idn cadernos

VII SEMINÁRIO IDN JOVEM

JOANA FILIPA CARDOSO FERNANDES, PATRÍCIA ALEXANDRA GONÇALVES NÉVOA, RAQUEL FERREIRA CAMPOS, SÓNIA FILIPA SILVA SOARES, FRANCISCA MARTINS REINA, ANA RAQUEL ALMEIDA DIAS, CONSTANÇA JOSÉ ALMEIDA DE QUEIRÓS, HUGO ALVES QUARTEU, JOANA PEREIRA PIRES, MARIA FRANCISCA VELOSO VOLTA, ANABELA PAULA BRÍZIDO, VITÓRIA SIGAREVA

COVILHÃ, 6 E 7 DE DEZEMBRO DE 2022

idn Instituto da Defesa Nacional

Junho
2023
Nº 49

VII Seminário IDN Jovem

Moderadores:

Professora Doutora Maria Francisca Saraiva
Professor Doutor Bruno Ferreira Costa
Professor Doutor Pedro Silveira
Professora Doutora Liliana Reis Ferreira

Painéis:

Segurança Humana, Direitos Humanos e Defesa
Ameaças e Riscos
Defesa Nacional: Contextos, Políticas e Atores
Transformação Digital e Novas Tecnologias Militares

Covilhã, 6 e 7 de dezembro de 2022

Instituto da Defesa Nacional e
Universidade da Beira Interior

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
António Baranita

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

Composição, Impressão e Distribuição
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
ISBN: 978-972-27-1994-0
Depósito Legal 344513/12

Preâmbulo

Concluída com sucesso a 7ª edição do Seminário IDN Jovem, realizado na Universidade da Beira Interior entre 6 e 7 de dezembro de 2022, publica o Instituto da Defesa Nacional (IDN) mais um número especial do IDN Cadernos, reunindo alguns dos trabalhos considerados para a presente edição.

A publicação reúne seis dos onze textos apresentados pelos estudantes universitários/as provenientes de todo o país e de diversas áreas científicas, que apresentaram comunicações organizadas em seis painéis distintos, designadamente: Ameaças e Riscos; Defesa Nacional; Contextos, Políticas e Atores; Segurança Humana, Direitos Humanos e Defesa; Transformação Digital e Novas Tecnologias Militares.

O Seminário IDN Jovem é uma organização conjunta do IDN e dos Núcleos de Estudantes de Ciência Política e Relações Internacionais de universidades de todo o país, com o objetivo de proporcionar aos estudantes de licenciatura, pós-graduação, mestrado e doutoramento, um espaço de apresentação pública das suas reflexões e de debate sobre temáticas relacionadas com a segurança e defesa.

Para o sucesso desta iniciativa tem contribuído o decisivo apoio dos dirigentes e professores das universidades envolvidas, assim como das direções dos Núcleos de Estudantes de Relações Internacionais e de Ciência Política. Com esta atividade, o IDN procura fomentar o conhecimento e a investigação científica, promover a difusão de uma cultura alargada de segurança e defesa e incentivar a cooperação com instituições de ensino superior. Nesse sentido, este IDN Cadernos reflete o trabalho desenvolvido pelos estudantes cujo mérito resulta na publicação dos seus ensaios.

Por fim, gostaria de deixar uma nota de agradecimento a todas as entidades pela forma entusiástica como se envolveram em mais esta iniciativa dos Seminários IDN Jovem, a que se pretende dar continuidade para materializar esta importante missão do IDN, a de sensibilizar os jovens para os assuntos da segurança e defesa.

Isabel Ferreira Nunes

Índice

idn Instituto da Defesa Nacional

VII Seminário IDN Jovem

Covilhã, 6 e 7 de dezembro de 2022

Temas

- Ameaças e riscos
- Defesa Nacional: Contextos, Políticas e Atores
- Segurança Humana, Direitos Humanos e Defesa
- Transformação digital e novas tecnologias militares

UNIVERSIDADE BEIRA INTERIOR

Papers do "VII Seminário IDN Jovem"

Painel "Segurança Humana, Direitos Humanos e Defesa"

06 de dezembro, 11h15 às 12h30

Keynote Speaker & Comentadora

Professora Doutora Maria Francisca Saraiva

É desde 1995 docente do ISCSP da Universidade de Lisboa, onde exerce funções como Professora Auxiliar. É licenciada (1994) e mestre (1999) em Relações Internacionais pelo ISCSP, e Doutora em Ciências Sociais, na especialidade de Relações Internacionais (2009) pelo mesmo Instituto. Colabora como investigadora no Centro de Administração e Políticas Públicas (CAPP) do ISCSP, no Instituto da Defesa Nacional e no Centro de Investigação e Desenvolvimento do Instituto Universitário Militar (CIDIUM). Suas áreas de especialização são as Nações Unidas e o uso da força, resolução de conflitos, organizações de segurança e defesa, políticas públicas de segurança, controlo de armamentos, direitos humanos e justiça penal internacional.

Oradores

Lucie Calléja	Doutoramento em Relações Internacionais | Universidade Católica Portuguesa
Joana Filipa Fernandes	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Patrícia Névoa	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Raquel Campos	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Sónia Soares	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Francisca Reina	Mestrado em Estudos Internacionais | 2º ano | ISCTE - IUL
Victor Cioffi	Licenciatura em Relações Internacionais | 3º ano | Universidade Portucalense
Ema Sofia da Silva	Licenciatura em Relações Internacionais | 3º ano | Universidade Portucalense

Paper 1:

The Power of Grassroots Women in Building Peace: An analysis of Liberia

Lucie Calléja

Resumo

Entre 1989 e 2003, a Libéria sofreu por duas guerras civis que provocaram perdidas humanas e matérias significantes. As mulheres e crianças foram alvos de recrutamento pelas partes armadas e as estimações mostram que perto de 40,000 mulheres foram violadas e 2,000,000 pessoas foram deslocadas (United Nations, 2014). Este contexto de terror impulsou a necessidade de construir paz na região através da inclusão de todas as vozes. Ao mesmo tempo, as normas nacionais e internacionais sobre os direitos das mulheres em contextos de conflito e pós-conflito aumentaram, tal como a adoção da Resolução 1325 do Conselho de Segurança das Nações Unidas (UNSCR 1325) em 2000. Contudo, o progresso sobre a participação das mulheres nos processos de paz está fragilizado por vários obstáculos. Esta investigação analisa o papel das mulheres no processo de peacebuilding na Libéria, desde os esforços que permitiram a conclusão dos acordos de paz até as iniciativas desenvolvidas no período de reconstrução pós-conflito. Este ensaio salienta a importância dos atores grassroots para desenvolver uma paz inclusiva e sustentável, ilustrada pelo caso do Women in Peacebuilding Network (WIPNET) na Libéria.

Sobre a autora

Lucie Calléja

Lucie Calléja é investigadora de doutoramento no Instituto de Estudos Políticos da Universidade Católica Portuguesa (IEP-UCP) e bolseira de investigação pela Fundação para a Ciência e a Tecnologia (FCT) desde outubro 2021. Completou a sua licenciatura em Ciências Políticas na Université Lumière Lyon II (France) em 2015 e concluiu o seu Mestrado em 'Governance Leadership and Democracy Studies' no IEP-UCP em 2017. Tem interesse no estudo da sociedade civil e processos de paz (peacebuilding) e está a desenvolver a sua investigação na área da participação das mulheres ao nível local e nas iniciativas 'grassroots' para uma construção sustentável da paz.

Paper 2:

A violação dos Direitos Humanos na Prisão de Guantánamo: Terrorismo de Estado vs. Segurança Humana

Joana Filipa Fernandes | Patrícia Névoa | Raquel Campos | Sónia Soares

Resumo

A Guerra ao Terror foi a agenda norte-americana que abriu um precedente para a forma como os reclusos da prisão de Guantánamo foram tratados, sendo considerados, sob a perspetiva dos EUA como “combatentes inimigos ilegais”. O principal objetivo deste paper prende-se com uma análise da presença de terrorismo de estado na Prisão de Guantánamo, consistindo numa violação dos direitos humanos, sob a lente da Segurança Humana. Para esse fim, foi elaborada a seguinte pergunta de investigação que servirá de auxílio para conduzir a investigação: De que forma o terrorismo de Estado na prisão de Guantánamo constituiu uma violação dos direitos humanos? Foi ainda elaborada uma delimitação temporal com início em 2002, após a criação da prisão, e cujo término será em 2022 para que seja possível fazer um paralelo com a atualidade do status deste estabelecimento prisional.

