o Ocidente e a Rússia, como indicam o Conselho NATO-Rússia e a entrada da Rússia no Conselho da Europa em 1996. Estas iniciativas visavam aproximar Moscovo do quadro normativo e institucional ocidental, promovendo a convergência económica, social e política com a Europa. Contudo, não resultaram numa verdadeira integração da Rússia em estruturas como a NATO ou a UE, nem criaram mecanismos de diálogo eficazes. Isto deveu-se em parte à desconfiança ocidental face a Moscovo e às preocupações russas com o alargamento da NATO para Leste. Contudo, a interação com a Rússia continuou dada a sua importância geopolítica, económica e militar, muito embora a

Rússia de Putin identifique, desde 2000, a NATO como uma das principais fontes de insegurança (Trenin, 2006, pp. 89-90; Freire, 2013; Best et al., 2015c, pp. 547-548; Fernandes, 2021, p. 121).

O 11 de Setembro e a Guerra do Iraque marcaram um ponto de viragem na política externa russa. O primeiro levou a Rússia a reforçar o seu apoio aos Estados Unidos e a aceitar a sua liderança internacional, em troca do reconhecimento como aliado de grande relevância. Já o segundo motivou uma tentativa de aproximação ao eixo franco-alemão da *coalition of the unwilling*, que se opunha à invasão americana do Iraque. Nenhuma destas apostas produziu resultados significativos e, entretanto, a perceção ocidental sobre a Rússia mudou: uma possível transformação democrática passou a ser vista como cada vez mais distante, aproximando-a, em termos de classificação política, da China. Em contraste, o contexto económico internacional favoreceu as finanças russas, com a forte procura e os elevados preços de recursos, como o petróleo e o gás, permitindo a Moscovo recuperar do pós-Guerra Fria e das tribulações dos anos 90 e reafirmar-se como uma potência com grandes aspirações (Trenin, 2006). Porém, a Rússia permaneceria dependente das receitas destes recursos, tornando-a vulnerável a flutuações do mercado como se veria com a crise financeira de 2008 e a pandemia COVID-19. Contudo, o desejo da Rússia de se afirmar como uma grande potência num sistema internacional cada vez mais multipolar manteve-se. Mesmo durante o mandato de interlúdio de Medvedev (2008-2012) e o retorno de Putin à presidência (2012), este objetivo continuou a orientar várias das ações que analisaremos nos capítulos seguintes.(Freire, 2020, pp. 456-458)

China

Passando agora para a China, é de notar que iniciou o seu processo de liberalização económica com Deng Xiaoping durante a década de 1980, procurando atrair tecnologia e investimento externo. Com o fim da Guerra Fria à vista, a liderança do Partido Comunista Chinês temia que as reformas económicas de Deng Xiaoping conduzissem a uma liberalização política ou à perda de controlo social, num contexto em que a imagem internacional da China se deteriorava após a resposta aos protestos de Tiananmen (1989) e a ocupação do Tibete. Com a queda da União Soviética em 1991, Pequim tornava-se na principal potência de matriz marxista-leninista, enquanto previa a deslocação do centro económico mundial para o Pacífico, impulsionada pelo dinamismo asiático. O país manteve, apesar dos problemas internos, um crescimento robusto, inclusive durante a crise financeira de 1997; contudo, a persistência de críticas internacionais relativamente aos direitos humanos reforçou o isolamento chinês. Perante o colapso soviético, Washington, enquanto a única superpotência, debateu entre estratégias de *containment* e de *engagement*. A administração Clinton por integrar a China no sistema económico internacional, decisão que consolidou a interdependência económica, mas preservou tensões políticas, sobretudo em torno de Taiwan (Best et al., 2015a, pp. 400-403).

O final da Guerra Fria, por outro lado, permitiu à China beneficiar de uma Ásia Oriental relativamente estável e pacífica, além dos bens públicos fornecidos pelos

Estados Unidos, como a garantia de rotas marítimas abertas ao comércio. Ademais, continuou a colher os benefícios económicos proporcionados pela globalização e pela liberalização do comércio internacional. Da mesma forma que muitos outros Estados, a China aspirava a integrar a Ordem Internacional, vendo nela a melhor oportunidade de desenvolvimento. Uma economia global aberta oferecia às potências emergentes a melhor chance de crescimento económico e de influência nas "regras do jogo" (Wright, 2014, pp. 11-12).

A Convergência Sino-Russa

O período unipolar[1] que se seguiu à Guerra Fria consolidou a hegemonia norte-americana e a predominância da Ordem Internacional Liberal, moldando o pensamento estratégico de Washington, que via ultrapassada a lógica da competição securitária entre grandes potências e acreditava na cooperação como via preferencial. Contudo, esta hegemonia revelou-se transitória: a ascensão da China e o ressurgimento da Rússia, que procuravam e exigiam maior influência nas suas regiões geográficas de interesse. Porém, esta acomodação não interessava a Washington, que alargava as suas alianças, tanto na Europa Oriental, através da NATO, como na Ásia-Pacífico, com o reforço de parcerias regionais. Por sua vez, este alargamento de alianças alimentou perceções de contenção em Pequim e Moscovo. Embora os Estados Unidos não pretendessem derrubar os regimes russo ou chinês, a crença de que a interação internacional poderia promover transformações internas aumentou as desconfianças destas potências face à Ordem Liberal. A insegurança agravou-se com os protestos pró-Ocidente no espaço pós-soviético e culminou em crises sucessivas com o revisionismo russo: a invasão russa da Geórgia (2008), a anexação da Crimeia (2014) (e, eventualmente, a invasão em larga escala da Ucrânia em 2022) e a intervenção na Síria em 2015. Essas ações revelavam a insatisfação da Rússia com o *statu quo*, já expressa por Putin em Munique (2007); indicavam também a afirmação de um sistema multipolar e do seu estatuto enquanto grande potência nesse sistema, bem como a determinação de ver esse estatuto reconhecido. Paralelamente, a crise financeira de 2008 fragilizou o prestígio americano e europeu, reforçando em Pequim a perceção de declínio americano e encorajando uma política externa mais assertiva. Ainda assim, ao contrário da Rússia, a China manteve interesse na estabilidade da Ordem Liberal, da qual continua beneficiária devido à sua inserção na economia global (Wright, 2014, pp. 16-21; Freire, 2020, pp. 451, 456-458).

Assim, o período pós-2008 demonstrou, simultaneamente, a fragilidade e a resiliência do sistema liberal ocidental: se por um lado este revelou sinais de desgaste, por outro confirmou a hegemonia americana. Ainda assim, a "porta da contestação" estava aberta, algo explorado pela Rússia e China, que encontraram neste ponto um fator de convergência. Contudo, esta cooperação já se verificava na década de 1990, com a desilusão russa face ao Ocidente e o isolamento chinês a permitirem uma aproximação entre

1 Identificado por Wright como sendo entre 1990 e 2008.

Moscovo e Pequim, expressa em acordos de não agressão, cooperação nuclear, desmilitarização de fronteiras e na proclamação de uma "parceria estratégica" e de uma futura "ordem multipolar", embora sem políticas comuns. Esta convergência ganhou novo fôlego no início do milénio, se tornou claro o desejo de resistir à supremacia americana e à pressão ocidental em matéria de direitos das minorias, contexto em que foi assinado o Tratado de Boa Vizinhança, Amizade e Cooperação (16 de julho de 2001) e fundada a Organização de Cooperação de Xangai (15 de junho de 2001), permitindo aprofundar a cooperação sinorussa, sobretudo na coordenação de interesses comuns na Ásia Central (Berkofsky, 2014, pp. 117-118).

Distanciada do Ocidente e encorajada pela rápida vitória na Geórgia em 2008, a Rússia passou a concentrar-se cada vez mais na Ucrânia, cuja deriva em direção ao Ocidente (sobretudo através do aprofundamento das relações económicas com a União Europeia) colidia com as suas ambições regionais. Em 2010, a eleição de Yanukovych parecia significar um realinhamento de Kiev com Moscovo; porém, a decisão de não assinar o acordo de associação com a UE em 2013 e sob pressão do Kremlin desencadeou os protestos da praça Maidan, forçando Yanukovych a fugir para a Rússia no início de 2014. Em resposta, Moscovo anexou a Crimeia e apoiou movimentos separatistas no Leste e no sul da Ucrânia, procurando negar estes territórios ao Ocidente. Perante estas ações, os países ocidentais impuseram sanções à Rússia, enquanto a Ucrânia acabaria por assinar o acordo de associação com a UE em março de 2014. Negociações em Minsk resultariam num cessar-fogo frágil e instável (Rutland, 2015), eventualmente violado em fevereiro de 2022 com a invasão russa em larga escala da Ucrânia.

A anexação da Crimeia revelaria também tensões na cooperação sino-russa. Por um lado, a Ucrânia era estrategicamente importante devido a importações militares, agrícolas e investimentos regionais. Ademais, Pequim condenava a ingerência externa, sendo este um forte ponto de crítica a Washington, sobretudo devido à ambição chinesa de reintegrar Taiwan, algo que o precedente aberto referendo na Crimeia podia prejudicar. Contudo, a China viu nas ações de Putin o positivo de contrariarem os interesses ocidentais e resultaram numa maior dependência russa face à China em matérias energéticas e económicas (Bolt, 2014, p.52). Esta postura manifestou-se no silêncio chinês face à anexação da Crimeia e reforçou-se posteriormente com a recusa em descrever as ações russas na Ucrânia como "invasão", enquadrando-as no contexto do alargamento da NATO para Leste. No dia seguinte ao início da invasão em 2022, Pequim absteve-se ainda na resolução do Conselho de Segurança da ONU que condenava a Rússia (Fernandes e Cruz, 2022, p. 9). A invasão russa da Ucrânia em 2022 seguiu-se ao anúncio de uma parceria "sem limites" entre Pequim e Moscovo, sem áreas "proibidas" de cooperação; algo encarado pelo Ocidente como um alinhamento implícito com as ações russas. Ao longo de 2023, este alinhamento materializou-se ainda mais: China e Rússia posicionaram-se mutuamente como "contrapeso" ao mundo ocidental, enquanto Pequim buscava assumir um papel preponderante nos assuntos de segurança global, facto inclusive reconhecido por Washington na conferência bilateral em novembro desse ano (Leandro, 2025a, pp. 28-32).

Porém, estas duas potências não são parceiras iguais, dada a crescente dependência russa da China, nem são tratadas de forma igual pelo Ocidente. O conceito estratégico da NATO de 2022 considera a China como um "desafiador sistémico" e a Rússia como uma ameaça direta. Já a *Bússola Estratégica da UE* (2022) considera a China como um parceiro para cooperação, mas simultaneamente, um concorrente económico e um rival sistémico, e a Rússia também como uma ameaça direta (Pizarro, 2022).

Podemos interpretar um reconhecimento, por parte do Ocidente (em particular da Europa), da Rússia como uma ameaça militar direta, face às suas ações expansionistas na Ucrânia, que ameaçam os Bálticos e a Europa de Leste. No entanto, é a China que detém capacidade para alterar profundamente a ordem internacional liberal, contrariando os interesses europeus. Apresenta uma visão alternativa, a "comunidade global de futuro partilhado", materializada, em parte, através da *Belt and Road Initiative*, que investe em grandes infraestruturas de ligação entre a China, a Ásia e a Europa. Esta visão chinesa, contudo, apresenta aspetos que colidem com valores basilares da Ordem Liberal (nomeadamente respeito pela soberania e integridade territorial), como as "preocupações legítimas de segurança" utilizadas a respeito da invasão russa da Ucrânia. Paralelamente, a China fortalece a sua influência global ao criar parcerias estratégicas e integrar fóruns como os BRICS+, o Novo Banco de Desenvolvimento e a Organização de Cooperação de Xangai, ampliando a sua rede de aliados e o controlo sobre infraestruturas críticas (Ribeiro Gomes, 2024; Tomé, 2024a).

O público-alvo destas investidas diplomáticas chinesas tende a ser, sobretudo, economias emergentes e países em desenvolvimento do Sul Global, tentando-se colocar como líder do mesmo. Contudo, resta saber se a China tem efetivamente interesse em desmantelar toda a Ordem Liberal que a beneficiou desde o fim da Guerra Fria e se terá capacidade de mundializar uma alternativa (Tomé, 2024a). A forma como esta nova ordem proposta pela China se materializará permanece incerta, incluindo o papel que Pequim desempenhará e, sobretudo, o lugar que a Rússia nela ocupa. Uma eventual visão hegemónica chinesa pode colidir com a pretensão russa de ser reconhecida como grande potência e de manter uma zona de influência sobre a Europa de Leste e a Ásia Central, regiões onde os interesses de ambos também se sobrepõem (Bolt, 2014, p. 50).

Porém, a ascensão chinesa tem sido forte de crescente oposição, em particular desde a administração Obama (2009-2017), com o chamado *pivot to the Pacific* (Clinton, 2011). O exemplo mais relevante de contenção na década de 2020 foi a fundação do pacto AUKUS em setembro de 2021.AUKUS (acrónimo de Austrália, Reino Unido e Estados Unidos) é uma parceria trilateral de segurança reforçada que estabelece um quadro de cooperação no domínio da defesa entre as três partes. Esta parceria traduz o reconhecimento, por parte de Washington, da China como uma "ameaça sistémica" e, por isso, os EUA passaram, à época, de alianças sobretudo bilaterais para uma arquitetura multilateral. Nesta arquitetura também se inseria a Trans-Pacific Partnership (2016), um acordo de comércio livre entre Japão, Austrália, Nova Zelândia, Vietname, Malásia, Bornéu, Singapura, Estados Unidos, Canadá, México, Chile e Peru. O objetivo deste acordo era a contenção da ascensão económica chinesa na Ásia, embora este objetivo

tenha sido comprometido pela saída norte-americana sob Trump (2017). O passo seguinte foi a institucionalização da parceria QUAD (Quadrilateral Security Dialogue, que agrupa Estados Unidos, Japão, Austrália e Índia), existente desde 2007 e relançada em 2017 com a primeira administração de Donald Trump (Gaspar, 2021; Rodrigues e Neves, 2021). O AUKUS, embora não altere de forma significativa a distribuição de meios no Pacífico, representa um claro posicionamento da Austrália face à "diplomacia guerreira" chinesa, levando Washington a reconhecer Camberra como um aliado indispensável na contenção da China. Ao mesmo tempo, revela uma aposta crescente dos Estados Unidos no Pacífico, procurando dificultar uma eventual ação militar chinesa na região, ainda que à custa de compromissos com a Europa, como simbolizado pela secundarização do acordo entre Camberra e Paris. Assim, o AUKUS reforça o estatuto norte-americano como potência do Pacífico e evidencia a determinação de Washington em defender os seus interesses regionais, incluindo, se necessário, através do recurso à força (Reis, 2021; Soller, 2021). A reação chinesa foi agressiva, acusando os países membros de fomentarem uma nova Guerra Fria e uma corrida aos armamentos, sendo ameaças à paz e estabilidade regional e internacional, criando clivagens regionais sobre a criação do AUKUS. A Rússia, por sua vez, apoiou as críticas chinesas ao pacto, que vê como uma afronta ao *statu quo* de uma região cada vez mais relevante para os cálculos estratégicos russos (Freire, 2021; Tomé, 2021).

As Ameaças Pós-Guerra Fria – Redes Transnacionais de Crime Organizado e Terroristas

Após analisar como os principais atores estaduais representam uma ameaça à Ordem Internacional Liberal, é importante abordar os principais atores não estaduais. No mundo globalizado do pós-Guerra Fria, especialmente após o 11 de setembro, as redes transnacionais representavam uma ameaça significativa ao sistema internacional e à soberania estatal devido à sua capacidade de atuar e movimentar-se para além das fronteiras tradicionais dos Estados-Nação. Isto destaca o aspeto globalizado e sem fronteiras destas ameaças, conforme enfatizado por Bush ao dizer que "os terroristas não têm fronteiras", mas possuem um "alcance global" (O'Loughlin, Tuathail e Kolossov, 2004, p. 10).

É relevante destacar como os processos de globalização têm beneficiado as redes transnacionais. Por exemplo, a crescente interconexão global, a interdependência financeira e o desenvolvimento de novas tecnologias, especialmente a internet, têm facilitado a ascensão de um novo tipo de fundamentalismo islâmico. Esta maior "proximidade" possibilitada pela globalização tem permitido uma cooperação mais estreita em nível internacional e uma troca livre e rápida de informações. No entanto, este contexto também tem ampliado a disparidade entre o Norte e o Sul Global, levantando questões sobre a justiça socioeconómica do sistema global. Um exemplo notável destas organizações é a Al-Qaeda, que opera para além das fronteiras tradicionais dos Estados,

transformando-se numa rede global com bases territoriais em constante mudança, células em vários países muçulmanos e uma comunidade de apoio global, que inclui desde os talibãs até comunidades on-line (Best et al., 2015b, p. 521).