Palavras-chave: Direitos Humanos; EUA, Prisão de Guantánamo; Segurança Humana; Terrorismo de Estado.

Sobre as autoras

Joana Filipa Cardoso Fernandes

23 anos, natural de Vila Nova de Famalicão. Licenciada em Gestão de Atividades Turísticas pelo Instituto Politécnico do Cávado e do Ave. Recebeu em abril de 2022, o certificado de Líder dos Direitos Humanos após participar no Youth Summit de Direitos Humanos em Istambul, com bolsa completa por parte do United States Institute of Diplomacy and Human Rights. Atualmente frequenta o 2º ano do Mestrado em Relações Internacionais na Universidade do Minho e está a desenvolver a sua dissertação no âmbito dos Estudos Migratórios na União Europeia e de Direitos Humanos.

Patrícia Alexandra Gonçalves Névoa

22 anos, natural de Braga. Licenciada em Relações Internacionais pela Universidade do Minho. Atualmente a frequentar o 2.º ano do Mestrado em Relações Internacionais na Universidade do Minho e a desenvolver a dissertação no âmbito dos estudos de segurança e vigilância. Proficiência em Inglês pelo Instituto Britânico de Braga. A frequentar o nível B1 em Alemão no Instituto Britânico de Braga.

Raquel Ferreira Campos

23 anos, natural de Vila Nova de Famalicão. Licenciada em Relações Internacionais pela Universidade do Minho. Realizou o último semestre da licenciatura na Universidade Vytautas Magnus na Lituânia no âmbito do programa Erasmus+. Atualmente a frequentar o 2º ano do mestrado em Relações Internacionais na Universidade do Minho e a desenvolver a dissertação de mestrado no âmbito dos estudos do terrorismo e cooperação internacional, com ênfase no Médio Oriente. Recentemente iniciou a aprendizagem da língua Árabe na Faculdade de Letras da Universidade do Porto.

Sónia Filipa Silva Soares

22 anos, natural de Vila Nova de Gaia. Licenciada em Ciência Política pela Universidade do Minho; Experiência na maior organização de liderança jovem (AIESEC in UMinho), onde alcançou o cargo de Diretora de Recursos Humanos. Experiência enquanto promotora de ONGs na empresa Yupi! It’s possible. Atualmente a frequentar o 2º ano do Mestrado em Relações Internacionais na Universidade do Minho e está a desenvolver a dissertação no âmbito dos estudos de Humanitarismo e Segurança Humana.

Paper 3:

Gendering Global Actorness: Uma Análise Crítica da Implementação da Resolução 1325 na União Europeia

Francisca Reina

Resumo

Na sequência da Resolução 1325 (2000) das Nações Unidas sobre Mulheres, Paz e Segurança (MPS), que apelou aos Estados para integrarem uma perspetiva de género nas suas políticas de segurança e construção da paz, a União Europeia (UE) tem dados alguns passos no sentido de integrar as questões de género na sua política externa e de segurança. Apesar destes desenvolvimentos empíricos, a literatura sobre segurança no espaço europeu não tem prestado a atenção devida aos processos através dos quais as questões de género e a agenda MPS podem contribuir para a construção da UE como um ator global. Este artigo procura aprofundar o debate sobre global actorness numa perspetiva de género, tendo em conta as seguintes questões: (1) que dimensões são relevantes para conceptualizar a UE como um actor global? (2) como é que a igualdade de género e a agenda MPS estão integradas na política externa e de segurança da UE? (3) como é que a UE moldou e promoveu a agenda MPS na arena global? Para responder a estas questões, partimos do modelo conceptual de global actorness de Bretherton e Vogler (2006) e na literatura sobre as dimensões de género da política externa e de segurança da União Europeia.

Sobre a autora

Francisca Reina

Francisca Reina é estudante de mestrado em Estudos Internacionais no ISCTE-IUL. A sua investigação explora as tensões entre o discurso global sobre Mulheres, Paz e Segurança (MPS) e o contexto local dos movimentos de mulheres na Palestina. Concluiu uma licenciatura em Ciência Política e Relações Internacionais na Universidade Nova de Lisboa (2018-2021) e colaborou com o Observatório das Desigualdades (CIES-ISCTE) como estagiária de investigação (2021). Atualmente é estagiária no Instituto de Defesa Nacional (IDN), onde assiste na investigação sobre MPS, género e defesa. Os seus interesses de investigação centram-se nos estudos de segurança feministas, estudos críticos da paz, e movimentos de mulheres no Médio Oriente.

Paper 4:

Consistência ou hipocrisia? A posição de Portugal perante a securitização das migrações na União Europeia sob a ótica Construtivista, 2015-2019

Ema Sofia da Silva | Victor Cioffi

Resumo

A ação da União Europeia em matéria da chamada “crise” dos refugiados em 2015, tanto por meios jurídicos, como por meios discursivos, apresentou sinais de incoerência e hipocrisia. Pretendemos com este trabalho analisar, sob uma ótica construtivista das Relações Internacionais, o posicionamento de Portugal em relação às políticas migratórias impostas pela União e procurar compreender de que forma o país se assemelha ou se distancia do resto dos países membros e da União Europeia como instituição. Discutimos elementos essenciais para o entendimento do tema, como as jurisdições regentes e os discursos proferidos, a fim de poder concluir se Portugal apresenta um comportamento consistente ou hipócrita tal qual outros membros da União.

Palavras-chave: Discurso; Refugiados; Portugal; Relações Internacionais; União Europeia.

Sobre os autores

Ema Sofia Pinto da Silva

Ema Sofia (1999) atualmente frequenta o último ano da Licenciatura em Relações Internacionais com Especialização em Diplomacia e Estudos da Área. Anteriormente frequentou a licenciatura de Administração Público-Privada na faculdade de Direito de Coimbra. Publicações relevantes: Sleep Habits during COVID-19 Confinement: An Exploratory Analysis from Portugal; MDPI.

Victor Cioffi Netto Silva

Victor Cioffi (2001) é luso-brasileiro e frequenta o último ano da Licenciatura em Relações Internacionais com Especialização em Diplomacia e Estudos da Área. Possui diploma técnico em Comércio Exterior, curso no qual foi premiado pela Escola Superior de Publicidade e Marketing de São Paulo.

Painel "Ameaças e Riscos"

06 de dezembro, 14h às 15h30

Comentador

Professor Doutor Bruno Ferreira Costa

Doutorado em Ciências Sociais, na especialidade em Ciência Política pelo Instituto Superior de Ciências Sociais e Políticas (ULisboa). É mestre (2009) e licenciado (2006) em Ciência Política pelo mesmo instituto. Professor Auxiliar da Universidade da Beira Interior e Investigador do Praxis - Centro de Filosofia, Política e Cultura. Os principais interesses e publicações incidem sobre a temática dos sistemas políticos, participação política e qualidade da democracia, comunicação política e União Europeia.

Oradores

Ana Raquel Almeida Dias	Doutoramento em Ciência Política e Relações Internacionais | Universidade do Minho
Ivan Chacon	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Pedro Corceiro	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Ana Jacinta Sampaio	Mestrado em Direito da União Europeia | 1º ano | Universidade do Minho
Alona Bondarenko	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Joana Machado Marcos	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
José António Pereira	Mestrado em Relações Internacionais | 2º ano | Universidade do Minho
Vitaliy Venislavskyy	Mestrado em História Militar | 2º ano | Universidade de Lisboa
Laura Semblano Teixeira	Pós-Graduação em Direito Internacional Humanitário e Direitos Humanos em Situações de Conflito | Universidade de Lisboa
Ricardo Pereira	Mestrado em Ciência Política | 1º ano | Universidade de Aveiro

Paper 5:

Climate Security and Security Governance beyond the Central State: Moving the Debate Forward

Ana Raquel Almeida Dias

Resumo

Improvement of security governance on climate security is critical if fast-paced threats caused by the emission of greenhouse gases are to be dealt with. This article envisions climate security as a global public good, moving the debate beyond traditional security discussions and refocusing attention upon climate security governance for its effective provision. Additionally, having in mind the recognition granted to sub-state authorities under the Paris Agreement, it suggests that the provision of security governance in matters of climate change requires a multilevel governance (MLG) approach whereby sub-state actors become inescapable agents of climate security governance. In doing so, it is our wish to move the debate forward in two complementary ways: first, by expanding the notion of security in order to perceive climate security as a global public good and second, by shedding light on the reinforced role of sub-state authorities under the Paris agreement using the framework of MLG.