Entretanto, as redes transnacionais jihadistas são apenas um exemplo das muitas organizações não estatais que se beneficiaram deste mundo globalizado. Outros exemplos incluem redes terroristas num âmbito mais amplo e até redes criminosas que aproveitam das mesmas vantagens da globalização já mencionadas. Com as barreiras ao movimento de bens e fundos removidas, torna-se mais fácil para estas organizações estabelecerem operações em diversos países, facilitando a produção e distribuição de bens ilícitos. Isto é possível graças à exploração de recursos públicos como a internet ou as rotas marítimas de comércio (Forest, 2020).

A globalização permitiu também oportunidades de interseção entre redes criminosas e redes terroristas (Forest, 2020) como Putin denotou: "terrorism, just as narco-business, has a ramified international network and without doubt bears a transnational character" (O'Loughlin, Tuathail e Kolossov, 2004, p. 10). Para ambas as redes, surgem oportunidades com a internet, já que esta facilita o acesso a armamento, redes de tráfico, crimes cibernéticos, lavagem de dinheiro, contratação de pessoal e comunicação com operativos no terreno (Forest, 2020).

As redes transnacionais de crime organizado e terrorismo desafiam a soberania dos Estados na era da globalização, mas demonstram simultaneamente a sua importância na resposta às mesmas. Devido à ameaça que representam, estas redes têm sido retratadas por forças políticas populistas e nacionalistas como uma ameaça existencial. Isto alimenta visões xenófobas do mundo, especialmente no contexto da crise identitária ocidental já identificada. Por exemplo, desde os ataques de 11 de Setembro e os subsequentes atentados na Europa, têm aumentado os sentimentos negativos em relação aos muçulmanos e ao mundo islâmico, em geral, equiparando extremistas a uma identidade religiosa ou cultural específica (Melnitsky, 2023). Esta onda tem sido aproveitada por forças políticas populistas para securitizar e militarizar a identidade. Além disso, a associação de determinados povos a redes criminosas também foi utilizada por estas forças, como evidenciado pela associação dos povos da América Latina aos cartéis de droga, conforme exemplificado no famoso discurso de Donald Trump: "When Mexico sends its people, they're not sending their best. […] They're sending people that have lots of problems, and they're bringing those problems with them. They're bringing drugs. They're bringing crime. They're rapists. And some, I assume, are good people" (A.B.C. News, 2016).

A Globalização de Crises Regionais

A década de 2020 foi inaugurada por três crises regionais de proporções significativas: a pandemia de COVID-19, a guerra na Ucrânia e a instabilidade no Médio Oriente, todas causando um impacto profundo em todos os aspetos da vida social.

COVID-19

Começando pela crise que marcaria o início da década de 2020, a COVID-19, é crucial destacar que a pandemia não gerou realinhamentos políticos, mas sim acelerou e exacerbou certas tendências pré-existentes. Por exemplo, ao analisar o impacto geoeconómico da pandemia, observa-se que seis dos sete países do G-7 e quatro dos cinco BRICS estão entre os 20 países mais afetados. Tal resultou num abrandamento económico global com efeitos profundos e distribuídos de forma desigual, levando os países que mais sofreram com a crise de 2008 a perderem as pequenas recuperações alcançadas ao longo da década de 2010. Além disso, a pandemia expôs as fragilidades da ordem internacional, embora tendências como a deterioração das relações transatlânticas, o papel disruptivo da Rússia e a rivalidade sino-americana já estivessem presentes anteriormente (Pinéu, 2020).

Outro ponto crucial a mencionar é a erosão do multilateralismo liberal e dos princípios que o sustentam, com o avanço da desregulação económica neoliberal e a ascensão da democracia iliberal de inclinação populista/nacionalista. Além disso, a pandemia evidenciou os riscos associados à crescente competição estratégica entre países e ao abandono progressivo de soluções de cooperação multilateral, num contexto em que as ameaças são complexas e requerem abordagens multilaterais para serem enfrentadas de maneira eficaz (Pinéu, 2020).

A fragilização do multilateralismo é visível em diversos aspetos, como o ataque direto à Organização Mundial da Saúde. No entanto, de forma mais subtil, observa-se uma tendência de muitos países para se voltarem para dentro, num momento que demandava cooperação internacional. A emergência sanitária serviu de pretexto para violações do direito internacional, como a recusa ao acolhimento de refugiados (Moita, 2020).

Por outro lado, esta recentralização na soberania do Estado também evidencia a importância do papel do Estado como regulador e protetor. A pandemia expôs dependências excessivas de fontes externas e as vulnerabilidades decorrentes da deslocalização de indústrias europeias estratégicas, essenciais para o combate à pandemia (Gomes, 2020). Isto levou a um movimento em direção a uma "reindustrialização" europeia (Cunha, 2020) e a um desejo de "desacoplamento" ou "redução de riscos", conforme colocado pela Presidente da Comissão Europeia, das economias ocidentais em relação à China, tema frequentemente abordado por líderes políticos.

Observa-se que tanto atores estaduais – Israel face a Gaza ou o conflito entre a Etiópia e o Egito –, como não estaduais passaram a adotar políticas agressivas e oportunistas face ao momento de fragilidade internacional, exacerbando os riscos para a segurança global. Em Estados frágeis[2], com capacidade limitada de resposta aos efeitos

2 Um Estado Frágil pode ser entendido como um Estado que perdeu controlo físico do seu território ou monopólio do uso legítimo da violência. Tem a autoridade para tomar decisões coletivas erodida, é incapaz de fornecer bens públicos, é incapaz de interagir com outros Estados como um membro pleno da comunidade internacional (Fragile States Index, 2026).

da pandemia, há uma conexão entre a insegurança alimentar e económica e o aumento da violência, com grupos radicais que aproveitam estas circunstâncias, como no caso do Afeganistão. Ao mesmo tempo, atores estatais têm usado esta oportunidade para intensificar tecnologias de vigilância social e política sob o pretexto da saúde pública, além de adotar uma postura externa mais agressiva (Pinéu, 2020).

Guerra da Ucrânia

A guerra na Ucrânia é possivelmente o exemplo mais claro deste reposicionamento agressivo e revisionista por parte de algumas potências. No contexto da eleição de Joe Biden, que prometeu que a América voltaria a assumir o papel de líder do mundo livre contra uma crescente ameaça autocrática, a guerra na Ucrânia tornou-se o primeiro desafio a esta nova visão americana (Soller, 2022). Além disso, a Guerra da Ucrânia representa o fim do mundo pós-Guerra Fria, especialmente na Europa, marcando o término da paz europeia e uma mudança nos arranjos regionais e internacionais de segurança (Gaspar, 2023). A invasão russa da Ucrânia, em que um estado violou a independência, a soberania e a integridade territorial de outro, colocou em xeque os pressupostos da Ordem Liberal e a capacidade da liderança americana de responder a desafios.

A guerra na Ucrânia também dividiu o mundo entre aqueles que apoiam a Ucrânia, os que apoiam o regime russo e os que preferem manter-se neutros. Embora se tenda a associar o primeiro grupo às democracias em geral, transformando o conflito num confronto entre democracias e autocracias, países como Brasil e Índia mantiveram-se neutros. A divisão tende a ser entre o Ocidente, representado pelo eixo euro-atlântico, o Japão, a Austrália e a Nova Zelândia ("Norte Global"), e o "Sul Global", que tende a manter-se indiferente aos eventos na Ucrânia, mantendo relações e transações normais e até aumentando o volume de trocas comerciais (Tomé, 2023).A guerra na Ucrânia também é um teste para outras tensões latentes, como Taiwan, especialmente num contexto em que a pandemia de COVID-19 permitiu à diplomacia chinesa adotar uma postura mais revisionista e confrontacional em relação ao Ocidente, acompanhada de uma maior assertividade regional, seja em Hong Kong, no Mar da China Meridional ou em relação a Taiwan (Cunha, 2020), e sobre a qual a China sempre reservou para si o direito de intervir militarmente (Cunha, 2022).

No entanto, os impactos da guerra na Ucrânia transcenderam o âmbito geopolítico, num mundo ainda a recuperar de dois anos de pandemia. As perturbações nas cadeias de abastecimento e a forte procura global elevaram os custos de produção, repercutindo rapidamente nos preços ao consumidor. Este aumento deu-se especialmente nos setores da energia e alimentação, afetados pela redução da produção russa e ucraniana e pelas sanções a Moscovo. A inflação, ao ultrapassar o crescimento salarial em muitos países, agravou o custo de vida, com efeitos negativos na saúde e no bem-estar das populações, evidenciando novamente as desigualdades da ordem internacional, onde os mais pobres suportaram o maior fardo. O conflito comprometeu também a segurança alimentar global: antes da guerra, Rússia e Ucrânia respondiam por 36% das exportações mundiais de

trigo. As economias emergentes, dependentes destes dois países para abastecimento alimentar e energético, sofreram impactos significativos, uma vez que a invasão russa bloqueou os portos ucranianos. Embora a Black Sea Grain Initiative tenha facilitado a exportação de parte do trigo ucraniano, a maior fatia destinou-se a países desenvolvidos, deixando apenas cerca de 20% para os restantes (Kilfoyle, 2023), aumentando mais uma vez as assimetrias entre Norte e Sul Global.

Médio Oriente

Outra região importante a considerar é o Médio Oriente. O intervencionismo unilateral americano na guerra do Iraque não só demonstrou que ações militares têm limites na promoção da democracia. Este intervencionismo contribuiu para o desgaste da ordem internacional ao romper com a unidade nas instituições internacionais e permitiu que o estigma da violação do direito internacional se fosse desvanecendo, abrindo precedente para o que aconteceria na Geórgia, Ucrânia e Síria (Marcos e Alcario, 2023).

Anos depois, a Primavera Árabe abalaria ainda mais a ordem, começando na Tunísia e propagando-se pela região do Magrebe e do Médio Oriente, que levaria ao derrube de décadas de ditadura, mas também, em alguns casos, ao surgimento de guerras civis que durariam anos. A Primavera Árabe acabaria também com o equilíbrio delicado da região já afetado pela Guerra do Iraque, no entanto, nenhum protesto resultaria, numa democracia estável, mas sim em duas guerras civis longas, na Síria e na Líbia, na queda de três ditaduras, na Tunísia, no Egito e na Líbia, bem como fortes respostas por parte de outros regimes. Porém, este desfecho pôs em causa a atratividade do modelo ocidental com grande parte das experiências a resultarem em guerras civis de anos, como a Síria e a Líbia, sem que nenhuma democracia consolidada surgisse. A mudança de foco estratégico da Administração Obama fez as suas advertências americanas aos regimes ditatoriais regionais inconsequentes, acabando por fortalecer as suas posições e por os aproximar de adversários como a Rússia, como foi o caso de Al-Assad na Síria. Este retraimento não seria revertido por Donald Trump, nem sequer por Joe Biden, que assumiria a retirada do Afeganistão. Esta hesitação e retirada desgastariam a imagem norte-americana enquanto potência hegemónica ao longo de mais de uma década e permitiriam que países como a China, Rússia ou Irão preenchessem os vácuos de poder deixados por Washington. Este vácuo seria aproveitado especialmente pela Rússia, que em 2015 apoiaria Al-Assad, virando a batalha a seu favor e procurando reforçar o seu estatuto de grande potência num sistema internacional tendencialmente multipolar (Wright, 2014; Freire, 2020; Marcos e Alcario, 2023, pp. 456-457). A China tem também emergido como mediadora no Afeganistão, procurando impedir a consolidação de organizações terroristas e capitalizar o fracasso norte-americano na região (Leandro, 2025a, pp. 32-33).

Por outro lado, a violência contínua entre Israel e grupos palestinianos não pareceria ter fim. Durando praticamente mais de 80 anos, seria um fenómeno recorrente ao longo do início da década de 2020 e da expansão dos colonatos israelitas. No dia 7 de outubro de 2023 teve lugar um dos maiores ataques terroristas perpetrados pelo Hamas,

que despoletou a resposta desproporcional de Israel, interrompeu um longo período de normalização de conflito no quotidiano, não havendo guerra, mas também não havendo paz, sobretudo nas áreas palestinianas. Este conflito tem gerado forte oposição, sobretudo do Sul Global, envolvendo processos no Tribunal de Justiça Internacional contra Israel e com mandados de captura do Tribunal Penal Internacional contra oficiais israelitas como o Primeiro-Ministro e o Ministro da Defesa. A abertura de uma nova frente no Líbano, depois de mais de um ano de destruição de Gaza, e posteriormente com o colapso do regime de Al-Assad e os avanços de forças israelitas por território sírio agravaram a instabilidade regional, que ameaça alastrar-se cada vez que o envolvimento direto iraniano se torna plausível. Por sua vez, o apoio incondicional americano, independente das "linhas vermelhas" desenhadas, da administração Biden, e que Donald Trump prometeu continuar, tem contribuído para o desgaste da imagem norte-americana junto do Sul Global (Ricarte, 2024; Tomé, 2024b).

O que Trump procura não é isolacionismo, mas sim um envolvimento seletivo, pautado pelo que a sua administração considerar como "interesse nacional". Inevitavelmente isto enfraquecerá, ainda mais, o multilateralismo, forçando os aliados a assumir maiores encargos na segurança e no funcionamento e na reforma das organizações internacionais. Para Trump, a força militar, a vontade de a empregar e tarifas comerciais são vistas como instrumentos geopolíticos que manterão os EUA prósperos e farão aliados e rivais recalcular as suas interações com Washington. Parte deste caminho passa pelo fortalecimento interno da indústria americana, sacrificando a globalização, de modo a perseguir os dois objetivos máximos de contenção à China e conquistar novos mercados no Pacífico emergente. Este foco no Pacífico pode, por sua vez, colocar em rota de colisão as duas margens do Atlântico, sobretudo porque o que Trump propõe em termos de política externa ameaça redefinir tudo o que sustenta a atual Ordem Internacional Liberal (Rato, 2024).

A China continuará a ser o foco da política externa norte-americana, como foi desde Obama, no primeiro mandato de Trump e no "interlúdio" de Biden. É provável que áreas em que Biden e Xi cooperaram se tornem novos campos de competição, como a inteligência artificial e as alterações climáticas. A intensificação da competição a nível económico, comercial e tecnológico é expectável. É possível especular que a estratégia de Trump passe em parte por atrair a Rússia e afastá-la da China, dada a sua pressão a Kiev para aceitar uma paz favorável a Moscovo. Porém, este caminho ameaça acelerar o colapso da rede de alianças americana e a Ordem Liberal, já que por um lado, afasta aliados como a Europa, e por outro, incentiva o expansionismo russo e chinês que pode provocar novos problemas no futuro (Tomé, 2024). É também uma incógnita se a nova administração Trump terá vontade de continuar a suportar o fardo de manter a Ordem Liberal a funcionar, ou se não se tornarão numa democracia iliberal, ou mesmo se não contribuirão mesmo para a desconstrução definitiva da Ordem Liberal (Tomé, 2024a).

Consequências no Contexto Europeu e Nacional

As crises da ordem liberal há muito que se fazem sentir no espaço europeu e nacional, considerando especialmente a evolução das relações entre as duas margens do Atlântico e como se têm alterado neste contexto de crise. A guerra do Iraque foi um ponto de viragem nas relações transatlânticas em que, mesmo com a oposição dos aliados europeus, Washington decidiu avançar com a invasão com a sua "coalition of the willing", o que gerou uma deterioração da imagem internacional americana na Europa, até ao fim da Administração Bush. A Administração Obama, embora procurasse restabelecer a convergência transatlântica, agravaria as tensões com a Europa, com a deslocação do foco estratégico americano para o Indo-Pacífico. Obama procurava assim tentando que os aliados europeus assumissem maior responsabilidade na sua segurança regional, especialmente no contexto de invasão russa da Geórgia e da Crimeia. Posteriormente, revisionismo russo conjugado com a eleição de Donald Trump, o Brexit e a instabilidade da vizinhança geográfica da Europa deixaram o espaço estratégico e securitário europeu mais frágil e instável (Marcos e Alcario, 2023).

Os efeitos da COVID-19 e da invasão russa da Ucrânia de 2022 mostraram a necessidade europeia de uma maior autonomia estratégica, dada a dependência europeia de energia russa, segurança americana e da economia chinesa, segundo a Bússola Estratégica da União Europeia (2022). A articulação com a NATO, ainda assim, continua a ser destacada como essencial para a segurança europeia, especialmente quando enquadrada no contexto que a União Europeia apresenta, em que o terrorismo e o extremismo continuam a ameaçar a paz e segurança europeia, vindo de diversas fontes. Verifica-se um risco acrescido de proliferação nuclear, tanto com o alargamento do arsenal russo e chinês como com o desenvolvimento de capacidades nucleares por Estados como a Coreia do Norte e o Irão. Atores estatais e não estatais empenham-se em ataques híbridos com Estados-membros da UE e aliados, influenciando eleições através de desinformação e tecnologias disruptivas, como a inteligência artificial, o que conjugado com fenómenos sociais – o crescimento de movimentos populistas e nacionalistas, muitas vezes eurocéticos, que instrumentalizam as crises de refugiados e o aumento das desigualdades internas – desgasta os valores liberais europeus e nacionais (Santos Pinto e Raimundo, 2016).