Palavras-chave: climate change; climate security; security governance; multilevel governance.

Sobre a autora

Ana Raquel Almeida Dias

Ana Raquel Dias é Doutoranda em Ciência Política e Relações Internacionais na Universidade do Minho. É Mestre em Ciência Política e licenciou-se em Relações Internacionais, ambos pela Universidade do Minho. Atualmente é bolseira da Fundação para a Ciência e Tecnologia (FCT) com o seu projeto de investigação focado nas dinâmicas de governação global (Global Governance), mais particularmente, o surgimento da ação climática subestadual sob o Acordo de Paris.

Paper 6:

O Crime Organizado Transnacional na Europa: a Ação da Europol e dos Estados-Membros perante a ‘Ndrangheta Calabresa

Ivan Chacon | Pedro Corceiro

Resumo

Este trabalho aborda a presença do crime organizado transnacional (COT) e os mecanismos de cooperação policial no contexto da União Europeia. Para a definição do estudo de caso, foi escolhida a ‘Ndrangheta calabresa, pelas suas especificidades de afirmação transnacional e pelo seu peso significativo nos efeitos nefastos do COT, nomeadamente no que respeita àquele de origem italiana. Os dois quadros teóricos escolhidos são a Teoria da Securitização e o Neoliberalismo. A primeira parte visa explicar brevemente ambas estas teorias, bem como alguns conceitos estruturantes, tendo em conta definições institucionais e académicas. A segunda parte consiste numa explicação do estudo de caso, olhando às suas várias componentes: Europol e ‘Ndrangheta, bem como quatro operações da Europol em conjunto com vários Estados-membros especificamente contra a ‘Ndrangheta. A terceira parte aplica os quadros teóricos mencionados ao estudo de caso, a que se seguem as conclusões obtidas.

Palavras-chave: ‘Ndrangheta; Crime organizado transnacional; Europol; Neoliberalismo; Teoria da Securitização.

Sobre os autores

Ivan Chacon

Nascido em 1998 no Estado de Roraima no Brasil. Iniciou o curso de Relações Internacionais na Universidade Federal de Roraima em 2016 e depois iniciou o curso de Ciência Política e Relações Internacionais pela Universidade da Beira Interior em 2018, se formando em 2021 pela mesma. Atualmente cursando Mestrado em Relações Internacionais pela Universidade do Minho.

Pedro Corceiro

Natural de Aveiro e Licenciado em Línguas e Relações Internacionais pela Faculdade de Letras da Universidade do Porto, onde, em termos linguísticos, se focou no Alemão e no Inglês. Atualmente a concluir o Mestrado em Relações Internacionais pela Escola de Economia e Gestão da Universidade do Minho, com uma dissertação incidindo na análise do cruzamento do crime organizado transnacional com a cibercriminalidade e da abordagem securitária da União Europeia em relação a essa questão.

Paper 7:

A escola intergovernamental liberal e o Brexit – efeito dominó?

Ana Jacinta Sampaio

Resumo

Nesta composição serão abordadas evidências teóricas, tendo como base estrutural a teoria intergovernamental liberal de Andrew Moravcsik, que, juntamente com pertinentes contextualizações sobre a geopolítica europeia, irá aspirar a responder ao conflito relacionado – e provocado – pelo Brexit. Para além de explanar as principais razões que causaram a mais recente mudança na União Europeia, este trabalho propor-se-á a antever um possível futuro para a UE, de modo a evidenciar se o caso do Reino Unido foi um acontecimento histórico único e isolado ou se, à saída, no meio de tamanha complicação burocrática, deixou a porta aberta como exemplo.

Palavras-chave: Teoria intergovernamental liberal; Geopolítica europeia; Brexit; Reino Unido.

Sobre a autora

Ana Jacinta Sampaio

Ana Jacinta Sampaio é, atualmente, estudante do 1º ano do Mestrado em Direito da União Europeia pela Universidade do Minho. Também em terras minhotas, finalizou a licenciatura em Ciência Política, onde, juntamente com a aprendizagem decorrente do âmbito associativo e político, fomentou o seu interesse no campo da geopolítica europeia, no exercício de poder, na problemática dos refugiados e a Europa, assim como no binómio da Europa e Cidadania e Europa e Soberania. Resultante da experiência enquanto Presidente do Núcleo de Estudantes de Ciência Política da Universidade do Minho, estagiária do Observatório do Mundo Islâmico, e, atualmente, estagiária no Instituto de Defesa Nacional (IDN) o seu principal foco passa pela intenção de conciliar o estudo das ideologias políticas contemporâneas, das relações entre os Estados e os seus cidadãos, do panorama europeu, e do Estado de Direito.

Paper 8:

A presença da OTAN no Mar Egeu no contexto da crise migratória

Alona Bondarenko | Joana Machado Marcos | José António Pereira

Resumo

Em 2015, a UE deparou-se com uma crise migratória que se apresentou como um momento complexo e desafiador. Este contexto pôs em evidência a necessidade de uma cooperação entre a OTAN e a Frontex, com a finalidade de responder de uma forma coesa e atempada aos fluxos de refugiados e migrantes. Com o entender da natureza da OTAN e tendo esta uma força de reação permanente no mar – o SNMG2, era de todo pertinente e aconselhável empenhá-lo no Mar Egeu, uma vez que, pela geografia, era um dos centros da transição migratória, classificada na sua maioria como ilegal. O envolvimento da OTAN na gestão crise migratória no Mar Egeu, no contexto da cooperação com a Frontex, foi bem-sucedido e tornou-se fundamental não só na segurança europeia, com uma diminuição significativa dos fluxos migratórios, como a nível do Direito Internacional, sendo a OTAN um intermediário entre a UE e a Turquia.

Palavras-chave: crise migratória; Frontex; Mar Egeu; OTAN; segurança; UE.

Sobre os autores

Alona Bondarenko

Mestranda em Relações Internacionais (2º ano) na Escola de Economia e Gestão da Universidade do Minho (UMinho). Licenciada em Ciência Política e Relações Internacionais pela Universidade da Beira Interior (UBI). Coautora do capítulo de livro “The Integration of the Eastern and Western Balkans into the EU and NATO: A Longitudinal and Integrated Analysis” em “Challenges and Barriers to the European Union Expansion to the Balkan Region”, editado por Bruno Ferreira Costa e publicado em janeiro de 2022 pelo IGI Global Publisher (Hershey, Pennsylvania, USA). É membro do Council for European Studies (Columbia University, USA).

Joana Machado Marcos

Mestranda em Relações Internacionais (2ºano) na Escola de Economia e Gestão da Universidade do Minho. Licenciada em Ciência Política e Relações Internacionais pela Universidade da Beira Interior. Estagiária durante 3 meses no Estado Maior da Armada, na secção das Relações Externas da Marinha Portuguesa.

José António Pereira

Mestrando em Relações Internacionais (2º ano) na Escola de Economia e Gestão da Universidade do Minho. Licenciado em Ciências da Comunicação, na Faculdade de Letras da Universidade do Porto. Jornalista da RTP desde julho de 2015. Professor Assistente Convidado da Universidade da Beira Interior, onde dá aulas de Jornalismo.

Paper 9:

A Marinha Portuguesa e a Política Externa de Portugal
Uma aproximação ao Atlântico que complementa os compromissos europeus

Vitaliy Venislavskyy

Resumo

Numa altura em que a Europa procura responder à maior ameaça securitária desde a sua criação, Portugal está num processo de definição do novo Conceito Estratégico de Defesa Nacional. Neste ensaio, é defendida uma aproximação diplomática portuguesa do Atlântico, nomeadamente à luz da sua crescente importância no comércio internacional e, por isso, na geopolítica internacional. Através de uma imersão histórica na Estratégia Nacional, desde a criação de Portugal até à atualidade, defende-se a ideia da criação de uma estratégia global de Portugal, inserida no quadro institucional em que Portugal está inserido. Esse ponto é reforçado com uma reflexão sobre as possibilidades e o papel que a Marinha Portuguesa e as Forças Armadas, enquanto instrumento de Política Externa, terão para Portugal cumprir o seu objetivo primário nas Relações Internacionais – o estabelecimento de um parceiro credível e produtor líquido de segurança internacional.