Neste contexto, a segunda administração Trump representa um sério risco para a União Europeia. A guerra comercial e aduaneira lançada por Donald Trump no início do seu segundo mandato teve como objetivo "quebrar" as regulações impostas pelo mercado europeu às empresas norte-americanas, nomeadamente nos setores digitais. O acordo de 27 de julho de 2025 significou uma vitória significativa para Washington, com a União Europeia a aceitar tarifas de 15% sobre bens europeus, enquanto os bens industriais norte-americanos ficaram isentos de tarifas. Em contrapartida, a União Europeia comprometeu-se a investir 600 mil milhões de dólares nos Estados Unidos e a gastar outros 750 mil milhões em compras de bens energéticos. Estas cedências decorrem, em grande medida, da dependência europeia em relação a Washington em matéria de defesa e, em particular, para a resolução da guerra na Ucrânia (Corlin, 2025). Isto, conjugado

com as intenções expressas no documento "National Security Strategy", publicado em dezembro de 2025, de promover a "european greatness" e salvá-la do declínio económico e da "civilizational erasure", indica um objetivo de subverter a União Europeia através do reforço de forças políticas "patrióticas" (isto é, de extremadireita) que se oponham ao trajeto atual do continente e de abrir o mercado europeu aos produtos norte-americanos (The White House, 2025). Por outro lado, é também importante não descurar a ameaça militar representada pelos Estados Unidos. A intervenção na Venezuela, em janeiro de 2026, demonstrou que a administração Trump não revela consideração pelo direito internacional, pilar basilar da ordem liberal. Isso torna-se ainda mais relevante quando, ao renovar as exigências de cedência da Gronelândia (território autónomo dinamarquês), Trump não excluiu o recurso à força militar norte-americana, mesmo que tal pudesse significar o fim da NATO (Euronews, 2026; Hasselbach, 2026; Khan, 2026). Assim, torna-se evidente que os Estados Unidos, sob a administração Trump, representam uma ameaça cada vez mais concreta para a União Europeia e os seus Estados-membros.

Em termos nacionais, as mudanças na distribuição de poder internacional devido à competição entre grandes potências, a erosão da ordem multilateral e as crises desencadeadas pela pandemia e pela invasão russa da Ucrânia passaram ao lado de Portugal. Os impactos das crises na Ordem Internacional Liberal sobre Portugal podem ser categorizados em duas áreas principais: materiais e simbólicas. Em termos materiais, há implicações económicas significativas, uma vez que os efeitos económicos, como a inflação e o aumento do custo de vida, resultantes de crises como a pandemia de COVID-19 e a Guerra da Ucrânia, também se fizeram sentir no país, em parte devido à intricada rede de interdependências da Ordem Liberal. Além disso, movimentos de "*decoupling*" podem prejudicar a capacidade de Portugal de manter relações profundas com alguns dos países afetados, especialmente no contexto da União Europeia. Através do ciclo de revisão do Conceito Estratégico de Defesa Nacional (2023), é possível observar um consenso em Portugal sobre a importância da consolidação do espaço transatlântico, através da articulação entre a NATO e a UE. Também que os Estados que o constituem defendam os princípios fundamentais da Ordem Liberal, como o primado do direito, o multilateralismo e uma economia global aberta e sustentável. Além disso, Portugal vê nesta ordem a melhor oportunidade para a sua projeção internacional e para promover e defender os seus interesses e assegurar a sua segurança.

Conclusão

Em conclusão, considera-se que a crise da Ordem Internacional resulta de contradições internas e de efeitos sistémicos acumulados desde o fim da Guerra Fria. Embora esteja baseada em princípios como a democracia, multilateralismo, direito internacional e livre comércio, esta ordem permanece estruturalmente marcada por profundas desigualdades entre o Norte e o Sul Global e pela hegemonia norte-americana, por vezes exercida de forma unilateral.

A globalização económica e institucional, enquanto reforçou a ordem liberal, permitiu a ascensão de potências como a China e a Rússia, que passaram a contestá-la, tanto por desconfiança face às instituições liberais quanto pela perceção de ameaças aos seus regimes políticos. Paralelamente, a desregulação neoliberal aprofundou as desigualdades socioeconómicas presentes internamente nas democracias liberais, favorecendo movimentos nacionalistas e populistas, enquanto enfraquecia o compromisso com valores fundamentais da ordem, como o multilateralismo. A abertura de fluxos financeiros, comerciais e digitais facilitou também a expansão de atores não estatais, como redes terroristas ou de crime organizado, que exploraram assimetrias globais e desafiaram a soberania do Estado. Estas fragilidades tornaram-se mais evidentes com a pandemia da COVID-19 e com a guerra na Ucrânia, crises que reforçaram o papel do Estado e expuseram os limites da globalização e do desenho da Ordem Internacional, com o ressurgimento do revisionismo no Sistema Internacional.

Finalmente, as persistentes desigualdades globais, agravadas pelas crises da década de 2020, levantaram dúvidas sobre o caráter internacional e liberal da Ordem, sobretudo devido à adesão seletiva dos Estados Unidos às instituições da Ordem. Neste contexto, o futuro da Ordem Liberal permanece incerto, com a liderança norte-americana crescentemente contestada e a China emergindo como um polo de poder alternativo. Em última análise, a centralidade e a unilateralidade das ações norte-americanas revelaram-se fatores-chave na erosão da ordem que sustentou a sua hegemonia, produzindo efeitos diretos para Estados como Portugal. Isto, por sua vez, agravou-se quando o principal parceiro europeu, os Estados Unidos, passou a manifestar-se como uma ameaça aos princípios da ordem (como integridade territorial) no espaço euro-atlântico.

Referências

A.B.C. News (2016) *What Donald Trump Has Said About Mexico and Vice Versa*. 31 de agosto. Disponível em: https://abcnews.go.com/Politics/donald-trump-mexico-vice-versa/story?id=41767704 (Acedido em: 9 de janeiro de 2026).

Berkofsky, A. (2014) "Russia and China: The Past and Present of a Rocky Relationship", *Il Politico*, 79(), pp. 108-123.

Best, A. et al. (2015a) "The People's Republic of China and North Korea: Ideology and Nationalism, 1949-2014", in *International History Of The Twentieth Century and Beyond*. 3.ª ed. Routledge, pp. 385-410.

Best, A. et al. (2015b) "The Rise Of Political Islam: 1928-2014", in *International History Of The Twentieth Century and Beyond*. 3.ª ed. Routledge, pp. 501-532.

Best, A. et al. (2015c) "The End of the Cold War and the «New World Order», 1980-2000", in *International History Of The Twentieth Century and Beyond*. Routledge, pp. 533–554.

Best, A. et al. (2015d) "US Decline In A Globalized World?", in *International History Of The Twentieth Century and Beyond*. 3.ª ed. Routledge, pp. 605-629.

Bolt, P.J. (2014) "Sino-Russian Relations in a Changing World Order", *Strategic Studies Quarterly*, 8(4), pp. 47-69.

Bull, H. (1977) "Part 1: The Nature of Order in World Politics", *The Anarchical Society: A Study of Order in World Politics*. Nova Iorque: Columbia University Press.

Clinton, H. (2011) "America's Pacific Century", *Foreign Policy*, 11 outubro. Disponível em: https://foreignpolicy.com/2011/10/11/americas-pacific-century/ (Acedido em: 18 de agosto de 2025).

Corlin, P. (2025) «In 2025, global trade cracked under tariffs and new China shock», *Euronews*, 29 de dezembro. Disponível em: http://www.euronews.com/my-europe/2025/12/29/in-2025-global-trade-cracked-as-europe-hurt-by-us-tariffs-and-new-china-shock (Acedido em: 9 de janeiro de 2026).

Cunha, L. (2020) "China: a Oportunidade Perdida", *IDN Brief | A Nova (Des)Ordem Mundial: Efeitos da Pandemia*, pp. 2-3.

Cunha, L. (2022) "O DRAGÃO NA SALA", *IDN Brief | A Guerra Na Ucrânia*, pp. 9-10.

Deudney, D. e Ikenberry, G.J. (1999) "The nature and sources of liberal international order", *Review of International Studies*, 25(2), pp. 179-196. Disponível em: https://doi.org/10.1017/S0260210599001795.

Euronews (2026) "Trump diz que pode ter de escolher entre a NATO e a Gronelândia | Euronews", 9 de janeiro. Disponível em: https://pt.euronews.com/2026/01/09/trump-diz-que-pode-ter-de-escolher-entre-a-nato-e-a-gronelandia (Acedido em: 9 de janeiro de 2026).

Fernandes, S. (2021) "Rússia: estratégia de Segurança Nacional", in *Documentos Estratégicos de Segurança e Defesa*. Instituto da Defesa Nacional (IDN Cadernos, 44). Disponível em: https://hdl.handle.net/1822/83811 (Acedido em: 23 de janeiro de 2026).

Fernandes, S. e Cruz, M. (2022) "O dilema de segurança na nova estratégia nacional de segurança russa: entre militarismo e pivot geográfico". Disponível em: https://doi.org/10.26619/1647-7251.13.1.1.

Forest, J.J.F. (2020) "Globalization and Transnational Crime", *E-International Relations*, 16 de setembro. Disponível em: https://www.e-ir.info/2020/09/16/globalization-and-transnational-crime/ (Acedido em: 14 de março de 2024).

Fragile States Index, 2026. *What Does State Fragility Mean? | Fragile States Index*, *What Does State Fragility Mean?* Disponível em: https://fragilestatesindex.org/frequently-asked-questions/what-does-state-fragility-mean/ (Acedido em: 23 de janeiro de 2026).

Freire, M.R. (2013) "Política externa russa: as dimensões material e ideacional nas palavras e nas ações", *e-cadernos CES* [Preprint], (19). Disponível em: https://doi.org/10.4000/eces.1554.

Freire, M.R. (2020) "Vladimir Putin, Twenty Years On: Russia's Foreign Policy", *Vestnik RUDN International Relations*, 20(3), pp. 449-462. Disponível em: https://doi.org/10.22363/2313-0660-2020-20-3-449-462.

Freire, M.R. (2021) "O AUKUS e a Rússia" *IDN Brief | AUKUS e os Interesses de Segurança e Defesa no Pacífico*, pp. 10-11.

Gaspar, C. (2021) "Três Notas Sobre o AUKUS", *IDN Brief | AUKUS e os Interesses de Segurança e Defesa no Pacífico*, pp. 4-5.

Gaspar, C. (2023) "A GUERRA DA UCRÂNIA E A EUROPA", *IDN Brief | Ucrânia Um Ano Depois*, pp. 8-9.

Gomes, J.M. (2020) "A Erosão da globalização: Desafios Geoestratégicos", *IDN Brief | A Nova (Des)Ordem Mundial: Efeitos da Pandemia*, pp. 4-5.

Hasselbach, C. (2026) "Ação dos EUA na Venezuela foi ilegal, afirmam especialistas" *DW,* 07 de janeiro de 2026. Disponível em: https://www.dw.com/pt-br/a%C3%A7%C3%A3o-dos-eua-na-venezuela-foi-ilegal-afirmam-especialistas/a-75421332 (Acedido em: 9 de janeiro de 2026).

Ikenberry, G.J. (2018) "The end of liberal international order?", *International Affairs*, 94(1), pp. 7-23. Disponível em: https://doi.org/10.1093/ia/iix241.

Khan, M. (2026) "US military is «always an option» for Trump to acquire Greenland, White House official says", *ABC News*, 6 de janeiro. Disponível em: https://abcnews.go.com/Politics/us-military-option-acquiring-greenland-white-house-official/story?id=128960041 (Acedido em: 9 de janeiro de 2026).

Kilfoyle, M. (2023) "Ukraine: what's the global economic impact of Russia's invasion?", *Economics Observatory*, 24 de outubro. Disponível em: https://www.economicsobservatory.com/ukraine-whats-the-global-economic-impact-of-russias-invasion (Acedido em 20 de março de 2024).

Kolb, M. (2018) *What Is Globalization?* Disponível em: https://www.piie.com/microsites/globalization/what-is-globalization (Acedido em 5 de março de 2024).

Leandro, F.J. (2025a) "Introduction: Why Is It Important to Discuss the Globalness of China?", in F.J. Leandro (ed.) *Is China a Global Power? The Three Great Walls of the Middle Kingdom*. Singapore: Springer Nature, pp. 1-58. Disponível em: https://doi.org/10.1007/978-981-96-4451-3_1.

Leandro, F.J. (2025b) "Is China a Global Power? Twelve Arguments Suggesting a Global Power in the Making", F.J. Leandro (ed.) *Is China a Global Power? The Three Great Walls of the Middle Kingdom*. Singapore: Springer Nature, pp. 447-470. Disponível em: https://doi.org/10.1007/978-981-96-4451-3_6.

Lo, B. (2008) "The Burden Of History", in *Axis of Convenience: Moscow, Beijing, and the New Geopolitics*. Brookings Institution Press, pp. 17-37. Disponível em: https://www.jstor.org/stable/10.7864/j.ctt6wphdn (Acedido em: 4 de janeiro de 2024).

Louro, M. e Gomes Ferreira, A. (2018) "Trump retira os EUA do acordo com o Irão", 8 de maio. Disponível em: https://www.publico.pt/2018/05/08/mundo/noticia/trump-ja-tera-avisado--macron-que-vai-sair-do-acordo-com-o-irao-1829279 (Acedido em 20 de janeiro de 2026).

Marcos, D. e Alcario, I. (2023) "A invasão do Iraque, vinte anos depois A ordem internacional em crescente tensão", *Relações Internacionais*, 78, pp. 33-45.

Meiser, J.W. (2018) "Introducing Liberalism in International Relations Theory", *E-International Relations*, 18 de fevereiro. Disponível em: https://www.e-ir.info/2018/02/18/introducing--liberalism-in-international-relations-theory/ (Acedido em: 5 de dezembro de 2023).

Melnitsky, R. (2023) *Islamophobia Surges in the U.S. Due to Global and National Tensions*, *New York State Bar Association*. Disponível em: https://nysba.org/islamophobia-surges-in-the-u-s-due-to-global-and-national-tensions/ (Acedido em: 18 de março de 2024).

Moita, L. (2020) "O Impacto Internacional da Pandemia", *IDN Brief | A Nova (Des)Ordem Mundial: Efeitos da Pandemia*, pp. 7-8.

Moravcsik, A. (1992) *Liberalism and International Relations Theory*. Center for International Affairs, Harvard University. Disponível em: https://www.princeton.edu/~amoravcs/library/liberalism_working.pdf.

Moravcsik, A., 1997. "Taking Preferences Seriously: A Liberal Theory of International Politics", *International Organization*, 51(4), pp. 513-553.

Nye, J.S. (2004) "The Changing Nature of Power», em *Soft Power: The Means To Success In World Politics"* 1.ª ed. Nova Iorque: PublicAffairs, pp. 1-32.

O'Loughlin, J., Ó Tuathail, G. e Kolossov, V., 2004. "A «Risky Westward Turn»? Putin's 9-11 Script and Ordinary Russians", *Europe-Asia Studies*, 56(1), pp. 3-34.

Pinéu, D. (2020) "COVID-19 e Volatilidade Internacional", *IDN Brief | A Nova (Des)Ordem Mundial: Efeitos da Pandemia*, pp. 7-8.

Pizarro, N. (2022) "Bússola Estratégica e a Política de Defesa Europeia", *IDN Brief | Bússola Estratégica: Perspetivas*, pp. 2-3.

Público (2017) "Trump retira EUA do Acordo de Paris", *Público*, 1 de junho. Disponível em: https://www.publico.pt/2017/06/01/mundo/noticia/trump-retira-eua-do-acordo-de-paris-1774288 (Acedido em: 20 de janeiro de 2026).

Rato, V. (2024) "Trump e a Revolução Externa", *IDN Brief | O efeitoTrump 2.0*, pp. 3-4.

Reis, B.C. (2021) "AUKUS: Vários Equívocos, Alguma Relevância", *IDN Brief | AUKUS e os Interesses de Segurança e Defesa no Pacífico*, pp. 3-4.

Ribeiro Gomes, T. (2024) "A infraestrutura da globalização no regresso da desordem mundial", *Relações Internacionais*, (84), pp. 87-106.

Ricarte, J. (2024) "Regresso da guerra no Médio Oriente? Conflito prolongado, (des)ordem global e insegurança ontológica na era da polarização", *Relações Internacionais*, 84, pp. 107-129.

Rodrigues, D. e Neves, N.C. (2021) "AUKUS – Estabilidade ou uma Nova First Fleet?", *IDN Brief | AUKUS e os Interesses de Segurança e Defesa no Pacífico*, pp. 6-7.

Rutland, P. (2015) "An Unnecessary War: The Geopolitical Roots of the Ukraine Crisis", *E-International Relations*, 9 de abril. Disponível em: https://digitalcollections.wesleyan.edu/islandora/unnecessary-war-geopolitical-roots-ukraine-crisis (Acedido em: 19 de agosto de 2025).

Santos Pinto, A. e Raimundo, F. (2016) "Nota introdutória", *Relações Internacionais*, 50, pp. 05-09. Disponível em: RI50_01NotaIntrodutoria.pdf (Acedido em: 19 de agosto de 2025).

Simão, L. (2019) "As crises da ordem liberal", *Relações Internacionais*, 63, pp. 39-51. Disponível em: https://doi.org/10.23906/ri2019.63a04.

Soller, D. (2022) "A Fraqueza Relativa Norte-Americana e a Guerra na Ucrânia", *IDN Brief | A Guerra Na Ucrânia*, pp. 5-6.

The White House (2025) "National Security Strategy of the United States of America". Disponível em: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

Trezzini, M., 2020. "Trump retira Estados Unidos da Organização Mundial de Saúde", *Observador*, 7 julho. Disponível em: https://observador.pt/2020/07/07/trump-retira-estados-unidos-da-organizacao-mundial-de-saude/ (Acedido em: 20 de janeiro de 2026).

Tomé, L. (2021) "AUKUS: criando o "Atlântico-Pacífico" e dividindo o Atlântico e o Pacífico", *IDN Brief | AUKUS e os Interesses de Segurança e Defesa no Pacífico*, pp. 9-10.

Tomé, L. (2023) "A Guerra na Ucrânia dividiu o mundo, mas não exatamente entre democracias e autocracias", *IDN Brief | Ucrânia Um Ano Depois*, pp. 9-10.

Tomé, L. (2024a) "A retórica da China de Xi propondo uma ordem mundial alternativa", *Relações Internacionais*, 84, pp. 71-86.

Tomé, L. (2024b) "Trump 2, China e Ásia/Indo-Pacífico: Continuidades e Descontinuidades", *IDN Brief|O efeitoTrump 2.0*, pp. 5-7.

Trenin, D. (2006) "Russia Leaves the West", *Foreign Affairs*, 85(4), pp. 87-96.

Wright, T. (2014) "The Rise and Fall of the Unipolar Concert", *The Washington Quarterly*, 37(4), pp. 7-24. Disponível em: https://doi.org/10.1080/0163660X.2014.1002150.

Capítulo III

SEGURANÇA INTERNACIONAL E DIREITO INTERNACIONAL (1)

Multiculturalismo em França: paz estrutural ou evasão social?

Cristóvão Simão Oliveira de Ribeiro
João Pedro Ferreira Geraldes
Tiago Manuel Barbosa Ramalho
Finalistas da licenciatura de Relações Internacionais na Universidade Portucalense.

Resumo

Johan Galtung, através do seu pensamento consolidado nas áreas da paz e segurança, forneceu contributos teóricos fundamentais para a sua consolidação enquanto ciência. A sua categorização dos diferentes tipos de paz e a sua construção metódica em torno da ideia de violência são, ainda hoje, fundamentais para qualquer estudo neste campo científico. Apesar de o Estado francês reconhecer apenas "cidadãos", não fazendo, portanto, qualquer distinção jurídica entre eles, este ensaio argumenta que existem, na sociedade francesa, intensas e permanentes tensões sociais com motivação étnico-religiosa, cuja origem merece a atenção desta reflexão. Este artigo pretende estudá-las, criando uma abordagem sistemática de correlação entre tais postulados galtunianos e os conceitos de Etnia, Nação, Estado-Nação, identidade nacional e a construção de um discurso populista de securitização em França como resultado de tal fricção.

Palavras-chave: Paz e Segurança; Galtung; Estado-Nação; França.

Abstract

Johan Galtung, through his consolidated thinking in the areas of peace and security, made fundamental theoretical contributions to the consolidation of the science. His categorisation of the different types of peace and his methodical construction around the idea of violence are still fundamental to any study in this scientific field today. Even though the French state only recognizes "citizens" and therefore makes no distinction between them, this essay argues that there are, in French society, intense and permanent social tensions with an ethnic-religious motivation, the origins of which deserve the attention of this reflection. This article aims to study them, creating a systematic approach to correlating these galtunian postulates with the concepts of ethnicity, nation, Nation-State, national identity, and the construction of a populist discourse of securitization in France as a result of this friction.

Keywords: Peace and Security; Galtung; Nation-State; France.

Introdução

Tal como a história da integração europeia nos demonstrou, a França foi indubitavelmente um *player* central e decisivo na evolução da arquitetura institucional da União Europeia. Exemplos disso foram o papel que esta e os seus atores políticos desempenharam na criação da CECA (Glockner e Rittberger, 2012) enquanto primeira entidade Europeia supranacional, bem como no falhanço da CED (Griffiths, 2012) cuja iniciativa de criação, bem como o seu destrutivo veto, paradoxalmente, foi francês (motivado por uma alteração interna do equilíbrio de forças politicas na Assembleia Nacional) e cuja consequência ainda hoje ecoa na forma como a União Europeia se rege institucional e organicamente no seu equilíbrio entre intergovernamentalismo e supranacionalismo e, entre métodos comunitários e intergovernamentais de votação e decisão. Daí a escolha do nosso *case study*. Pretendemos com este estudo relacionar o atual contexto social e étnico deste país, figura central na história europeia, tentando entender como é que tal contexto político interno francês está ou não a mudar em consequência da evolução do seu tecido étnico e social. Tentaremos, pois, verificar se existe uma relação direta entre a matriz multicultural francesa e o seu panorama político, correlacionando tudo isto com a noção científica de Paz. Para tal, usaremos os contributos científicos de Johan Galtung e as suas classificações que, adiante, explicitaremos.

Como resultado de um espaço intelectual para a estruturação académica de pensamento e como uma declaração de compromisso à não violência e à realização da paz por meios pacíficos, a primeira reflexão cientificamente consistente e transversal nestas matérias, o *Journal of Conflict Resolution* data de 1957. Dois anos depois, em 1959, dá-se a criação do *Center of Conflict Resolution* na Universidade de Michigan. Contudo, seria apenas com Johan Galtung, entendido pela literatura como "o pai" dos estudos para a paz, que, no âmbito do Peace Research Institute Oslo (PRIO), foi criado em 1959 o *Journal of Peace Research,* publicado pela primeira vez em 1964, veiculando uma visão disruptiva e assertiva relativamente ao conceito de paz enquanto ciência. Partindo da análise da sua publicação de 1969 (Galtung, 1969), afirmamos que o autor, de forma pragmática, partiu de três premissas essenciais: a primeira, refletir sobre a ideia de paz enquanto utopia ingénua; a segunda, a paz enquanto tradição de pensamento não científico (que este pretendia mudar) e a terceira, a paz enquanto pacificação dos conflitos de larga-escala (Cravo, 2023).

A conclusão do trabalho de Galtung (1969), para além de definir, com exatidão, o âmbito dos estudos para a paz e segurança, forneceu-nos quatro definições fundamentais para a compreensão científica destas matérias. As definições de paz positiva, paz negativa, violência cultural e violência estrutural (Lawler, 2013) são fulcrais para o entendimento do objeto de análise do nosso estudo.

O foco da nossa análise diz respeito à correlação de tal postulado galtuniano com os conceitos de etnia, Estado-nação, identidade nacional e a sua relação com um discurso populista de securitização (com os critérios de análise da Escola de Copenhaga) em França (McDonald, 2023), tentando compreender a relação destes fenómenos com a evolução eleitoral da FN/RN.

Para concretizar tal investigação recorre-se complementarmente aos métodos qualitativo (revisão de literatura, analise discursiva e análise Jurídico-política) e quantitativo (análise de inquérito estatístico e resultados eleitorais).

Formulamos a seguinte questão de partida:

Partindo do *framework* teórico oferecido por Galtung, de que forma a *Rassemblement National* contribui, através da mobilização dos argumentos de rejeição étnico-religiosa, para um crescente discurso de securitização em França?

Deste modo, focaremos a nossa investigação no período temporal compreendido entre 2012 e 2024 (espaço temporal que compreende três eleições presidenciais e quatro eleições legislativas em França, com vista a análise da evolução da representação da Front National / Rassemblement National).

Acerca da liberdade religiosa, uma análise Jurídico-Política

A União Europeia é uma união fundada na legalidade e na primazia do Direito, com base em mecanismos interinstitucionais (integrados) e alicerçada nos seguintes princípios: Princípio do Primado; do Efeito Direto; da Interpretação Conforme; da Subsidiariedade; e da Atribuição (Pais, 2020). Alicerça-se também num complexo sistema de normas inerentes à arquitetura prática integracionista da União Monetária e de uma economia social de mercado que esta postula.

Portanto, "tendo por objeto, promover a paz, os seus valores e o bem-estar dos seus povos (…)", a União Europeia "proporciona aos seus cidadãos um espaço de liberdade, segurança e justiça (..) "combate a exclusão social e as discriminações e promove a justiça e a proteção social e a igualdade (…)", tal como enunciado nos artigos 2.º, 3.º e 6.º do TUE.

Mas serão estes bens juridicamente absolutos? Sem exceções? De modo inultrapassável pelos Estados-membros?

Princípio do primado

Princípio de origem jurisprudencial, cuja raiz não encontra precedência direta nos textos dos tratados, nomeadamente no Tratado da União Europeia, tendo sido, portanto, fixado pela ação e atuação do Tribunal de Justiça da União Europeia (TJUE) na fixação do Direito (Martins, 2017).

"*O princípio da primazia do direito da união determina que, em caso de conflito, o direito da UE aplica-se com preferência sobre o direito nacional dos Estados Membro. No Acórdão Costa/Enel (Ac. De 15 de julho de 1964, proc. 6/64), o TJUE afirmou e fundamentou, pela primeira vez, de forma inequívoca, e em termos constitucionais, a superioridade das normas do direito da união sobre as normas nacionais*." (Martins, 2017, pp. 339-340).

Na demanda da nossa investigação, cumpre-nos, pois, encetar uma breve reflexão acerca do alcance deste princípio jurisdicional. Segundo a remissão efetuada pelo artigo

6.º DO TUE, a liberdade de pensamento, de consciência e de religião vêm consagradas no topo da hierarquia das normas do Direito Europeu. Logo no n.º 1 do Artigo 10.º da CDFUE, tal liberdade fundamental é enunciada: "Todas as pessoas têm direito à liberdade de pensamento, de consciência e de religião (…). Liberdade de manifestar a sua religião ou a sua convicção, individual ou coletivamente, em público ou em privado, através do culto, do ensino, de práticas e da celebração de ritos." (Pais, 2020).

Se é verdade que o Princípio do primado, aparentemente se afigura como absoluto, não é menos verdade que este, não só admite exceções, como na realidade estas podem estar na base do nosso objeto de estudo. Olhemos então, com atenção, para o conteúdo n.º 2 do artigo 4.º do TUE, "A União respeita as funções essenciais do Estado, nomeadamente as que se destinam a garantir a integridade territorial, a manter a ordem pública e a salvaguardar a segurança nacional. Em especial, a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-membro."

Por tudo isto, afirmamos que, se o DUE se afigura como um dos principais baluartes na defesa da liberdade étnico-religiosa, e por isso da coexistência pacífica da pluralidade de identidades, também não é menos verdade que ele próprio cria a sua exceção e aponta o caminho para a sua restrição.

Numa interpretação mais extensiva, cruzando o DUE com conceitos da Ciência Política e das Relações Internacionais, afirmamos que na base normativa da construção do conceito de identidade que nos leva, entre muitos outros fatores, ao conceito de nação, está a proteção e salvaguarda jurídica conferida pelo Artigo 10.º da CDFUE, conjugado com os Artigos 2.º,3.º e 6.º do TUE e, por outro lado, o seu contraponto está no n.º 2 do artigo 4.º do TUE, numa clara aceção da natureza intergovernamental (Moravcsik, 1998) inerente a génese do projeto europeu.

Deste modo, olhamos para a proibição do uso do véu islâmico em espaços públicos franceses, enviesado pela proteção das liberdades individuais e a pretexto da segurança e ordem pública como um exemplo prático daquilo que acabamos de expor, como previsto na Lei n.º 2004-228 da República Francesa, citada em Guérios e Kamel (2014), gerando protestos e fortes tensões sociais nas ruas de várias cidades francesas (Euronews, 2019).

Acrescentando ainda uma nova camada de complexidade a tal problemática, entendemos mesmo que tal espaço jurídico consubstancia o clima perfeito para o discurso e para o processo de securitização que a Escola de Copenhaga nos ensina (McDonald, 2023).

No que concerne ao Direito da União Europeia, parece-nos consistente dizer que a primazia do vetor mais intergovernamental do que supranacional, intrínseca à ontologia da União Europeia e vertida no seu enquadramento normativo e institucional, não só não contribui para uma salvaguarda da liberdade étnico-religiosa em termos (jurídicos) absolutos, como abre ela própria a "caixa de Pandora" para a própria salvaguarda de uma não violência cultural galtuniana, ficando ainda demonstrado que, apesar de todos os mecanismos funcionais e intergovernamentais altamente transparentes que a UE tem ao seu dispor (por exemplo, o Mecanismo Europeu para o Estado de Direito) para a salvaguarda do Estado de Direito e para a garantia estratégica da segurança e paz em sentido

positivo (Estratégia para a União da Segurança), que contribui para as sociedades pacíficas e inclusivas (European Commission, 2020), estão feridos pela sua própria complexidade, que se traduz em pouca eficácia na salvaguarda preventiva de tais fenómenos.

Acerca das tensões étnico-religiosas em França

Um dos principais desafios ao Estado moderno pós-vestefaliano, em concreto ao Estado-nação, que – apesar de uma certa erosão da sua soberania (Kaldor, 2012) continua a ser a base do sistema anárquico das Relações Internacionais no atual contexto de multipolaridade (Deutsche e Singer, 1964) – é a construção e coesão da sua identidade nacional. Conjugar processos e desafios históricos, que contribuem para a criação de uma memória coletiva com os fenómenos da multiculturalidade societária resultante do processo de globalização e das vagas migratórias, assume-se como algo complexo e que, não raras vezes, é a base do surgimento de tensões (Zhang, 2023).

Neste tópico, debruçamo-nos sobre a forma como a República Francesa que, segundo Zhang (2023), é um Estado secular e laico, tem lidado com a multiplicidade étnica e religiosa, em particular com o islamismo, no contexto da sua constante tentativa de afirmação enquanto Estado-nação. Veja-se, a título de exemplo entre muitos outros discursos políticos franceses, o discurso proferido por Emmanuel Macron aquando da reabertura de Notre-Dame em Paris: "Esta Catedral é uma feliz metáfora do que é uma nação" (Macron, 2024).

É indubitável que a história contemporânea francesa tem sido marcada por uma constante tensão étnico-religiosa, ora associada a vagas migratórias muçulmanas (Meier e Hawes, 2009), ora a algo socialmente mais estrutural, isto é, as segundas e terceiras gerações, já nascidas em território francês, descendentes de tais imigrantes (Beaman, 2016) que, sendo cidadãos franceses, não encontram correspondência étnico-valorativa na representação do seu Estado. Apesar da cidadania francesa destas pessoas, a sua herança cultural mantém-se rigidamente enraizada, conflituando com a cultura francesa. Por outras palavras, o Estado francês não foi capaz de operar uma assimilação ou conformação cultural e religiosa destes povos, compatível com a sua aspiração à categoria de Estado-nação. Ora, embora exista na literatura quem advogue o contrário, em nossa perspetiva, é justamente neste "erro estratégico" (Zhang, 2023) que residem as bases de tais tensões. França, ao tentar forçar uma uniformidade cultural artificial – a proibição do véu islâmico em escolas e a utilização recorrente do conceito de Estado-nação nos discursos políticos são um bom exemplo disso, entre muitos outros – quase que "institucionaliza" a prática constante de um dos mais importantes postulados teóricos de Galtung, a violência cultural. Tal relação encoraja, aliás, numa quase estrutura de inspiração *top-down* (do Estado que contagia a sociedade) de islamofobia estrutural que facilmente pode ser construída (Wendt, 1999) como um confronto antagónico de duas visões radicalmente etnocêntricas. Tal configura, portanto, a base da posição que aqui assumimos, mesmo sabendo que esta não é consensual entre a literatura.