Palavras-chave: Discurso; Portugal, Marinha, Estratégia, Defesa Nacional, Atlântico.

Sobre o autor

Vitaliy Venislavskyy

Licenciado em Relações Internacionais pela Faculdade de Economia da Universidade de Coimbra e mestrando em História Militar pela Faculdade de Letras da Universidade de Lisboa. As áreas de interesse são o estudo e investigação na matéria de Segurança e Defesa Nacional e Europeia, com especial ênfase na Europa de Leste, e no espaço pós Soviético. Com participação em diferentes ambientes e contextos de debate académico sobre a matéria da Segurança Europeia, no contexto da Guerra da Ucrânia. Membro da Direção da EuroDefense Jovem Portugal.

Paper 10:

A NATO e a Securitização Coletiva da COVID-19: a análise do discurso da construção da ameaça (fevereiro-maio 2020)

Laura Semblano Teixeira | Ricardo Pereira

Resumo

O presente artigo pretende analisar como o discurso da NATO, compreendido entre fevereiro e maio de 2020, construiu a COVID-19 como uma ameaça existencial através da Securitização Coletiva. A relevância deste estudo prende-se com a necessidade de entender como a NATO aproveitou esta janela de oportunidade para demonstrar a sua resiliência e justificar a sua necessidade face ao ceticismo criado. Para tal, recorreu-se à teoria da Securitização Coletiva e à análise de discurso para trabalhar sobre uma seleção de declarações da organização. Através destes é possível observar uma tentativa de alargamento, que já vinha a ser trabalhada, sobre questões tradicionalmente não ligadas à realpolitik, como a saúde e o ambiente, que culminam em ações como coordenação de missões de resgate de civis e o uso de meios científicos para responder ao vírus SARS-CoV-2.

Palavras-chave: NATO, COVID-19, securitização coletiva, análise de discurso.

Sobre os autores

Laura Semblano Teixeira

Laura Semblano é licenciada em Relações Internacionais pela Universidade do Minho, tendo exercido a função de dirigente associativa enquanto Presidente do Centro de Estudos do Curso de Relações Internacionais. Atualmente, frequenta o Curso de Pós-Graduação em Direito Internacional Humanitário e Direitos Humanos em Situações de Conflito, realizado pelo Instituto Europeu da Faculdade de Direito da Universidade de Lisboa, em parceria com o IDN e o ICJP. É, também, ativista no coletivo Humans Before Borders (HuBB).

Ricardo Magalhães Pereira

Ricardo Pereira, Mestre em Relações Internacionais pela Universidade do Minho, licenciado em RI pela mesma universidade, atualmente está a frequentar o Mestrado em Ciência Política na Universidade de Aveiro. No seu percurso académico conta com participações em conferências nacionais e internacionais como o IDN Jovem, Lisbon Arctic International Conference and Workshop e o VI CIED. No presente ano é detentor de uma bolsa de investigação, estando a trabalhar como research assistant no CICP, na Universidade do Minho. Anteriormente, participou no projeto europeu EXCEPTIUS, como data Coder para Portugal.

Painel “Defesa Nacional: Contextos, Políticas e Atores”

06 de dezembro, 15h35 às 17h15

Comentador

Professor Doutor Pedro Silveira

Professor Auxiliar da Universidade da Beira Interior e investigador do Praxis-UBI e do IPRI-NOVA. Licenciado em Direito (2008) pela Universidade do Lisboa e em Ciência Política e Relações Internacionais (2012) pela Universidade Nova de Lisboa. É Mestre em Ciência Política e Relações Internacionais (2013) e Doutor em Ciência Política (2019) pela FCSH-UNL. Os seus interesses de investigação incluem as elites políticas, o governo e a liderança política.

Oradores

Constança Magalhães	Licenciatura em Línguas e Relações Internacionais | 3º ano | Universidade do Porto
Hugo Quarteu	Licenciatura em Línguas e Relações Internacionais | 3º ano | Universidade do Porto
Joana Pires	Licenciatura em Línguas e Relações Internacionais | 3º ano | Universidade do Porto
Maria Francisca Volta	Licenciatura em Línguas e Relações Internacionais | 3º ano | Universidade do Porto
Bárbara Monteiro	Mestre em Relações Internacionais | Universidade Nova de Lisboa
Mário Santos	Pós-graduação em Globalização, Diplomacia e Segurança | Universidade Nova de Lisboa e Instituto Universitário Militar
Gonçalo Margato	Mestrado em História Moderna e Contemporânea | 1º ano | ISCTE-IUL
Afonso Torres	Mestrado em Ciência Política | 1º ano | Universidade de Aveiro
Gonçalo Oliveira	Mestrado em Ciência Política e Relações Internacionais | 2º ano | Universidade Nova de Lisboa
Leandro Breia	Licenciatura em Ciência Política e Relações Internacionais | 3º ano | UBI
Andreia Pinho	Licenciatura em Ciência Política e Relações Internacionais | 3º ano | UBI
Carla Leal	Licenciatura em Ciência Política e Relações Internacionais | 3º ano | UBI
Gabriela Mota	Licenciatura em Ciência Política e Relações Internacionais | 3º ano | UBI

Paper 11:

As Alterações Climáticas e a Defesa Nacional

Constança Magalhães | Hugo Quarteu | Joana Pires | Maria Francisca Volta

Resumo

As alterações climáticas são a grande ameaça às gerações vindouras a nível mundial. Portugal não é exceção: as particularidades geográficas, num cenário de crise, representam um risco de defesa nacional e de segurança. Neste sentido, procura-se indicar qual o plano de ação que o governo português – e europeu, uma vez que, sendo Portugal um Estado-membro, é impossível não mencionar a legislação europeia – têm vindo a traçar no sentido de combater a emergência ambiental através dos mecanismos da defesa nacional e/ou europeia.

Assim, na prossecução desse objetivo analisam-se briefs recentemente publicados pelo IDN que relacionam as duas realidades, alterações à legislação ambiental, vários planos de ação da organização supranacional, iniciativas em território português – e ibérico – e resultados até agora obtidos. Por fim, abordam-se ainda propostas de apoio a um modo de vida mais verde: a criação de um exército pacífico europeu, aposta na ferrovia lusa e alterações à indústria pecuária.

Sobre os autores

Constança José Almeida de Queirós e Gonçalves de Magalhães

Natural de Marco de Canaveses, tem 20 anos e atualmente é estudante do 3º ano de Línguas e Relações Internacionais na Faculdade de Letras da Universidade do Porto.

Hugo Alves Quarteu

Natural de Bragança, tem 19 anos e atualmente é estudante do 3º ano de Línguas e Relações Internacionais na Faculdade de Letras da Universidade do Porto.

Joana Pereira Pires

Natural de Cerdedo, concelho de Boticas, tem 20 anos e atualmente é estudante do 3º ano de Línguas e Relações Internacionais na Faculdade de Letras da Universidade do Porto.

Maria Francisca Veloso Volta

Natural de Vitória, concelho do Porto, tem 20 anos e atualmente é estudante do 3º ano de Línguas e Relações Internacionais na Faculdade de Letras da Universidade do Porto.

Paper 12:

A Defesa Nacional e as relações internacionais: a construção de um mapa concetual

Bárbara Monteiro

Resumo

A idealização de um mapa concetual que permita justificar as premissas que constituem a elaboração da defesa nacional de um Estado e o conceito estratégico a si associado deve ser feito à luz das teorias das relações internacionais.

Nesse sentido, a abordagem teórica de Alexander Wendt parece revelar-se como a mais adequada, uma vez que analisa conceitoschave que auxiliam na sua construção.

A importância dos atores, no que toca à defesa dos seus interesses e assegurando a sua identidade perante os outros, quer a nível doméstico quer a nível internacional, os contextos que influenciam diretamente a forma como são percecionadas as ameaças e as políticas que são desenvolvidas como resposta à dinâmica do sistema internacional, com a formação de alianças são aspetos que têm um impacto imediato na formulação de uma defesa nacional e constituem-na como parte integrante do comportamento dos Estados na ordem internacional.