Uma das manifestações deste fenómeno encontra correspondência, por exemplo, até na forma como alguns meios de comunicação social abordam tal multiculturalidade. É certo que este tem na sua base uma matriz humorística, mas, ainda assim, a forma como o *Charlie Hebdo*, entre outros periódicos, transpõe esta tensão societária para o campo do escárnio e da sátira advém, em nossa opinião, de uma certa ideia de subalternização ou inferioridade cultural e civilizacional que se tem perpetuado entre a consciência coletiva dos franceses não descendentes de imigrantes muçulmanos. Acrescentamos ainda o facto de não se poder aqui ignorar também historicamente alguma iconoclastia herdada do anticlericalismo da Revolução Francesa em relação à religião. Já no século XVIII, autores como Voltaire ou Rousseau escarneciam ferozmente da religião.

A complicada relação histórica entre a França e o mundo islâmico remonta a um longo passado colonial, com o qual a França não aprendeu a lidar (Zhang, 2023). A própria tentativa de contrariar tal realidade por via legal, proibindo a distinção de cidadãos franceses com base na sua fé (Beaman, 2016) é a demonstração cabal de tal intenção, como exploramos no capítulo anterior. Tal como pertinentemente afirma Valentine Zuber (2010, pp. 161), "Os valores apregoados pelo modelo da República tradicional francesa são cada vez mais contestados por uma parte crescente da população. Os principais pilares da ética laica – o Progresso, a Nação, a Razão – perdem a sua pertinência. Novos combates surgem para mobilizar o conceito de laicidade de uma maneira inédita (como o combate pela santuarização da escola ou para a defesa dos direitos das mulheres)". Tal relação tumultuosa só poderia ter um resultado quando confrontada com outro polo etnocêntrico: a exacerbação de fanatismos identitários, ideológicos e religiosos que transpõem a sociedade para uma realidade de repetidos episódios de violência direta (Euronews, 2015), resultante da incapacidade de moderação da manifestação social, artística e comportamental de tais diferenças, que mais não são senão o resultado óbvio da violência estrutural e cultural da qual a sociedade francesa é protagonista.

Tendo por base ainda a análise ao inquérito do Observatoire du Zemmourisme [1](citado em Zhang, 2023), realizado em 2021, os resultados são amplamente demonstrativos desta realidade que acabamos de descrever: 68% dos cidadãos franceses acreditam que o islão representa uma ameaça para a identidade francesa[2], o que perpetua a ideia de

1 O Observatoire du Zemmourisme é um instrumento de estudos discursivos políticos, realizados pelo instituto francês de opinião publica em conjunto com a fundação Jean – Joaurès, com a finalidade de identificar a sua correspondência com as ideias de Eric Zemmour, um político francês de extrema-direita, isto é, com a finalidade de avaliar o grau de extremismo das narrativas políticas e a sua influência na sociedade francesa.

2 Esta "identidade francesa" é levantada pelos partidos de extrema-direita (tal como em quase todos os países ocidentais, em que se alimenta um discurso hostil contra os imigrantes através da defesa de uma "identidade nacional" em perigo). O que é paradoxal em França é a transmutação da "identidade republicana" (laica) em "identidade nacional", sendo que, à partida, a tal identidade republicana não era propriamente neutra ou desprovida de traços culturais. Voltando a dois conceitos que nos ajudam a problematizar as questões de identidade, a distinção entre nacionalismo étnico e nacionalismo cívico, estabelece-se pelo carácter voluntário ou involuntário da pertença a um coletivo. A nação francesa em termos "republicanos/cívicos" seria uma escolha voluntária de cada indivíduo que se revê num determinado projeto político. A nação "identitária/étnica" é quase uma fatalidade, um "nós" e "eles" inescapável.

um "nós coletivo" diferente "do outro coletivo". Um "nós coletivo" com direito originário a este território, que se sente invadido e expropriado pelo "outro coletivo" numa realidade por "nós" percecionada como um ato de quase "vingança colonial", o qual se traduz numa perceção de "roubo do nosso emprego", "roubo da nossa habitação, "roubo das nossas oportunidades", "roubo do nosso território" e até por fim, "roubo da nossa identidade nacional". Esta é a perceção da mainstream society (Beaman, 2016).

Em contraste, os franceses muçulmanos na sua maioria são altamente influenciados por valores como a liberdade, igualdade e fraternidade, transversais ao arquétipo idílico de identidade nacional francesa (Zhang, 2023). A grande questão geradora de um ciclo vicioso de tensão é a ideia da sua não aceitação por tal sociedade *mainstream*, isto é, tal sociedade arroga-se o direito e a propriedade exclusiva da defesa de tais valores, levando a uma forma estrutural de exclusão e de perpetuação de um sentimento de não pertença ao "nós coletivo" (Zhang, 2023). "O estatuto incompleto dos Muçulmanos como membros da nação francesa contribui para um sentimento de alienação, no qual os impede de reconhecer a identidade nacional francesa." (Zhang, 2023, pp.10). Deste modo, somando à disseminação *top-down*, macroestrutural e forçada do conceito de nação propagado pelo Estado francês, está a ideia de que este processo é simultaneamente acompanhado pelo *engagement* rotineiro dos cidadãos anónimos comuns num exercício prático de tal discriminação (Fox e Miller-Idriss, 2008).

A tensão identitária (também) espelhada no contraste entre autores ocidentais muçulmanos e não muçulmanos

Objeto de um vasto estudo no âmbito das Relações Internacionais e da Ciência Política, a obra de Samuel Huntington providencia uma útil teorização para a compreensão desta temática. Atentemos na forma como autores ocidentais muçulmanos analisam esta obra.

Samuel Huntington, na obra intitulada *Clash of Civilizations* (Huntington, 1993), argumentou que há no mundo várias civilizações e que a maior fonte de conflito humano seria resultante do facto de a civilização ocidental, definida como sendo a Europa e os EUA, tentar impor os seus padrões societários e políticos a outras civilizações, provocando, inevitavelmente, um "choque" identitário. Este seria a base de todos os conflitos. Huntington versou sobre um confronto de padrões societários por contraste antagónico de normas e valores baseados nas distintas perceções da história, da economia, dos direitos humanos, da religião e da cultura.

Zahra Seif-Amirhosseini Rafie, muçulmana, professora de sociologia na universidade da Virgínia do Norte, interpreta que Huntington, na sua obra, descreveu as culturas não ocidentais como bárbaros, selvagens e não civilizados. Esta sustenta a ideia de que Huntington defende implicitamente que a única forma de estas sociedades não civilizadas passarem a ser encaradas como civilizadas e modernas seria pela assimilação das orientações civilizacionais e culturais ocidentais (Seif-*Amirhosseini*, 2013), quando Huntington descreve que tal realidade confrontacional seria inevitável (Huntington,

1993). Hussain Alhussainy, professor assistente de ciência política na universidade de Alberta, Canada, argumenta que Huntington defende ainda que as democracias ocidentais têm direito a disseminar tais valores e que todas as culturas teriam a ganhar com isso, num Sistema Internacional dominado pelo Ocidente (Alhussainy, 2023).

Escusamo-nos, obviamente, de relembrar as consequências deste choque de pensamentos; porém, julgamos importante utilizá-lo para o nosso objeto de análise. Se Huntington prevê a existência de um choque de civilizações à escala mundial e versa até sobre a relação conflituosa dos muçulmanos com os demais cidadãos em França (Huntington, 1993), o que este não previu é que o próprio conceito de *Clash of Civilizations* se adequaria até à forma como a sua própria obra seria interpretada pelos muçulmanos ocidentais. Tal questão é mais uma demonstração do quão sensível e conflituoso é o tema da identidade com fundamentos étnico-religiosos.

A interpretação que estes investigadores muçulmanos fazem da obra de Huntington assenta perfeitamente no entendimento que os franceses muçulmanos fazem da abordagem discriminatória (cultural) *top-down* que acima expusemos em relação ao Estado Francês e oferece-nos, ainda que indiretamente, uma boa sustentação teórica para a matriz ideacional e de pensamento da própria sociedade civil dos franceses não-muçulmanos. Assim, sem defendermos, claro está, tal interpretação do pensamento de Huntington, nela encontramos um padrão que, para além de ajudar a explicar a forma de agir da sociedade francesa perante a multiculturalidade, mais não gera senão violência cultural e estrutural em França.

A relação entre o discurso de securitização em França e a Rassemblement National

Analisando o artigo *Myth and Mobilization: The Triadic Structure of Nationalist Rethoric* de Levinger e Lytle (2001), entendemos que existem duas correntes teóricas dominantes na tentativa de explicação da retórica nacionalista. A instrumentalista e a construtivista.

Deste modo, por um lado, dizemos que a grelha de análise instrumentalista olha para a retórica nacionalista como um meio de encontrar suporte e adesão popular à persecução de determinados interesses (escondidos) específicos das elites, sob o manto e o pretexto da ideia de "nação". Por outro lado, a grelha de compreensão construtivista firma a sua análise na construção da própria ideia de "nação" assente na correlação multifatorial de elementos tais como raça, linguagem, cultura e geografia. Esta escola de pensamento explica ainda a "poderosa atração" da ideologia nacionalista como resposta à erosão do tradicionalismo cultural da sociedade (Levinger e Lytle, 2001).

Focamos a nossa abordagem na formação e construção dos elementos discursivos (teoria construtivista) e também na forma como esta construção é usada como meio de mobilização política e social (teoria instrumentalista), em que o "auto-entendimento" nacionalista da ideia de "nação" serve de base para a arquitetura da identidade política e social, através da mobilização popular. Desta feita, tal construção (teoria construtivista) é

realizada através da combinação de três fatores discursivos e ideacionais, que, ao mesmo tempo, são a "ferramenta" de mobilização popular (segundo a teoria instrumentalista): **1) Um "passado glorioso"**, onde a nação existia como pura, unida e harmoniosa. **2) Um "presente degradado"**, em que o desmantelamento desta unidade nacional é o fator-chave e os bodes expiatórios são os diferentes, os "não puros", que destroem a conceção harmoniosa da "nação". **3) "Um futuro utópico"**, em que, através da ação coletiva, a nação terá condições de se revitalizar, corrigindo os fatores que prejudicaram a harmonia original, combatendo a degradação e recuperando o esplendor glorioso (Levinger e Lytle, 2001).

Assim, no caso da construção de narrativas nacionalistas em França, com vista à mobilização popular em torno desta tríade, convém-nos observar o "tentador discurso fácil" da Rassemblement National através de frases como "A França e a Europa estão a ser inundadas por imigrantes" (Le Pen, J.M., 2010, citado em Rocha, J., 2015); "A imigração descontrolada e em larga escala (..) prejudica gravemente a identidade (…) das nações que a compõem" (Le Pen, M., 2010, citado em Rocha, J., 2015).

Na nossa interpretação de tais discursos, os dirigentes da FN/RN pretendem explicar a não assimilação cultural por parte dos franceses "não puros", os muçulmanos, expressa em "práticas das comunidades que se recusam a respeitar as nossas leis e nossos costumes e que ainda pretendem impor-nos as suas próprias leis e costumes", tal como disse Bruno Gollnisch (Gollnisch, B., 2010, citado em Rocha, J., 2015). Assim, segundo a nossa interpretação das palavras de tais atores políticos, a "culpa da degradação da nação" (conforme a classificação da tese instrumentalista) assenta nas práticas culturais dos imigrantes muçulmanos, crentes numa religião que, segundo a RN/FN, impõe os seus hábitos e violenta as mulheres (Gollnisch, B., 2010, citado em Rocha, J., 2015) "ao estabelecer a burca, os casamentos forçados, a poligamia, a excisão, os crimes de honra e outros comportamentos de outras eras que não são suportáveis" (Le Pen, M., 2009, citado em Rocha, J., 2015).

Tal degradação da "nação" só pode ser combatida, segundo estes, recuperando "o passado glorioso" e construindo o "futuro utópico", pela expulsão dos franceses "não puros". Assim, entendemos que estes se autoassumem quase como um antibiótico para a cura de "tal doença", quando, por exemplo, defendem o fim do espaço Schengen, como meio de garantir não só tal originalidade e pureza da raça e nação, mas também a sua própria segurança (Gollnisch, B., 2009, citado em Rocha, J., 2015). Schengen e a consequente abertura das fronteiras internas são encarados como o caminho que leva a "extraordinárias oportunidades oferecidas aos terroristas de todos os credos" (Gollnisch, B., 2009, citado em Rocha, J., 2015). Outra ideia é a do crime organizado e transnacional como um resultado negativo da globalização que urge combater (Rocha, 2015).

Tal narrativa da Rassemblement National, no nosso entendimento, não é mais do que a tentativa de afirmação de uma manobra de securitização, através de um discurso securitário como resposta a ameaça existencial de que a "nação" tem sido alvo, preenchendo, portanto, todos os requisitos teóricos da escola de Copenhaga (McDonald, 2023). A situação de tensão multicultural vivida em França está, portanto, no domínio da

política ou situação do "anormal ou invulgar" no que à perceção construtivista diz respeito, não pela suspensão total da política "normal" mas pela introdução de medidas restritivas (anormais) de liberdades individuais (que o próprio DUE consente), como a liberdade de culto religioso a pretexto da segurança nacional, que no caso do não uso do véu muçulmano se traduz, na prática, como uma quase proibição da religião (não há forma possível de usar o véu islâmico de forma oculta, ao contrário da cruz cristã, por exemplo. Para um muçulmano, proibir a manifestação de objetos religiosos significa proibir a sua religião e a sua própria identidade.

Observemos agora a relação entre esta narrativa e o comportamento eleitoral da RN/FN entre 2012 e 2024. Como demonstram os arquivos dos resultados eleitorais do sítio oficial do Ministère de L'Intérieur francês a FN/RN evoluiu da seguinte forma:

Eleições Legislativas:

A FN/RN, numa evolução contínua crescente, passou de uma votação de 13,60% dos votos em 2012, para 32,05% dos votos na segunda ronda das eleições legislativas de 2024 (Ministère de L'Intérieur, 2024).

Eleições Presidenciais:

Verificando-se novamente a mesma evolução contínua crescente, a candidata apoiada pela FN/RN, Marine Le Pen passou de 17,90 % dos votos em 2012, não conseguindo passar a segunda ronda das eleições, para 41,45 % dos votos em 2022 (Ministère de L'Intérieur, 2024).

Tal como o supracitado nos demonstra, existe uma espécie de relação de mutualismo *win-win* entre resultados eleitorais e discurso securitário, assim como entre discurso securitário e resultados eleitorais.

Deste modo, se é verdade que tal comportamento discursivo de securitização configura uma exploração das tensões étnico-religiosas por parte da RN/FN – o que tem levado ao aumento da sua representatividade política, isto é, na prática, ao sucesso do processo de mobilização popular em torno dos seus objetivos - também é verdade, por outro lado, que tal aumento de representatividade política, por via do uso de tal discurso, tem levado à repetição e "endurecimento" desse mesmo discurso securitário.

Conclusão

Como argumentamos e sustentamos com esta investigação, existem na sociedade francesa intensas e permanentes tensões com motivação étnico-religiosa, cuja origem remonta não só a um passado colonial com o qual França não aprendeu a lidar, mas também à perpetuação de uma ideia de nação impossível de replicar e de fazer corresponder na organização estadual vigente. A República Francesa não só não é um Estado-nação – na medida em que os franceses muçulmanos não conseguem "encaixar"

na imagem idealizada de nação por parte do Estado – como a sua tentativa forçada de o ser é o sustento ideacional e social da violência estrutural, cultural e direta que se observa e aqui se demonstra. A perceção societária de um "glorioso nós coletivo" molda e dita as regras com as quais a abordagem *top-down* do Estado francês mina e inspira negativamente a sociedade civil, contribuindo, ainda que sem o desejar, para o crescente oportunismo de manipulação do discurso securitário por parte da FN/RN, alicerçado em tais diferenças étnico-religiosas – A nação «identitária/étnica".

Na linha do que propusemos investigar e responder, concluímos que tal complexidade identitária, combinada com o desacerto do vetor institucional do Estado, associado a um discurso e movimento de securitização segregador – assente na devolução da pureza e unidade da nação cívica francesa – é aproveitado de forma populista por algumas elites (FN/RN) e conduz a uma sociedade fraturada e fragmentada. Esta observação leva-nos a concluir que França, uma república laica e secular, padece hoje de um permanente estado de paz negativa resultante da violência estrutural e cultural que se tem perpetuado na sociedade.

Referências

Alhussainy, H. (2023) "Clash Of Civilizations, Orientalism, and the «Civilized" and "Uncivilized»", *Special Edition: Stories of Hope*, 3(2), pp.15-23. https://doi.org/10.29173/crossings128

Assemblée Nationale (2010) *Projet de Loi interdisant la dissimulation du visage dans l'espace public*. Disponível em: https://www.assemblee-nationale.fr/13/ta/ta0524.asp (Acedido em 2 de março de 2026).

Beaman, J. (2016) "As French as Anyone Else: Islam and the North African Second Generation in France", *International Migration Review*, 50(1), pp. 41-69. https://doi.org/10.1111/imre.12184

Brandão, A. P., Coutinho, F. P., Camisão, I. e Abreu, J.C (2017) *Enciclopédia da União Europeia*, Lisboa: Petrony Editora.