Palavras-chave: Construtivismo, defesa nacional, contextos, Médio Oriente, Israel

Sobre a autora

Bárbara Monteiro

Bárbara Monteiro é licenciada em Filosofia e também em Ciência Política e Relações Internacionais na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa, onde fez também o Mestrado de Relações Internacionais.

Paper 13:

Tão Perto, Mas Tão Longe – A Importância do Magrebe para a Segurança Nacional Portuguesa

Gonçalo Margato | Mário Santos

Resumo

No contexto da lógica da segurança e defesa de Portugal, qual o papel desempenhado pelo Magrebe? O presente artigo pretende, a partir de uma análise da região, pensar os principais riscos securitários que o Magrebe representa para Portugal, partindo de uma abordagem estatocêntrica. Sustentamos que a instabilidade da região é um vetor de extrema importância para a avaliação da segurança portuguesa, analisando várias dessas dimensões.

Sobre os autores

Gonçalo Margato

Gonçalo Margato é mestrando em História Moderna e Contemporânea no ISCTE-IUL e bolseiro de investigação no projeto «ARCHWAR - Controle e violência através da habitação e da arquitetura, durante as guerras coloniais» do DINAMIA'CET-ISCTE. Licenciou-se em Ciência Política e Relações Internacionais pela NOVA-FCSH e ganhou o Prémio de Ensaio «25 de abril» do Instituto Português de Relações Internacionais e do Departamento de Estudos Políticos da NOVA-FCSH.

Mário Santos

Mário Alexandre Leiria dos Santos é licenciado em Ciência Política e Relações Internacionais pela Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa. Frequenta a Pós-Graduação em Globalização, Diplomacia e Segurança na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa em colaboração com o Instituto Universitário Militar.

Paper 14:

Política Externa e Defesa Nacional
Os três vetores essenciais da política externa portuguesa revisitados

Afonso Torres

Resumo

A política externa portuguesa tem-se, ao longo dos últimos 200 anos, mantido fiel aqueles que são os seus três vetores essenciais: o Atlântico, o Europeu e o Colonial/Lusófono. O desafio tem sido o de navegar entre as exigências de cada um destes vetores e a opção de um em detrimento de outro, quando em conflito. A viragem para o século XXI e os desenvolvimentos no espaço europeu, ocorridos nesta segunda década, trazem novos desafios para Portugal e requerem um novo diálogo estratégico e um repensar da abordagem portuguesa no sistema internacional. Esta exposição propõe-se precisamente a contribuir para o reacender deste debate, explorando as necessidades estratégicas de cada um destes três vetores e avaliando o equilíbrio possível e necessário entre eles.

Sobre o autor

Afonso Soares da Costa Vilar Torres

Afonso Soares da Costa Vilar Torres nasceu em outubro de 2002 em Lisboa, onde reside. Terminou o Ensino Secundário no ano de 2020, no Colégio de Santa Doroteia. Atualmente frequenta o 3.º ano da Licenciatura em Ciência Política e Relações Internacionais na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa.

Paper 15:

A Diplomacia de um (não tão) Pequeno Estado: O caso de Portugal

Gonçalo Oliveira

Resumo

Portugal, ao longo da sua história, deteve diferentes classificações em termos das suas capacidades enquanto potência. No entanto, após a perda da independência em 1580, e particularmente após a independência do Brasil, houve um declínio acentuado que culminou na sua classificação enquanto pequena potência, categoria na qual ainda agora se insere. Apesar de esta avaliação ser correta e inescapável por todas as métricas habitualmente utilizadas, o que encontramos é que a diplomacia portuguesa, no seu alcance e escopo, vai além das capacidades de uma pequena potência. O presente artigo pretende expandir e problematizar o estudo da diplomacia portuguesa, assim indicando as áreas em que Portugal se destaca dos restantes pequenos estados.

Palavras-chave: Portugal, diplomacia, diplomacia cultural, soft power, lusofonia.

Sobre o autor

Gonçalo Jorge Mata de Oliveira

Licenciado em Línguas, Literaturas e Culturas – Estudos Ingleses e Norte Americanos. Mestrando em Ciência Política e Relações Internacionais pela Universidade Nova de Lisboa – Faculdade de Ciências Sociais e Humanas, estando neste momento a desenvolver uma dissertação intitulada “Europa em Crise – Mapeamento do Discurso Eurocético na Europa do Sul”. As principais áreas de interesse são Estudos Europeus, Euroceticismo, Análise Discursiva, Política Externa Portuguesa e Identidade.

Paper 16:

Política Energética em Portugal

Andreia Pinho | Carla Leal | Gabriela Mota | Leandro Breia

Resumo

O presente trabalho tem como objetivo uma explicação sobre a Política Energética da União Europeia. O nosso projeto começa com uma breve introdução, onde explica de um modo geral a Política energética e o seu enquadramento no Tratado de Funcionamento da União Europeia. Analisamos também a agência que vem materializar a Política, a Agência de Cooperação dos reguladores de Energia (ACRE). Em seguinte, analisamos os vários prepostos defendidos pela Política Energética. A questão da segurança no abastecimento de energia à União Europeia e os benefícios que Portugal ganhará neste sentido. Por último, a aplicabilidade da Política Energética em Portugal.

Palavras-chave: Política Energética, União Europeia, Portugal, Segurança Energética.

Sobre os autores

Andreia Pinho

Andreia Pinho tem 20 anos e atualmente estuda Ciência Política e Relações Internacionais na Universidade da Beira Interior.

Carla Leal

Carla Leal nasceu em 2002 e estuda Ciência Política e Relações Internacionais na Universidade da Beira Interior.

Gabriela Mota

Gabriela Mota tem 20 anos e é natural de Pombal. É aluna do 3º ano da Licenciatura em Ciência Política e Relações Internacionais na Universidade da Beira Interior.

Leandro Breia

Leandro Breia, natural de Castelo Branco, estuda Ciência Política e Relações Internacionais na Universidade da Beira Interior.

Painel "Transformação digital e novas tecnologias militares"

07 de dezembro, 10h00 às 11h15

Comentadora

Professora Doutora Liliana Reis Ferreira

É atualmente Professora Auxiliar Convidada da Universidade da Beira Interior e Investigadora do IPRI-NOVA. Licenciada em Relações Internacionais pela Universidade do Minho, Pós-Graduada em Teoria e Prática Diplomática pela Universidade Lusíada e Pós-Graduada em Segurança e Defesa pelo Instituto de Estudos Políticos da Universidade Católica Portuguesa. É, também, mestre em Relações Internacionais e Ciência Política, pela mesma Universidade, e é doutorada em Ciência Política e Relações Internacionais, pela Universidade do Minho.

Oradores

Anabela Paula Brízido	Doutoramento em Direito | Universidade Nova de Lisboa
Vitória Sigareva	Mestrado em Ciência Política e Relações Internacionais | 2º ano | Universidade Nova de Lisboa
Patrícia Bastos	Mestra do em Ciência Política e Relações Internacionais: Segurança e Defesa | 2º ano | Universidade Católica Portuguesa

Paper 17:

Quando a Ciberconflitualidade Desafia as Regras Cinéticas – As Ciberoperações Militares e a Noção de Ataque Constante no Artigo 49.º do Primeiro Protocolo Adicional às Convenções de Genebra

Anabela Paula Brízido

Resumo

Este artigo analisa a noção de ataque constante do art.º 49.º do I PA às CG e a sua adequabilidade em relação às ciberoperações militares. A metodologia assentou na revisão do estado de arte, no recurso às leis e às regras jurídicas aplicáveis, à jurisprudência, à doutrina e à soft law. Foram analisadas as diferentes correntes doutrinárias (Schmitt, Dörmann e Melzer) e conclui-se que o conceito de hostilidade, embora não seja perfeito, todavia, é o que oferece mais garantias para proteger os civis, população civil e objetos civis.

Palavras-chave: ataques; ciberoperações militares; efeitos cinéticos; hostilidades.

Sobre a autora

Anabela Paula Brízido

Anabela Paula Brízido é doutoranda na NOVA School of Law. A sua dissertação tem como objeto a ciberconflitualidade armada internacional e o fenómeno da privatização da guerra. É investigadora do CEDIS, da NOVA BHRE Centre e é membro da Sociedade Portuguesa de Direito Internacional (SPDI); Competitive Intelligence & Information Warfare Association (CIIWA); Ordem dos Advogados portuguesa. As suas áreas de interesse são o Direito Internacional, Direito Internacional Humanitário, Direito Militar, Direitos Humanos, Direito da Sociedade da Informação, cibercrime, cibersegurança e ciberdefesa. Dá formação em várias áreas do Direito e lecionou, em co-regência, na NOVA School of Law História do Direito, Introdução ao Direito e ao Pensamento Jurídico e Direito das Finanças Públicas. É, ainda, jurista e Presidente da Assembleia Geral da Associação Nacional de Famílias para a Integração da Pessoa Deficiente – AFID.

Paper 18:

Um Olhar Sobre a Cibersegurança em Portugal

Vitória Sigareva

Resumo

No mundo globalizado atual, o ciberespaço apresenta inúmeras oportunidades de cooperação e progresso, as também de ameaças e ataques. A cibersegurança dos Estados pode-se encontrar em risco, na falta de formação pertinente, recursos financeiros ou cooperação eficaz.

O presente trabalho analisa de que maneira Portugal se encontra preparado para enfrentar as ameaças cibernéticas. Para isso, são apresentadas as principais tendências em cibercriminalidade em Portugal e os mecanismos de lidar com os desafios. Sugere-se que os ciberincidentes agravam as vulnerabilidades estatais, criam alguma desconfiança nas instituições nacionais. Porém, simultaneamente, impulsionam os avanços tecnológicos em ciberproteção. As capacidades nacionais estão, por isso, a ser direcionados para a formação tecnológica, a consolidação do corpo jurídico e o desenvolvimento de medidas de proteção, em parcerias regionais e internacionais.

Sobre a autora

Vitória Sigareva

Mestranda em Ciência Política e Relações Internacionais, na Universidade NOVA de Lisboa, com especialização em Relações Internacionais. Estagiária no Ministério dos Negócios Estrangeiros, na DGPEMOM. Vice-Presidente do Escritório Local Lisboa Centro de AIESEC in Portugal, nos mandatos 22-23 e 23-24.

Paper 19:

Transformação digital e novas tecnologias militares: Cibersegurança e ameaças híbridas

Patrícia Bastos

Resumo

Vivemos na era da informação, do conhecimento e da globalização onde tudo depende da internet. O ciberespaço tornou-se um “oásis” para aparecimento de novas ameaças híbridas, as quais vêm representar a nova geração de conflitos do séc. XXI. Ao longo do milénio temos tido provas como um ciberataque tem o poder de paralisar e prejudicar seriamente uma nação causando danos, muitas das vezes, irreversíveis.

Os Estados e as Organizações Internacionais foram confrontados com uma nova realidade para a qual não estavam preparados para lidar, tendo sido obrigados a mudar drasticamente as suas políticas de defesa passando a incluir termos como “cibersegurança” e “ciberdefesa”, os quais não tinham grande enfoque antes do início do milénio.

Revela-se primordial a continuação do desenvolvimento dos trabalhos nestas áreas pois a nossa sociedade será cada vez mais digital no futuro, pelo que urge o respetivo acompanhamento tecnológico dos organismos de defesa.

Sobre a autora

Patrícia Ramos de Carvalho Barros Bastos

Licenciada em Ciência Política e Relações Internacionais pelo Instituto de Estudos Políticos da Universidade Católica Portuguesa. Atual aluna de Mestrado no programa de Ciência Política e Relações Internacionais: Segurança e Defesa no Instituto de Estudos Políticos da Universidade Católica Portuguesa.

Capítulo I

SEGURANÇA HUMANA, DIREITOS HUMANOS E DEFESA

A Violação dos Direitos Humanos na Prisão de Guantánamo: Terrorismo de Estado vs. Segurança Humana

Joana Filipa Cardoso Fernandes
Patrícia Alexandra Gonçalves Névoa
Raquel Ferreira Campos
Sónia Filipa Silva Soares

Introdução

O presente estudo tem como principal objetivo analisar o terrorismo de Estado aplicado à prisão de Guantánamo sob a lente teórica da Segurança Humana. Por essa razão, este *paper* propõe-se responder à seguinte pergunta de investigação como ponto de partida: de que forma o terrorismo de Estado na prisão de Guantánamo constituiu uma violação dos direitos humanos?

Desde a abertura da prisão de Guantánamo, em 2002, são muitos os relatos do contexto de terror que são vividos dentro do estabelecimento prisional, um contexto que perdurou em 2022. Deste modo, este será o nosso período de análise.

Este tema mostra-se relevante para a realidade atual, continuando a causar uma grande contestação entre a comunidade internacional, havendo ainda uma falta de consenso por parte das presidências norte-americanas. Por exemplo, Biden, o vigente presidente dos Estados Unidos da América (EUA) tem realizado esforços para libertar os presos de Guantánamo, contudo não têm sido suficientes para colmatar a situação, como iremos desenvolver durante a investigação. Para além da falta de consenso, ocorrem ainda práticas duvidosas na prisão, onde são postos em causa os direitos humanos. Desta forma, procuramos com este estudo trazer *insights* importantes para a comunidade epistémica.

Além do mais, o interesse deste *paper* prende-se ainda pela novidade científica gerada ao examinar o fenómeno do terrorismo de Estado, que em si viola os direitos humanos pela ótica da Segurança Humana que procura defender os mesmos.

Para a concretização desta pesquisa, foram utilizadas fontes primárias e fontes secundárias, que se revelaram úteis para a complementação da informação obtida, proveniente de uma análise da literatura.

Desta forma, a investigação encontra-se dividida por capítulos e subcapítulos, iniciando-se com um enquadramento teórico-conceptual onde se irá contextualizar em que

consiste a Segurança Humana enquanto teoria que suportará a análise do estudo de caso desenvolvido na investigação e, desta forma, onde expomos também os conceitos necessários para a compreensão da temática. De seguida, irá realizar-se uma contextualização histórica do estudo, de maneira a compreender as motivações que levaram à criação da prisão de Guantánamo. Uma terceira parte aborda o terrorismo de Estado, quando surgiu, em que consiste, e ainda algumas definições do conceito, abrindo depois caminho para um subcapítulo que aplica essa noção aos Estados Unidos da América e outro subcapítulo que se inicia com o objetivo de aplicar o conceito principal à prisão de Guantánamo. Ainda, o quarto capítulo será dedicado à relevância do tema na atualidade, neste caso, em 2022. Por fim, o quadro teórico irá ser aplicado à temática analisando o terrorismo de Estado na prisão de Guantánamo na ótica da Segurança Humana e, de seguida, abordando a questão que se torna pertinente neste caso, a violação dos direitos humanos praticados nesta prisão.

1. Enquadramento Teórico-Conceptual

Neste primeiro capítulo tenciona-se analisar os alicerces teóricos e conceptuais do presente estudo.

O quadro teórico que suportará a análise do caso é a Segurança Humana. Esta escolha foi feita porque a Segurança Humana é uma doutrina que defende a proteção dos direitos humanos em detrimento dos interesses nacionais dos Estados e, portanto, aplica-se a este estudo ao considerar os indivíduos presos em Guantánamo como objetos de segurança com direito a serem tratados com humanidade em vez de impor os interesses dos EUA, algo que irá ser mais desenvolvido no último capítulo desta investigação.

Importa iniciar este enquadramento, explicando como surgiu o conceito de Segurança Humana. O conceito surgiu na década de 1990 quando o fim da Guerra Fria veio alterar o ambiente da segurança internacional (De Lauri, 2020). A Segurança Humana foi conceptualizada, pela primeira vez, no Programa das Nações Unidas para o Desenvolvimento (PNUD) de 1994, quando o Relatório de Desenvolvimento Humano forneceu uma definição ampla do conceito em termos de preocupação com a vida e a dignidade humana em vez de uma preocupação centrada no Estado, na guerra e no setor militar, uma preocupação predominantemente característica dos EUA. Foi através do PNUD, em 1994, que surgiu um novo paradigma de segurança que deixou de ser exclusivamente estatal, passando a incluir no debate da segurança questões como a defesa dos direitos humanos (Warren e Grenfell, 2017). Foi também neste Relatório de Desenvolvimento Humano (1994) que se identificou sete setores de ameaças não tradicionais à segurança das pessoas: segurança alimentar, segurança sanitária, segurança pessoal, segurança comunitária, segurança económica, segurança política e segurança ambiental (PNUD, 1994). Desta forma, a Segurança Humana procurou incluir outras ameaças na agenda da segurança internacional, ameaças essas mais diversas e generalizadas (Nyadera e Bincof, 2019). A Segurança Humana refere-se à segurança geral da pessoa contra todo o tipo de ameaças (Paulussen e Scheinin, 2020).