Cravo, T. A. (2023) "Johan Galtung e os estudos para a paz", *OBSERVARE*, Universidade Autónoma de Lisboa, pp. 455-465. Disponível em: http://hdl.handle.net/11144/6447

Deutsch, K. W. e Singer, J. D. (1964) "Multipolar Power Systems and International Stability". *World Politics*, 16(3), 390-406. https://doi.org/10.2307/2009578

Euronews (2020a) "Charlie Hebdo". Disponível em: https://pt.euronews.com/tag/charlie-hebdo (Acedido em 2 de março de 2026).

Euronews (2020b) "Identificados suspeitos de ataque com arma branca em Paris". Disponível em: https://pt.euronews.com/2020/09/25/identificados-suspeitos-de-ataque-com-arma-branca-em-paris (Acedido em 2 de março de 2026).

Euronews (2020c) "Manifestação contra Charlie Hebdo em Istambul". Disponível em: https://pt.euronews.com/2020/09/13/manifestacao-contra-charlie-hebdo-em-istambul (Acedido em 2 de março de 2026).

Euronews (2019d) "Milhares contra a Islamofobia em França". Disponível em: https://pt.euronews.com/2019/11/10/milhares-contra-a-islamofobia-em-franca (Acedido em 2 de março de 2026).

Euronews (2020e) "Professor decapitado para «vingar Alá»". Disponível em: https://pt.euronews.com/2020/10/17/professor-decapitado-para-vingar-ala (Acedido em 2 de março de 2026).

European Commission (2023) *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52023DC0306

EUR-Lex – 52023SC0822 – EN – EUR-Lex (Acedido em 2 de março de 2026).

Fox, J. E. e Miller-Idriss, C. (2008) "Everyday nationhood". *Ethnicities*, *8*(4), pp. 536-563.

Galtung, J. (1969) "Violence, Peace, and Peace Research". *Journal of Peace Research*, 6(3), 167-191. https://doi.org/10.1177/002234336900600301

Glockner, I. e Rittberger, B. (2012) "The European Coal and Steel Community (ECSC) and European Defence Community (EDC) Treaties". In Laursen, F. (ed.) *Designing the European Union*. Palgrave Studies in European Union Politics. Londres: Palgrave Macmillan, London. https://doi.org/10.1057/9780230367579_2

Griffiths, R. T. (2012) "*The Founding Fathers"* in Jones, E., Menon, A. e Weatherill, S. (eds.) *The Oxford Handbook of the European Union*. Oxford: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199546282.013.0013

Kamel, A. Y. e Guérios, V. M. (2014) "A proibição do véu islâmico na França sob o viés da proteção aos direitos individuais". *IUS GENTIUM*, 8(5), pp. 74-91. https://doi.org/10.21880/ius%20gentium.v8i5.104

Huntington, S. P. (1993) "The Clash of Civilizations?" in *Foreign Affairs*, 72(3), pp. 22-49.

Kaldor, M. (2012) *New and Old Wars: Organized Violence in a Global Era*. 3rd edn. Cambridge: Polity Press. DOI:10.1111/nana.12092_9

Lawler, P. (2013) "Peace Studies". in Williams, P. D. (ed.) *Security Studies: An Introduction*". 2nd edn, Routledge, pp. 73-88.

Levinger, M. e Lytle, P.F. (2001) "Myth and mobilisation: the triadic structure of nationalist rhetoric". *Nations and Nationalism*, 7(2) 175-194. https://doi.org/10.1111/1469-8219.00011

McDonald, M. (2023) "*Security Studies: An Introduction*". 4th edn, Routledge, pp. 63-76.

Meier, K. J. e Hawes, D. P. (2009) "Ethnic Conflict in France: A Case for Representative Bureaucracy?", *The American Review of Public Administration*, 39(3), pp. 269-285.

Moravcsik, A. (1998) "*The Choice for Europe. Social Purpose and State Power from Messina to Maastricht*. Routledge.

Pais, S. de O. (2020) "*Direito da União Europeia: Legislação e jurisprudência fundamentada*". 3.ª edição. Lisboa: Quid Juris?.

Rocha, J. M. D. (2015) *A Frente Nacional Francesa. Génese do Partido e análise das intervenções Parlamentares dos seus Eurodeputados durante a Sétima Legislatura (2009-2014) do Parlamento Europeu*. Dissertação de mestrado. Porto: Faculdade de Letras da Universidade do Porto. DOI: 10.34626/bhh1-5f89

RTP. (2024) "Notre-Dame. Macron aponta sinal de esperança e novo capítulo na história de França". Disponível em: https://www.rtp.pt/noticias/mundo/notre-dame-macron-aponta-sinal-de-esperanca-e-novo-capitulo-na-historia-de-franca_v1620131 (Acedido em 2 de março de 2026).

Seif-Amirhosseini, Z. (2013) "A Critical Reassessment of Huntington's «Clash of Civilizations» Thesis". *American Journal of Islam and Society*, *30*(2), pp. 42-76. https://doi.org/10.35632/ajis.v30i2.306

VOA (2011) "França: Entrou em vigor a proibição do uso do véu islâmico". Disponível em: https://www.voaportugues.com/a/article-04-11-11-france-veil-ba119612674/1259977.html (Acedido em 2 de março de 2026).

Wendt, A. (1999) "*Social Theory of International Politics*". Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511612183

Zhang, J. (2023) "Intrinsic conflicts within ethnic and religious issues in France", *International Journal of Anthropology and Ethnology*, 7,15, pp. 2-20 https://doi.org/10.1186/s41257-023-00093-0

Zuber, V. (2010) "A laicidade republicana em França ou os paradoxos de um processo histórico de laicização (séculos XVIII-XXI)", 59, pp.161-180. https://doi.org/10.4000/lerhistoria.1370

Capítulo IV

SEGURANÇA INTERNACIONAL E DIREITO INTERNACIONAL (2)

Enhancing the Effectiveness of Humanitarian Aid in Conflict Zones through Strategic Management Approaches

Ester Bezerra Vaz Ferreira Santos

MA in International Relations and Diplomacy – Specialization in Political Diplomacy, 2024-2025 | 1st Year Student, Portucalense University

Resumo

A ajuda humanitária em contextos de conflito desempenha um papel crucial na mitigação do sofrimento humano e no apoio aos processos de recuperação. Contudo, a sua eficácia é frequentemente limitada pela volatilidade do financiamento, por ineficiências operacionais e devido a falhas de coordenação e a riscos de segurança crescentes.

Este artigo analisa de que forma abordagens de gestão estratégica podem reforçar a eficiência, a resiliência e a responsabilização das respostas humanitárias em ambientes de elevado risco.

Com base numa análise documental qualitativa, avalia a aplicabilidade dos princípios de gestão *lean*, de sistemas integrados de informação e coordenação e de quadros estruturados de gestão do risco na governança humanitária.

Argumenta-se que a implementação articulada destas abordagens pode melhorar a alocação de recursos, reduzir duplicações, reforçar a interoperabilidade e assegurar maior continuidade operacional, contribuindo assim para respostas humanitárias mais eficazes e sustentáveis em contextos afetados por conflito.

Palavras-chave: ajuda humanitária; zonas de conflito; gestão lean; sistemas de coordenação; gestão de risco; governança humanitária.

Abstract

Humanitarian aid in conflict zones plays a critical role in alleviating human suffering and supporting recovery. However, its effectiveness is often constrained by funding volatility, operational inefficiencies, coordination gaps, and escalating security risks.

This paper examines how strategic management approaches can enhance efficiency, resilience, and accountability of humanitarian responses in high-risk environments.

Based on a qualitative documental analysis, it evaluates the applicability of lean management principles, integrated information and coordination systems, and structured risk management frameworks to humanitarian governance.

It argues that their combined implementation can improve resource allocation, reduce duplication, strengthen interoperability, and reinforce operational continuity, thereby contributing to more effective and sustainable humanitarian responses in conflict-affected environments.

Keywords: *Humanitarian aid; conflict zones; lean management; coordination systems; risk governance; humanitarian effectiveness.*

Introduction

Contemporary conflict environments are characterized by increased volatility, fragmentation, and protracted crises, significantly complicating humanitarian aid delivery. Armed conflicts, protracted crises, climate-related disasters, and health emergencies have expanded both the scale and complexity of humanitarian needs. International actors, such as the United Nations (UN), the Red Cross, the Red Crescent Movement, and some governmental international organizations, play a significant role, but there is a tendency of more local, national and international non-governmental relief groups. Despite substantial investment, humanitarian aid faces challenges in efficiency, coordination, and impact, undermining its contribution to peacebuilding and long-term stability. (Bjola and Kornprobst, 2018; Cooper et al., 2015)

This policy paper aims at studying "How can strategic management approaches improve the efficiency and effectiveness of humanitarian aid in conflict zones?" through identifying and analysing the operational and systemic barriers to effective humanitarian aid and attempts to address these challenges to improve the overall effectiveness of humanitarian aid.

The methodology for this study is qualitative, by carrying out a documental analysis to analyse academic literature, books, case studies, and policy reports. It first outlines the main structural and operational challenges affecting humanitarian responses, then evaluates strategic management approaches as policy options, and finally proposes an implementation framework with targeted recommendations.

This paper aims to contribute to the discourse of improving humanitarian aid's effectiveness, especially by employing strategic management approaches to address the effectiveness and sustainability of such responses. Building this bridge may contribute to policymakers, humanitarian organizations, investors, and other stakeholders who engage in these matters.

Humanitarian Aid, a Context

Societies around the world are exposed to natural disasters, climate change, wars, armed conflicts, and pandemics (Ratajczak and Broś, 2023). Humanitarian actors operate in more than thirty-armed conflicts and over one hundred natural disasters at any given

time. (Cooper, et al., 2015) According to the United Nations (2023), 362 million people are in need of humanitarian assistance, a record high, while over 110 million people have been displaced, and 260 million face acute food insecurity, with some at risk of famine. The Global Peace Index of 2023 concludes that there has been a deterioration in global peacefulness, with ongoing conflicts playing a significant role. (Institute for Economics and Peace, 2023)

The Council of the European Union (2025) states that around 80% of the humanitarian needs today result from armed conflict. At the same time, attacks against humanitarian personnel have increased significantly, with aid workers being frequently targeted in volatile environments, as proxy targets, revenue resources, and tools for terror or propaganda. (Stoddard, et al., 2017) These trends, compounded by climate change, environmental degradation, global population growth, governance fragility, and atypical forms of conflict, have pushed the humanitarian systems to their operational limits. (Development Initiatives, 2023; European Commission, 2021; Ryfman, 2007) highlights the constant evolution of the humanitarian landscape, noting extensive changes since the end of the Second World War.

Humanitarian aid and emergency aid are two terms highly utilized in the humanitarian field; nevertheless, one is the progress of the other. Humanitarian aid or assistance refers to material and logistical assistance provided to populations affected by natural or man-made disasters, with the objective of saving lives, alleviating suffering, and preserving human dignity. (González and Gan, 2024; Development Initiatives, 2024; Council of the European Union, 2025) While the terms humanitarian aid and humanitarian action are widely used as synonyms, the latter may include other types of activities as political lobbying, testimony, or public denunciation, which may not always follow the classical humanitarian principles rooted in the IHL adopted by the United Nations. Emergency aid, on the other hand, refers to actions carried out in the act of aid that do not necessarily follow these principles. Humanitarian aid is carried out by a complex ecosystem of International Organizations, UN Agencies, Red Cross and Red Crescent Institutions, and a growing number of governmental and non-governmental actors operating at international, national, and local levels. (Cooper et al., 2015; González and Gan, 2024)

Challenges in Humanitarian Aid

Humanitarian aid operating in conflict zones faces numerous obstacles that are a barrier to effective and efficient aid. These constraints are intensified by conflicts, climate change, and economic instability, which simultaneously increase the needs and reduce the operational space.

The World Disasters Report of 2018 categorises obstacles to aid delivery into three main categories: physical barrier including terrain, climate and lack of infrastructure; conflict and insecurity such as ongoing hostilities, violence against humanitarian

personnel or assets/facilities, presence of remnants of war; and political or administrative restrictions imposed by affected or donor governments, including access limitations and interference in humanitarian activities. (International Federation of Red Cross and Red Crescent Societies (IFRC), 2018) These constraints directly affect the capacity of humanitarian actors to deliver timely and principled assistance.

Building on this framework, this paper broadly categorizes these pressing challenges into four areas that will further be developed: funding, resource allocation and logistics, coordination among actors, and security risks for personnel and resources. These areas provide the analytical foundation for assessing how strategic management approaches can strengthen humanitarian performance in conflict-affected environments.

Funding

Funding limitations constitute one of the most persistent structural barriers to effective humanitarian aid. Although overall humanitarian expenditure has been increasing over the years, the growth of people in need of aid has outpaced available resources, resulting in the widening of the funding gap. In 2024, global humanitarian appeals reached record levels, with the number of humanitarian crises growing, yet funding coverage remained significantly below requirements, forcing actors to scale back and prioritize only the most urgent responses. (Development Initiatives, 2023; 2024)

Humanitarian aid relies mainly on donor funding, which is often dependent on a limited group, inconsistent, and correlated to geopolitical interests and subject to budget cuts. This concentration of funding reduces flexibility, fragments programming, and constrains long-term planning. (Development Initiatives, 2024; United Nations Office for the Coordination of Humanitarian Affairs, 2025) Chronic underfunding is widely documented by UN agencies, humanitarian organizations, and across the news highlights, such as Reuters, the World Food Program, and on the BBC, having direct consequences for food security, displacement responses, and protection mechanisms in protracted crises. (BBC News, 2009; Bradley, 2023; Farge, 2024; Foster, 2022; World Food Programme, 2023)

Beyond quantitative shortages, structural weaknesses in funding models contribute to operational inefficiencies. Short funding cycles encourage reactive responses rather than preventive or resilience-oriented approaches. Competition among agencies for limited resources may incentivise duplication, undermine coordination, and reduce overall system coherence. Moreover, politicised access conditions can distort allocation decisions. (ALNAP, 2025; Farber et al., 2024; Lombardo and Patrick, 2025; Stoddard et al., 2017; United Nations Regional Information Centre for Western Europe, 2025)

Funding constraints are increasingly correlated with issues of credibility and trust. Repeated funding appeals, visible inefficiencies, duplication of efforts, and cases of diversion or misuse of aid have contributed to donor scepticism and compassion fatigue. In politically polarized environments, humanitarian organizations are often scrutinized for perceived lack of neutrality, accountability, and measured impact. This erosion of

trust risks further constraining funding flows, creating a vicious cycle of underperformance and underfunding reinforcing each other. (Dreher et al., 2024; European Commission Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO), 2025; Gosp-Server, 2025; Lilly and Pearson , 2025; Lombardo and Patrick, 2025; Norman, 2024) Strengthening transparency, performance measurement, and accountability mechanisms is therefore not only an operational necessity but also a strategic imperative for sustaining donor confidence and long-term financial support.

Historical experiences, such as the Ethiopian famine of 1980s illustrate how political conditionality, misuse of aid and sovereignty concerns can undermine effectiveness and donor confidence. (BBC News, 2009; Bradley, 2023; Solomon, 2016) These dynamics demonstrate that funding challenges are not solely financial but organizational and strategic. Addressing them requires management approaches capable of improving resource optimisation, enhancing accountability, and strengthening prioritization mechanisms within constrained financial environments.

Resource Allocation and Logistics

Resource allocation and logistical management constitute critical determinants of humanitarian effectiveness in conflict environments. Damaged infrastructure, insecure transport routes, limited storage capacity, and restricted access significantly complicate supply chain operations, delaying the delivery of essential goods and services. In such contexts, inefficiencies in forecasting, procurement, and distribution may result in duplication, overstocking in certain areas, and acute shortages in others. (Heaslip, et al., 2024)

Environmental considerations form part of this broader logistical challenge. The International Committee of the Red Cross (ICRC) has acknowledged that humanitarian operations may generate unintended environmental impact, including resource overuse, waste accumulation, and infrastructure strain. (International Committee of the Red Cross (ICRC), Assistance Division, 2010) In conflict zones where waste management systems are disrupted, humanitarian packaging materials are often burned or buried, contributing to pollution and public health risks. (Joint Initiative for Sustainable Humanitarian Assistance Packaging Waste Management, 2023) These dynamics illustrate how logistical inefficiencies can undermine both sustainability and community resilience.