Os riscos mencionados à segurança dos indivíduos pela Segurança Humana são importantes para reconhecermos os perigos que os presos em Guantánamo se sujeitam, vendo os seus direitos humanos a serem constantemente desrespeitados. Os Estados deveriam entender a segurança para além de termos puramente estatais e militares (Betts e Eagleton-Pierce, 2005); contudo, a resposta dos EUA aos ataques do 11 de Setembro de 2001 através da doutrina "War on Terror" é o exemplo perfeito onde os interesses militares se sobrepuseram a qualquer ameaça à segurança e aos direitos das pessoas. Os Estados falharam muitas vezes na sua obrigação de proteger as pessoas, o que legitima a criação de um novo paradigma de segurança, neste caso, a Segurança Humana.

Esta legitimação do paradigma foi difícil, pois existia algum ceticismo por parte de alguns Estados com receio de perderem a sua soberania em questões relativas à concessão de segurança aos seus cidadãos (Tadjbakhsh, 2005), contudo, os atores no sistema internacional engajaram-se, cada vez mais, com o discurso da Segurança Humana especialmente quando países como o Canadá e a Noruega adotaram o conceito como parte da sua agenda (Wibben, 2008). Em 1998, os dois Estados definiram que a Segurança Humana seria um princípio orientador das suas políticas externas (Glasius, 2008). Também o Japão abriu um diálogo intelectual sobre a Segurança Humana ao anunciar o apoio a um Fundo das Nações Unidas para a Segurança Humana (Glasius, 2008).

O termo de Segurança Humana foi oficialmente formulado em 2001, pela Comissão de Segurança Humana, como a proteção das liberdades fundamentais e das ameaças generalizadas. Já nos anos seguintes, tornou-se claro que era necessária uma readequação às realidades do século XXI e às ameaças que doravante estavam a ser priorizadas, levando a que a Segurança Humana fosse um tema nas principais agendas mundiais (Tadjbakhsh, 2005). Em 2008, a Assembleia Geral das Nações Unidas iniciou um debate temático sobre a Segurança Humana e as suas implicações para os Estados-membros e as Nações Unidas. Em abril de 2010, o Secretário-Geral da ONU apresentou à Assembleia Geral o primeiro relatório oficial sobre o conceito, definindo-o amplamente como "livre do medo, livre de carências e liberdade para viver com dignidade" (Fukuda-Parr e Messineo, 2012). A Segurança Humana veio oferecer uma forma de responder aos desafios do novo século, salvaguardando os direitos daqueles que detinham menos poder. Ao longo dos anos este paradigma afirmou-se como válido para identificar, priorizar e resolver problemas emergentes de segurança transnacional. Houve uma mudança na perceção dos riscos, com o fim dos perigos tradicionais e com novas ameaças mais globais a estarem mais presentes na agenda mundial, como o terrorismo e o crime organizado quando as principais vítimas passaram a ser as pessoas.

O discurso da Segurança Humana é um discurso do indivíduo, procurando ultrapassar os estudos em que o objeto da segurança era o Estado e elevando a segurança dos seres humanos à prioridade mais alta que os Estados deveriam tomar (Burgess, 2017). A noção de Segurança Humana é centrada nas pessoas, baseada em necessidades humanas individuais e encorajando uma compreensão multidimensional da segurança (Nyadera e Bincof, 2019).

A verdade é que assistimos a graves violações de direitos humanos e da Segurança Humana dos reclusos em Guantánamo e é por essa razão que este quadro teórico se afirma como central para que as preocupações com a vida, a dignidade e a humanidade dos mesmos sejam cada vez mais parte de um discurso de Segurança e para que situações como a do 11 de Setembro não sirvam como justificação para que práticas ilegais, condenáveis e excessivas aconteçam. O objetivo é encontrar estratégias mais eficazes de forma a responder a essas ameaças e que sejam compatíveis com o que a Segurança Humana defende: a proteção das liberdades fundamentais e dos direitos humanos, criando-se um ambiente onde todas as pessoas se sintam seguras (Nuhiu, 2017).

De forma a estudar o tema proposto é necessário, de igual modo, enquadrá-lo em alguns dos conceitos estruturantes que constituem o quadro teórico sob análise e no qual se baseia esta pesquisa.

Segundo Brandão (2005, p. 111), o próprio conceito de segurança não é objetivo, mas sim socialmente construído, proveniente de um alargamento do conceito que originou questões sobre o mesmo por entre as abordagens construtivistas. Uma das principais características do termo "segurança" é o facto de estar há muito tempo associado ao Estado, no sentido de ser o próprio a garanti-la à sua população, uma vez que também é o próprio Estado que detém as capacidades, meios e mecanismos de uso da violência com o objetivo de garantir proteção aos seus cidadãos (Amaro, 2008, p. 84). Ainda, este conceito tende a aparecer num contexto de manutenção da ordem pública e do controlo da criminalidade (Amaro, 2008, p. 84). No entanto e como explicado anteriormente, o mundo como hoje o conhecemos foi sofrendo alterações, o que originou uma adaptação do que era o conceito de segurança humana, estando mais abrangente e fazendo parte dele várias áreas de atuação.

A privação de direitos políticos e direitos de segurança acabou por originar uma conjuntura propícia para a existência e propagação do terrorismo em si (Callaway e Harrelson-Stephens, 2006, p. 773). Este pormenor torna-se aqui relevante devido ao facto de os direitos humanos fazerem parte dos conceitos estruturais para a teoria da Segurança Humana. Para todos os efeitos, segurança humana e direitos humanos encontram-se intrinsecamente ligados, tornando-se óbvio que de modo a obtermos uma segurança humana alargada a todos, o próprio quadro teórico procura a defesa dos direitos humanos, aliados às liberdades fundamentais.

Desta forma, começamos a entender a conexão da teoria com os seus conceitos estruturais, tendo já analisado os conceitos de segurança e direitos humanos. Seguindo esse caminho é possível entender que, de modo a salvaguardar os direitos humanos e fundamentais, é necessário que haja um indivíduo pelo menos. E é por aqui que a Segurança Humana se destaca, sendo que, em oposição aos demais quadros teóricos, o indivíduo surge como ponto fulcral de proteção sob a segurança humana, onde o Estado desempenha apenas um papel de, no máximo, providenciador da mesma, com os mecanismos e meios de imposição da paz e ordem mencionados anteriormente.

Podemos terminar este enquadramento dizendo ainda que a teoria é multidisciplinar, fazendo parte um conceito alargado de segurança, princípios das Relações Internacionais, desenvolvimento humano e estudos estratégicos (Tărteaţă, 2021, p.178).

2. Contextualização histórica

A ideia de que a história entre Guantánamo e os Estados Unidos da América surge apenas após o fenómeno de "caça ao homem" subsequente ao 11 de Setembro é, facilmente, induzida em erro. Na verdade, é seguro afirmar que a história entre estes dois Estados surge por volta do século XIX e, desde aí, tem sido uma "montanha russa" de tensões entre ambos.

De modo a entender como surgiu este conflito, é necessário voltar ao passado colonial de Cuba que, na altura do século XIX, estava ainda sob o domínio espanhol, sendo aqui que os Estados Unidos da América começam por desenvolver os seus interesses económicos e geopolíticos pela ilha cubana. A doutrina Monroe fazia referência ao não objetivo colonialista dos EUA, pelo contrário. A partir desse ponto, o objetivo americano no mar das Caraíbas passou pela criação de um *mare nostrum* semelhante ao mar Mediterrâneo na época do império romano, influenciado por essa posição estratégica desse conjunto de ilhas. Este fenómeno espelhou ainda aquele que seria o principal objetivo americano em termos de política externa, o de espalhar pelo mundo a presença americana (Kaplan, 2005).