Case studies from protracted crises further demonstrate systemic weaknesses in humanitarian supply chains. In contexts such as Syria or the Great Lakes refugee crisis, damaged infrastructure, bureaucratic bottlenecks, and fragmented coordination delayed aid delivery and increased costs. (OCHA, 2024; Wilkinson, 1997) Inflation, fuel price volatility, and pandemic-related disruptions have further exacerbated transportation costs, reducing the proportion of resources available for direct assistance. (Margesson, et al., 2012)

Coordination and Duplication of Efforts

The expansion of humanitarian actors in the context of globalization has increased operational capacity but also intensified coordination challenges. International NGOs, UN agencies, regional organizations, and local actors frequently operate simultaneously in crisis environments, often with overlapping mandates and limited interoperability. The absence of effective coordination mechanisms may result in duplication of efforts in some areas and critical gaps in others. (Bildt, 2011; Cooper et al., 2015) Past large scale responses illustrate the systemic nature of this problem. During the 2010 Haiti earthquake response, hundreds of organizations operated independently, leading to overlapping interventions in certain sectors while other communities received limited assistance. The same happened with the Vanuatu crisis, where unsolicited bilateral donations were received, some inappropriate for the context, something that overwhelmed the government's warehousing and sorting capacity. (Inter-Agency Standing Committee, 2010; International Federation of Red Cross and Red Crescent Societies (IFRC), 2018; Weisenfeld, 2011) These cases reveal that fragmentation generates not only inefficiency but also reputational costs and erosion of trust.

Coordination challenges are further compounded by competition for funding and visibility. Agencies may prioritise projects aligned with donor preferences rather than context-specific needs, reinforcing fragmentation and reducing system-wide coherence. (Moers and Annen, 2017)

Ineffective Information Sharing

Limited information exchange exacerbates duplication and misallocation of resources. In rapidly evolving conflict environments, timely and interoperable data systems are essential for prioritization and adaptive response. Although initiatives such as the Humanitarian Data Exchange (HDX) created by OCHA have expanded data availability since 2014, coverage remains uneven and data integration across actors is inconsistent. (HDX Team, 2024) Without reliable real-time information, humanitarian actors face constrains in forecasting needs, coordinating interventions, and avoiding overlap. Timely information makes the allocation of resources more effective and helps adapt to the constantly evolving context of conflict zones.

The experience of global health crises, such as COVID-19, demonstrated how real-time dashboards and shared data platforms can enhance strategic coordination and resource allocation. (Johns Hopkins University Center for Systems Science and Engineering, 2020) Comparable integration remains limited in many humanitarian conflict settings.

Cultural and Political Barriers

Coordination is further weakened by organizational cultures, operational mandates, and political interests. Local actors, despite their contextual knowledge and proximity to

affected populations, are frequently marginalized in decision-making process. Language barriers, technical jargon, and institutional hierarchies restrict meaningful participation, particularly for smaller local organizations and women-led groups. (Inter-Agency Standing Committee (IASC), 2021) Power imbalances within coordination mechanisms can undermine inclusivity and reduce culturally appropriate responses. (Inter-Agency Standing Committee, 2019; Nyarko, Marnicio and Bollettino, 2024)

These structural, informational, and cultural constraints demonstrate that coordination challenges are systemic rather than incidental. Strengthening interoperability, enhancing data integration and institutionalising inclusive coordination frameworks are therefore essential to reducing duplication, improving accountability, and maximising collective impact in conflict-affected environments.

Security Risks for Personnel and Resources

Security constraints constitute one of the most critical challenges in conflict-affected environments. With approximately 80 percent of current humanitarian needs stemming from armed conflicts (Council of the European Union, 2025), aid operations are increasingly conducted in highly volatile and militarized contexts. These conditions expose humanitarian personnel and assets to significant risks, disrupting delivery mechanisms and constraining access to affected populations.

Although international humanitarian law guarantees the rapid and unimpeded passage of all relief consignments and personnel (Art. 70, Additional Protocol I to the Geneva Conventions), access is frequently restricted in practice. Blockades, bureaucratic impediments and deliberate targeting of humanitarian actors undermine operational continuity and increase delivery costs. (International Federation of Red Cross and Red Crescent Societies (IFRC), 2018)

The Aid Worker Security Report 2024 and the Aid Worker Security Database identified 2023 as the deadliest year for humanitarian personnel, with 280 aid workers killed and a total of 595 aid victims across 280 incidents. (Humanitarian Outcomes, 2024) The increasing involvement of state actors in attacks against aid workers further complicates advocacy efforts and challenges traditional protection strategies.

Beyond physical violence, theft, and diversion of resources remain persistent risks. In contexts such as Yemen, Syria, and Somalia, aid envoys have been blocked, looted, or manipulated by armed groups, significantly reducing effective coverage. (International Federation of Red Cross and Red Crescent Societies (IFRC), 2018; Rono, 2017; Tran, 2013) These disruptions not only exacerbate civilian suffering but also erode donor confidence and inflate operational costs.

Security risks therefore represent not only a humanitarian protection issue but also a strategic management challenge. Unpredictable access conditions, asset loss, and personnel threats need systematic risk assessment, contingency planning, and adaptative operational models. Strengthening risk governance mechanisms is essential to maintaining continuity, accountability, and effectiveness in high-risk environments.

Policy Options: Management Strategies for Humanitarian Aid

Building on the challenges identified – funding gaps, logistical inefficiencies, coordination failures, and security volatility – this section evaluates three contemporary management approaches: Lean Management for Efficiency, Integrated Coordination Systems, and Risk Management Frameworks. Together, these strategies provide structured mechanisms to enhance the effectiveness, accountability and operational resilience of humanitarian operations in conflict zones.

Resource Optimization through Lean Management

Lean management offers a systemic framework for improving efficiency in resource-constrained environments by eliminating non-value-adding activities and promoting continuous improvement. Originally developed within the manufacturing systems, lean principles have increasingly been applied in the healthcare sector, public sector organizations, and the banking sector, demonstrating their ability beyond industrial contexts. (Danese et al., 2024; Heizer and Render, 2013; Heizer et al., 2017; Kaizen Institute, n.d.; Klein et al., 2022; McKinsey and Company, 2011; Shingo, 1989)

In humanitarian settings characterized by funding volatility, logistical complexity, and urgent time pressures, lean principles can directly address operational inefficiencies. The core lean philosophy centres on five interrelated principles: defining value from a beneficiary's perspective; mapping the value stream to identify non-essential steps; ensuring continuous flow; adopting pull-based systems aligned with real-time demand; and pursuing continuous improvement through collective learning. (The Kaizen Institute, n.d.; The Access Group, 2019; Klein et al., 2022; Womack and Jones, 1996; Abdelhamid et al., 2008)

Applied to humanitarian operations, "value" is about the urgent need of affected populations – such as access to water, food, shelter, or even medical care. Value stream mapping enables organizations to distinguish between essential activities, such as last-mile delivery, and non-value-adding processes, including redundant paperwork or inefficient transport routes. Pull systems, supported by real-time data, reduce overstocking and misallocation by aligning distribution with evolving field conditions.

Heizer et al, (2017) state on their book that "Lean producers set their sights on perfection: no bad parts, no inventory, only value-added activities and no waste." (Heizer, et al., 2017, p. 676) Lean management also identifies eight categories of operational waste, commonly summarized as DOWNTIME, that stands for: defects, overproduction, waiting, non-utilized talent, transportation, inventory, motion and excess processing. (Abdelhamid et al., 2008; Heizer et al., 2017; Heizer and Render, 2013; Klein et al., 2022; Shingo, 1989; The Kaizen Institute, n.d.; Womack and Jones, 1996) Adapting to the humanitarian context, these can manifest as: defects are inaccurate need assessments or damaged supplies requiting relocation; overproduction, as delivery of inappropriate or premature aid; waiting refers to the delays caused by

bureaucratic approval or transportation bottlenecks; non-utilized talent is the marginalization of local actors and underuse of local and field expertise; transportation as inefficient routing that results in increasing cost or delay; inventory is the excess stockpiling or critical shortages; for motion, unnecessary movement of personnel due to poor planning; and finally excess processing takes place in the form of overly complex documentation or compliance procedures.

By systemically identifying and reducing these inefficiencies, lean management approaches can improve cost-efficiency, shorten delivery cycles, and enhance accountability. (Abdelhamid et al., 2008; Klein et al., 2022; Shingo, 1989; The Access Group, 2019; The Kaizen Institute, n.d.; Womack and Jones, 1996) In resource-constrained and donor-dependent conflict environments, even marginal gains in efficiency translate into expanded coverage and improved beneficiary outcomes.

Integrated Information and Coordination Systems

Effective humanitarian coordination depends fundamentally on timely, reliable, and interoperable information flows. As demonstrated in the previous sections, duplication of efforts, resource misallocation and delayed responses often stem from fragmented data systems and limited institutional interoperability. Integrated Information and Coordination Systems are comprehensive frameworks that facilitate efficient information sharing, processing, and coordination among various stakeholders, departments, or organizations. They offer a structural response to these deficiencies by enabling real-time data sharing, harmonized reporting standards, and coordinated decision-making across actors. (Skoumpopoulou and Abdelrahman, 2022; Stipić and Gambiroža, 2022; Varmus et al., 2024)

In humanitarian contexts, such systems can facilitate shared situational awareness, improved tracking of resources, and clearer identification of unmet needs. Digital coordination platforms and interoperable databases allow organizations to visualize operational gaps, reduce overlap, and prioritize interventions based on evolving field conditions. Experiences from global health crises have illustrated how centralized dashboards and open data platforms enhance coordination and strategic planning. (HDX Team, 2024; Johns Hopkins University Center for Systems Science and Engineering, 2020)

Beyond operational efficiency, an integrated system strengthens transparency and accountability. Real-time tracking of financial flows, procurement processes, and distribution channels can improve donor confidence and mitigate concerns regarding misuse or diversion of aid. In resource-constrained environments, enhanced visibility over resource allocation contributes directly to optimized decision-making and performance evaluation. (Düchting, 2024; Sahithi et al., 2025)

However, the implementation of integrated coordination systems in conflict-affected environments, also presents structural challenges. Local organizations may lack the digital infrastructure, technical capacity, or access to decision-making platforms, reinforcing existing power asymmetries. Ensuring inclusive system design and capacity-

building for local actors is therefore essential to avoid further marginalization. (Inter-Agency Standing Committee, 2019; Inter-Agency Standing Committee (IASC), 2021; Nyarko et al., 2024)

Additionally, centralized data architectures introduce cybersecurity risks. In conflict environments, sensitive operational data may become a target for state or non-state actors. (International Committee of the Red Cross, 2022) Robust data protection protocols and risk mitigation strategies must therefore accompany digital integration efforts.

When properly designed, integrated information and coordination systems can reduce fragmentation, enhance collective impact, and improve adaptive capacity in volatile environments. Their effectiveness depends not only on technological infrastructure but also in governance structures that promote interoperability, inclusivity, and shared accountability.

Risk Management Framework for Field Operations

Operating in conflict-affected environments requires structured approaches to managing uncertainty, volatility, and exposure to harm. Risk Management Framework (RMF) for field operations provides a structured approach to identifying, assessing, mitigating, and monitoring risks to ensure safety, efficiency, and effectiveness in dynamic and potentially high-risk environments. (National Institute of Standards and Technology (NIST), 2018) Although initially developed within technical and cybersecurity domains, RMF principles are increasingly applied across organizational settings, including humanitarian field operations.

In humanitarian contexts, risk governance is essential to safeguarding personnel, protecting assets, and ensuring continuity of operations. Organizations such as the International Federation of Red Cross and Red Crescent Societies (IFRC) have progressively integrated risk management principles in humanitarian field operations as part of institutional policy, recognising its centrality to operational resilience. (International Federation of Red Cross and Red Crescent Societies (IFRC), 2020; International Federation of Red Cross and Red Crescent Societies (IFRC), 2022)

A robust RMF for humanitarian field responses typically includes four interrelated components. First is risk identification, involving systematic threat analysis and contextual assessment of security, political, logistical and environmental risks. Second, risk assessment, in which likelihood and potential impacts are evaluated through structured prioritization tools, enabling resource allocation based on severity. Third, risk mitigation and contingency planning combine scenario-based preparedness and adaptative logistical strategies. Fourth, monitoring and review ensure continuous adjustments of operational plans in response to evolving field conditions.

In conflict zones characterized by restricted access, targeted violence, and asset diversion, structured risk governance enhances decision-making under uncertainty. It supports cost forecasting, strengthens accountability mechanisms, and reduces exposure to catastrophic operational failure.

Importantly, risk management in humanitarian settings must remain dynamic rather than compliance-driven. Real-time reporting mechanisms, scenario-modelling, and inclusive communication structures enable adaptative responses to rapidly shifting threats. Integrated risk assessment into strategic planning processes ensures that security considerations are not treated as external constraints but as core components of operational design.

When embedded within broader management reforms, a Risk Management Framework contributes to operational continuity, improved resource protection, and strengthened donor confidence in volatile environments.

Implementation Strategy and Policy Implications

The preceding analysis has demonstrated that inefficiencies in humanitarian aid responses are not isolated operational shortcomings, but manifestations of structural and systemic constraints. Funding volatility, logistical fragmentation, coordination gaps, and escalating security risks interact in ways that undermine the effectiveness and sustainability of humanitarian responses. Addressing these challenges requires not only the adoption of isolated managerial tools but also the integration of complementary management approaches within a coherent governance framework.

Lean Management contributes primarily at the operational level by enhancing internal efficiency and reducing waste across supply chains and administrative processes. By aligning activities with clearly defined beneficiary value and eliminating non-value-adding procedures, humanitarian actors can mitigate resource misallocation and improve responsiveness in time-sensitive contexts. However, efficiency gains within individual organizations remain insufficient if not supported by a system-wide coordination.

Subsequently, Integrated Information and Coordination Systems address this structural dimension. The standardisation of data-sharing protocols, improved interoperability across platforms, and inclusive coordination mechanisms can reduce duplication and enhance collective impact. In contexts characterized by multiple overlapping actors, digital integration must be accompanied by governance arrangements that ensure equitable participation, particularly for local actors whose contextual knowledge is critical to effective intervention.

Risk Management Frameworks complement these approaches by embedding structured risk assessment and adaptive planning within field operations. Given the volatility of conflict environments, operational continuity depends on the ability to anticipate disruption, protect personnel, and safeguard assets. Integrating risk governance into strategic planning processes strengthens institutional resilience and enhances donor confidence in high-risk settings.

Taken together, these three approaches form an interdependent model for humanitarian governance. Operational optimization without coordination reforms risks reproducing fragmentation at scale. Coordination without efficiency remains resource-intensive.

And both are vulnerable in the absence of structured risk governance. A coherent implementation strategy requires, therefore, a gradual institutional integration rather than an abrupt structural overhaul.

In practical terms, this implies embedding efficiency diagnostics within routine operational reviews, progressively strengthening data interoperability standards across humanitarian clusters, and formalizing risk assessment mechanisms within planning cycles. Such reforms must be aligned with funding structures that incentivise flexibility, collaboration, and long-term, capacity building. The transition toward more strategic governance is necessarily incremental, requiring institutional commitment, leadership engagement, and sustained investment in organizational learning.

Conclusion

Humanitarian aid in conflict zones remains essential for the protection of civilian populations and the mitigation of large-scale human suffering. Yet, as this study demonstrated, persistent inefficiencies in funding structures, logistical systems, coordination mechanisms, and security governance continue to limit overall effectiveness. These challenges are systemic rather than incidental, requiring structural rather than ad hoc responses.

By examining the potential contribution of strategic management approaches, this paper has argued that improvements in humanitarian performance depend on the integration of operational optimization, institutional interoperability, and structured risk governance. Lean Management offers mechanisms to reduce waste and align operations with beneficiary value; Integrated Information and Coordination Systems strengthen collective action and transparency; and Risk Management Frameworks enhance resilience in volatile environments. When implemented coherently, these approaches reinforce one another and contribute to a more adaptive and accountable humanitarian architecture.

The adoption of such management – oriented reforms does not imply the corporatisation of humanitarian responses. Rather, it reflects the necessity of equipping humanitarian systems with governance tools capable of responding to increasingly complex and protracted crises. As humanitarian needs continue to grow while resources remain constrained, the strategic optimization of existing capacities becomes imperative.

Strengthening efficiency, coordination, and risk governance ultimately enhances not only operational performance but also institutional credibility and donor confidence. In this sense, improving humanitarian effectiveness is both a strategic and ethical responsibility. Advancing toward more structured and resilient management modes can contribute to safeguarding humanitarian principles while ensuring that assistance reaches those most in need in a timely and sustainable manner.

References

Abdelhamid, T. S., El-Gafy, M. A. and Salem, O. M. (2008) "Lean construction: Fundamentals and principles". *The American Professional Constructor,* Fall 2008, pp. 8-19.

ALNAP (2025) *Global Humanitarian Assistance 2025,* London: ALNAP/ODI.

BBC News (2009) *Ethiopia admits aid problems.* [online] Available at: http://news.bbc.co.uk/2/hi/africa/2551589.stm [Accessed 01 2025].

Bildt, C. (2011) *Dag Hammarskjöld and United Nations peacekeeping.* [online] Available at: https://www.un.org/en/chronicle/article/dag-hammarskjold-and-united-nations-peacekeeping [Accessed 04 2025].

Bjola, C. and Kornprobst, M. (2018) *Understanding International Diplomacy: Theory, Practice and Ethics.* Routledge.

Bradley, M. (2023) *The Politics and Everyday Practice of International Humanitarianism.* Oxford: Oxford University Press.

Cooper, A., Heine, J. and Thakur, R. (2015) *The Oxford Handbook of Modern Diplomacy.* Oxford: Oxford University Press.

Council of the European Union (2025) *Humanitarian aid.* [online] Available at: https://www.consilium.europa.eu/en/policies/humanitarian-aid/[Accessed 01 2026].

Danese, P., Romano, P. and Sunic, H. A. M. (2024) Implementing lean management in hospitals: a survey on social and technical outcomes of kaizen initiatives. *International Journal of Production Research,* 62(24), pp. 8745-8765.

Development Initiatives (2023) *Global Humanitarian Assistance Report 2023.* [online] Available at: https://devinit.org/resources/global-humanitarian-assistance-report-2023 [Accessed 01 2025].

Development Initiatives (2024) *Falling short? Humanitarian Funding and Reform.* [online] Available at: https://devinit.org/resources/falling-short-humanitarian-funding-reform/methodology-definitions/#downloads [Accessed 01 2025].

Dreher, A., Lang, V. and Reinsberg, B. (2024) Aid effectiveness and donor motives. *World Development,* 176, (106501).

Düchting, A. (2024) *Humanitarian Topics explained: Digitalisation in humanitarian action to go,* Berlin: Centre for Humanitarian Action.

European Commission Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO) (2025) *Information manipulation and misinformation – A threat for EU civil protection & humanitarian aid.* [online] Available at: https://civil-protection-humanitarian-aid.ec.europa.eu/resources-campaigns/information-manipulation-and-misinformation_en [Accessed 01 2026].

European Commission (2021) *Communication from the Commission to the European Parliament and the Council on the EU's humanitarian action: New challenges, same principles (COM(2021) 110 final).* [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0110[Accessed 04 2025].

Farber, V., Reichert, P., Martin, M. and Galligo, J. L. C. (2024) *Humanitarian Impact Finance: Instruments & Approaches.* Lausanne: International Institute for Management Development.

Foster, A. (2022) *Syria: Food aid to 3m people at risk after UN stalemate*. [online] Available at: https://www.bbc.com/news/world-62066506 [Accessed 01 2025].

González, P. A. and Gan, R. K. (2024) The evolution of humanitarian aid in disasters: Ethical implications and future challenges. *Philosophies,* 9(3), 62. https://doi.org/10.3390/philosophies9030062

Gosp-Server, L. (2025) *The crucial role of humanitarian communication in the fake news and "infoglut" era*. [online] Available at: https://www.alternatives-humanitaires.org/en/2025/07/30/the-crucial-role-of-humanitarian-communication-in-the-fake-news-and-infoglut-era/ [Accessed 01 2026].

HDX Team (2024) *Reflecting on ten years of HDX*. [online] Available at: https://centre.humdata.org/reflecting-on-ten-years-of-hdx/ [Accessed 01 2025].

Heaslip, G., Listou, T., Skoglund, P. O. and Sigala, I. F. (2024) Guest editorial: Humanitarian logistics in conflict zones and complex emergencies. *Journal of Humanitarian Logistics and Supply Chain Management,* 14(2), pp. 137-139.

Heizer, J. and Render, B. (2013) *Operations Management*. 10th ed. Harlow: Pearson.

Heizer, J., Render, B. and Munson, C. (2017) *Operations Management: Sustainability and Supply Chain Management*. 12th ed. Harlow: Pearson.

Humanitarian Outcomes(2024) *Aid Worker Security Report 2024: Balancing advocacy and security in humanitarian action*. [online] Available at: https://humanitarianoutcomes.org/AWSR_2024 [Accessed 01 2025].

Institute for Economics & Peace (2023) *Global Peace Index 2023: Measuring peace in a complex world*. [online] Available at: https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf [Accessed 01 2025].

Inter-Agency Standing Committee (IASC) (2021) *Guidance on strengthening participation, representation, and leadership of local and national actors in IASC humanitarian coordination mechanisms*. Geneva: IASC.

Inter-Agency Standing Committee, 2010. *Response to the humanitarian crisis in Haiti following the 12 January 2010 earthquake: Achievements, challenges, and lessons to be learned.* . Geneva: IASC.

Inter-Agency Standing Committee, 2019. *Supporting principled national and local NGOs in humanitarian response*. [online] Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/2019-01-15-P2P-Localisation-Note_FINAL.pdf [Accessed 01 2025].

International Committee of the Red Cross (ICRC), Assistance Division, 2010. Framework for environmental management in assistance programmes. *International Review of the Red Cross,* pp. 92(879), 747-797.

International Committee of the Red Cross (2022) *Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people*. [online] Available at: https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people [Accessed 01 2026].

International Federation of Red Cross and Red Crescent Societies (IFRC) (2018) *World Disasters Report 2018,* Geneva: IFRC.

International Federation of Red Cross and Red Crescent Societies (IFRC) (2020) *Disaster risk management policy: From prevention to response and recovery,* Geneva: IFRC.

International Federation of Red Cross and Red Crescent Societies (2018) *World Disasters Report 2018: Leaving millions no one behind*. [online] Available at: https://www.ifrc.org/sites/default/files/2021-09/C-03-WDR-2018-3-reach.pdf [Accessed 01 2025].

Johns Hopkins University Center for Systems Science and Engineering (2020) *COVID-19 Dashboard.*

Joint Initiative for Sustainable Humanitarian Assistance Packaging Waste Management (2023) *Guidelines for packaging waste management in humanitarian operations.* [online]

Kaizen Institute (n.d.) *Definition and advantages of lean management.* [online] Available at: https://kaizen.com/insights/definition-advantages-lean-management/[Accessed 01 2025].

Klein, L. L. et al. (2022) The influence of lean management practices on process effectiveness: A quantitative study in a public institution. *SAGE Open,* 12(1), pp. 1-14.

Lilly, D. and Pearson , M., (2025) *In numbers we trust: How "prioritisation" makes humanitarian numbers murky.* [online] Available at: https://www.thenewhumanitarian.org/analysis/2025/01/27/numbers-we-trust-how-prioritisation-makes-humanitarian-aid-numbers-murky [Accessed 01 2026].

Lombardo, A. and Patrick, S. (2025) *The Painful, Seismic Shift in Humanitarian Aid—and What's Next.* [online] Available at: https://carnegieendowment.org/research/2025/12/the-painful-seismic-shift-in-humanitarian-aidand-whats-next [Accessed 12 2025].

McKinsey and Company (2011) *Lean management: New frontiers for financial institutions.* [online] Available at: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/financial%20services/latest%20thinking/reports/lean_management_new_frontiers_for_financial_institutions.pdf [Accessed 01 2025].

Moers, L. and Annen, K. (2017) Donor competition for aid impact, and aid fragmentation. *The World Bank Economic Review,* 31(3), p. 708–729.

National Institute of Standards and Technology (NIST), 2018. *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (Special Publication 800-37, Revision 2),* Gaithersburg, MD: U.S. Department of Commerce.

Norman, J. (2024) Humanitarian principles are under fire in Ukraine. *DIIS Policy Brief,* 2024.

Nyarko, G., Marnicio, A. and Bollettino, V. (2024) Understanding leadership challenges faced by humanitarian aid workers: Insights from the experiences of NNPHL training participants. *Journal of International Humanitarian Action,* 9(15).

OCHA (2024) *Syria: Recent developments in Aleppo – Flash Update No. 4.* [online] Available at: https://reliefweb.int/report/syrian-arab-republic/syria-recent-developments-aleppo-flash-update-no-4-01-december-2024 [Accessed 01 2025].

Ratajczak, M. and Broś , N. (2023) Humanitarian diplomacy: The case of Switzerland and Sweden. *Politeja,* 20(1(82)), pp. 143-163.

Rono, M. (2017) *Somalia food crisis: Has al-Shabab adopted new approach to food aid?.* [online] Available at: https://www.bbc.com/news/world-africa-39296517 [Accessed 01 2025].

Ryfman, P. (2007) Non-governmental organizations: An indispensable player of humanitarian aid. *International Review of the Red Cross,* 89(865), pp. 21-44.

Sahithi, M., Varsha, R., Dhanya, L. and Nambiar Pv, M. (2025) A Blockchain Based Solution for Transparent Charity Donations. *International Journal of Engineering Research & Technology (IJERT),* 14(05).

Shingo, S. (1989) *A study of the Toyota production system from an industrial engineering viewpoint.* Productivity Press.

Skoumpopoulou, D. and Abdelrahman, M. (2022) Integrated information systems in higher education: Systematic review and research opportunities. *ANWESH: International Journal of Management and Information Technology,* 7(2), pp. 57-64.

Solomon, N. (2016) *1984: The parable of Ethiopian famine and foreign aid.* [online] Available at: https://aidhistory.ca/1984-the-parable-of-ethiopian-famine-and-foreign-aid/ [Accessed 01 2025].

Stipić, V. V. and Gambiroža, D. (2022) Integrated information systems as support to controlling: A factor of successful business of the company. *Journal of Accounting and Management,* pp. 12(1), pp. 37-48.

Stoddard, A. et al. (2017) *Efficiency and Inefficiency in Humanitarian Financing.* London Humanitarian Outcomes.

Stoddard, A. et al. (2017) Out of reach: How insecurity prevents humanitarian aid from accessing the neediest. *Stability: International Journal of Security & Development,* 6(1), Article 1, pp. 1-25.

The Access Group (2019) *The Access Group.* [online] Available at: https://www.theaccessgroup.com/media/24539/five-principles-for-creating-superior-value.pdf [Accessed 01 2025].

Tran, M. (2013) *Al-Shabaab in Somalia exploited aid agencies during 2011 famine – report.* [Online] Available at: https://www.theguardian.com/global-development/2013/dec/09/al-shabaab-somalia-exploited-aid-agencies-famine [Accessed 01 2025].

United Nations Office for the Coordination of Humanitarian Affairs (2025) *Global Humanitarian Overview 2026*. [online] Available at: https://humanitarianaction.info/document/global-humanitarian-overview-2026 [Accessed 2025].

United Nations Regional Information Centre for Western Europe (2025) *Humanitarian aid: the most vulnerable already severely impacted by budget cuts.* [online] Available at: https://unric.org/en/humanitarian-aid-the-most-vulnerable-already-severely-impacted-by-budget-cuts/ [Accessed 01 2026].

United Nations (2023) *Record numbers of people need humanitarian assistance.* [online] Available at: https://unis.unvienna.org/unis/en/topics/related/2023/humanitarian-need.html [Accessed 01 2025].

Varmus, M., Kubina, M., Mičiak, M. and Šarlák, M. (2024) Integrated sports information systems: Enhancing data processing and information provision for sports in Slovakia. *Systems,* 12(6), 198.

Weisenfeld, P. E. (2011) Successes and challenges of the Haiti earthquake response: The experience of USAID. *Emory International Law Review,* pp. 1097-1120.

Wilkinson, R., 1997. *Heart of darkness.* [online] Available at: https://www.unhcr.org/publications/refugees-magazine-issue-110-crisis-great-lakes-cover-story-heart-darkness [Accessed 01 2025].

Womack, J. P. and Jones, D. T. (1996) *Lean thinking: Banish waste and create wealth in your corporation.* New York: Free Press.

World Food Programme (2023) *Syria in crisis: Food ration cuts set to plunge millions into severe hunger.* [online] Available at: https://www.wfp.org/stories/syria-crisis-food-ration-cuts-set-plunge-millions-severe-hunger [Accessed 01 2025].

Índice de IDN Cadernos Publicados

III SÉRIE		
2026	57	VII Seminário de Defesa Nacional
2025	56	VI Seminário de Defesa Nacional
2024	55	V Seminário de Defesa Nacional
	54	IX Seminário IDN Jovem
	53	VIII Seminário IDN Jovem
2023	52	As Consequências Estratégicas da Guerra Russo-Ucraniana
	51	IV Seminar of the Atlantic Centre
	50	IV Seminário de Defesa Nacional
2022	49	VII Seminário IDN Jovem
	48	*Zeitenwende:* a Alemanha, a NATO e a Segurança Europeia no Contexto da Guerra na Ucrânia
	47	VI Seminário IDN Jovem
	46	III Seminário de Defesa Nacional
	45	III Seminário do Centro do Atlântico
2021	44	Documentos Estratégicos de Segurança e Defesa
	43	II Seminário de Defesa Nacional
	42	Tattered Alliance: Donald Trump and Europe
	41	Cyber Defence in the 5+5 Area: Prospects for Cooperation
	40	Atlantic Centre
2020	39	Dragon Rejuvenated: Making China Greatest Again
	38	Atlantic Centre for Defence Capacity Building
	37	Prospects for Euro-Atlantic Cooperation
	36	V Seminário IDN Jovem
	35	A Antártida no Espaço Geopolítico do Atlântico Sul
2019	34	Despojos de Guerra: As Consequências e Sequelas da Primeira Guerra Mundial
	33	IV Seminário IDN Jovem
	32	Seminário de Defesa Nacional
2018	31	A Democracia na Europa: Alemanha, França, Reino Unido e Espanha Face às Crises Contemporâneas
	30	III Seminário IDN Jovem
	29	Cibersegurança e Políticas Públicas: Análise Comparada dos Casos Chileno e Português
	28	Contributos para uma Estratégia Nacional de Ciberdefesa

2017	27	Economia da Defesa Nacional
	26	Novo Século, Novas Guerras Assimétricas? Origem, Dinâmica e Resposta a Conflitos não-Convencionais
	25	II Seminário IDN Jovem
	24	Geopolitics of Energy and Energy Security
	23	I Seminário IDN Jovem
	22	Entering the First World War
2016	21	Os Parlamentos Nacionais como Atores Dessecuritizadores do Espaço de Liberdade, Segurança e Justiça da União Europeia: O Caso da Proteção de Dados
	20	América do Sul: uma Visão Geopolítica
2015	19	A Centralidade do Atlântico: Portugal e o Futuro da Ordem Internacional
	18	Uma Pequena Potência é uma Potência? O Papel e a Resiliência das Pequenas e Médias Potências na Grande Guerra de 1914-1918
	17	As Ásias, a Europa e os Atlânticos sob o Signo da Energia: Horizonte 2030
	16	O Referencial Energético de Gás Natural Euro-Russo e a Anunciada Revolução do *Shale Gas*
2014	15	A Diplomacia Militar da China: Tipologia, Objetivos e Desafios
	14	Geopolítica e Geoestratégia da Federação Russa: a Força da Vontade, a Arte do Possível
	13	Memória do IDN
2013	12	Estratégia da Informação e Segurança no Ciberespaço
	11	Gender Violence in Armed Conflicts
	10	As Revoltas Árabes e a Democracia no Mundo
	9	Uma Estratégia Global para Portugal numa Europa em Crise
2012	8	Contributo para uma "Estratégia Abrangente" de Gestão de Crises
	7	Os Livros Brancos da Defesa da República Popular da China, 1998-2010: Uma desconstrução do Discurso e das Perceções de (in)Segurança
2011	6	A Arquitetura de Segurança e Defesa da Comunidade dos Países de Língua Portuguesa
	5	O Futuro da Comunidade de Segurança Transatlântica
	4	Segurança Nacional e Estratégias Energéticas de Portugal e de Espanha
	3	As Relações Energéticas entre Portugal e a Nigéria: Riscos e Oportunidades
2010	2	Dinâmicas Migratórias e Riscos de Segurança em Portugal
	1	Acerca de "Terrorismo" e de "Terrorismos"

II SÉRIE		
2009	4	O Poder Aéreo na Transformação da Defesa
		O Programa de Investigação e Tecnologia em Veículos Aéreos Autónomos Não-Tripulados da Academia da Força Aérea
	3	Conhecer o Islão
2008	2	Cibersegurança
		Segurança e Insegurança das Infra-Estruturas de Informação e Comunicação Organizacionais
	1	Conflito e Transformação da Defesa
		A OTAN no Afeganistão e os Desafios de uma Organização Internacional na Contra-subversão
		O Conflito na Geórgia

I SÉRIE		
2007	5	Conselho de Segurança das Nações Unidas Modelos de Reforma Institucional
	4	A Estratégia face aos Estudos para a Paz e aos Estudos de Segurança. Um Ensaio desde a Escola Estratégica Portuguesa
2006	3	Fronteiras Prescritivas da Aliança Atlântica Entre o Normativo e o Funcional
	2	Os Casos do Kosovo e do Iraque na Política Externa de Tony Blair
	1	O Crime Organizado Transnacional na Europa: Origens, Práticas e Consequências

idn cadernos

IX SEMINÁRIO IDN JOVEM

PORTO, 8 E 9 DE ABRIL DE 2025

idn Instituto da Defesa Nacional

ISSN 1647-9068
00058
9 771647 906000