Com esse propósito, os Estados Unidos alocaram tropas americanas em Cuba em 1898, quando declararam guerra a Espanha, apoiando, ainda que *off the record*, movimentos de independência. O processo não foi demorado, tão pouco penoso, uma vez que seria uma tarefa difícil para Espanha a deslocação de tropas para o local, não apresentando máxima resistência. Após o sucesso no alcance da independência, os Estados Unidos transformaram Cuba num protetorado, respondendo sempre ao governo americano. Este tipo de regime iria durar até à revolução de 1959; até esse ano, a relação bilateral entre os dois Estados foi sempre pacífica, atraindo ainda investimento americano para Cuba. É neste plano que Guantánamo se insere, quando em 1903 é assinado um acordo que concede aos Estados Unidos o aluguer perpétuo de 116 km² da Baía de Guantánamo por um valor de cerca de 4.000$, após o último ajuste feito pelos americanos em 1973, onde apenas os americanos podem cancelar o acordo (Marco, 2016). Dentro do contexto de que a independência apenas foi alcançada através dos Estados Unidos, Cuba não teve outra opção que não a de cedência do território, o que não impediu, nos anos posteriores, tentativas de revogação do acordo, tentativas estas que se tornaram intensivas após a revolução cubana liderada por Fidel Castro que alegava que a aquisição da base não era legal, tendo apenas conseguido cortar o abastecimento de água e minar os terrenos em volta da base. A partir da revolução, motivada por intenções nacionalistas, começou o escalar de tensões entre Estados Unidos e Cuba, que se moveu no espectro político para a esfera soviética, dando origem, mais tarde, a um dos mais infames episódios da Guerra Fria, a Crise dos Mísseis de Cuba.

George W. Bush declarou a "Guerra ao Terror" como forma de combater o terrorismo num contexto pós 11 de Setembro, e a partir deste ponto começou a poder ser feita a associação da prisão de Guantánamo enquanto meio de combate ao terrorismo que foi prioridade nos Estados Unidos. Em 2002, os primeiros detidos provenientes da "caça ao homem" referida anteriormente, deram entrada na prisão de Guantánamo.

Esses detidos não eram mais do que cidadãos comuns afegãos e paquistaneses membros da Al-Qaeda ou Talibã, fruto da oferta de recompensas pela identificação de um tipo de perfil daquilo que seria expectável de um terrorista (Nolen, 2009). Foi devido a essas falhas legais e a um aproveitamento por parte do governo americano do pretexto de apanhar todos os responsáveis envolvidos no ataque de 11 de Setembro ou possíveis terroristas que poderiam atentar contra os Estados Unidos, que acabou por surgir a má fama à qual está associado Guantánamo, um local onde as regras não se aplicam e formas de tortura são consideradas métodos de obter informação (Bridge Initiative Team, 2020).

É seguro afirmar que, ainda que a história entre estas duas nações exista há mais de 100 anos, a revolução cubana foi considerada um momento de viragem nesta relação que, até esse momento, era de cooperação, tendo sido o 11 de Setembro um acontecimento que alterou toda a dinâmica de Guantánamo.

3. Terrorismo de Estado

Após a contextualização temática, é importante para este estudo salientar a definição de terrorismo de Estado, como surgiu e as suas principais causas, para assim percebermos o conceito e o porquê de Guantánamo ser atingido pelo mesmo, como iremos verificar ao longo deste terceiro capítulo.

Podemos dizer que o terrorismo de Estado é a prática de ações ilegítimas e ilegais por parte de um governo, comportando a violação dos direitos humanos que causam medo e terror, e, procurando, também, a submissão dos civis. Ainda, com o intuito de tentar legitimar estas práticas, os Estados alegam razões de causa maior: a segurança nacional e a sobrevivência do Estado (Stohl, 2006, p.2).

Quando tratamos estas práticas por partes dos Estados, estamos a falar de ações de retaliação contra civis, assédio pela aplicação da lei, o desaparecimento propositado de pessoas e ainda a tortura. Tudo isto é feito com o objetivo de impor uma ordem, uma ideologia à população, obrigando esta última a submeter-se aos interesses prioritários do Estado, bem como, permanecerem obedientes perante estas práticas criminosas. No entanto, é importante salientar no decorrer desta análise que, por se tratar das práticas ilegítimas de Estados, torna-se mais difícil e morosa a prova e a acusação de práticas terroristas, pois são estes os principais atores do sistema internacional (Stohl, 2006, p.4).

De forma sucinta, na tentativa de definir terrorismo de Estado, pois não há uma definição completa consensual, os principais pontos consideram-no como sendo o uso ilegítimo do aparelho do Estado contra civis. E, sem justificação legal aparente, abrange o monopólio da violência com falta à obrigação de a usar nos termos previstos pela lei (Stohl, 2006, pp. 4-5).

O governo desse mesmo Estado utiliza recursos à sua disposição, económicos, sociais, políticos e militares, para garantir o sucesso da sua ação, na intimidação da população a quem estas práticas se destinam. Alegando sempre "a melhor das intenções", isto é, na tentativa de dissipar as ameaças à sua segurança. De forma mais detalhada, na questão referida anteriormente, sobre quais são ou quais podem ser as práticas levadas a

cabo pelos Estados, para além das referidas, temos também a criação sigilosa de grupos ou de organizações clandestinas, que estão ao abrigo do Estado, para a perseguição e detenção de pessoas, bem como a criação e a utilização de centros de detenção próprios para os quais os detidos são enviados com a violação do direito ao processo judicial. E, finalmente, ao não proporcionar a emigração ou até mesmo o exílio desses civis, ou seja, a recusa e a proibição da própria mobilidade destes (Stohl, 2006, pp. 6-9).

Uma possível definição citada por Ruth Blakeley (2009), dada por Mitchell et al. (1986) nos anos 80 do séc. XX, foi um passo para uma evolução na agenda no estudo do terrorismo de Estado:

> Terrorismo, quer seja pelo Estado, quer por atores não estatais, inclui o exercício da coerção e violência deliberadas dirigidas a alguém, com o objetivo de induzir o medo a certos observadores de modo a que se identifiquem com a vítima de maneira a que se percecionem, elas mesmas, como futuras vítimas. Desta forma, são levadas a considerar mudar o seu comportamento para que este vá de encontro com o esperado pelo autor desta coerção (Mitchell et al., 1986, citado por Blakeley, 2009)[1].

Quando remontamos às origens do terrorismo de Estado, estas muitas vezes são representadas no século XIII, num espírito de revoluções onde se verificaram ações mais violentas:

> Foi a Revolução Francesa que (...). Compôs o terror de Estado, ultrapassando os suplícios, pela instituição da paz interna, conjugando o exercício das disciplinas, normalizações, medidas de exceção jurídico-políticas, e configurou a prisão como espaço corretivo para onde deveriam ser destinados os perigosos (Guilherme Castelo Branco, 2017, 17).

Quando falamos de terrorismo, seja qual o tipo, registamos uma evolução que relacionamos com o carácter geopolítico. Seja terrorismo nacional com grupos como ETA (Euskadi ta Askatasuna), IRA (Exército Republicano Irlandês), Brigadas Vermelhas, o terrorismo internacional, no caso, por exemplo, do massacre em Munique pela OLP (Organização para a Libertação da Palestina), e mais prementemente o terrorismo transnacional, com maior expressão, de cariz fundamentalista e "apocalíptico", explicado também pela rápida evolução do mundo devido à globalização. Contudo, não nos podemos esquecer de que a ênfase nesta análise é no terrorismo de Estado, a forma como os Estados gerem ou influenciam a sua condição no sistema internacional, dando resposta às suas necessidades geoestratégicas, com a intenção de fazer manter e, até aumentar, a sua relevância no palco, global (Guilherme Castelo Branco, 2017, p. 119).

3.1. Terrorismo de Estado nos Estados Unidos da América

Os EUA não faltam à lista de países que têm ou já tiveram adotadas estas práticas, pois, na verdade, estão dentro do grupo de Estados que, por muito tempo, prosseguiu

1 Tradução: Terrorism by the state (or non- state actors) involves deliberate coercion and violence (or the threat thereof) directed at some victim, with the intention of inducing extreme fear in some target observers who identify with that victim in such a way that they perceive themselves as potential future victims. In this way they are forced to consider altering their behaviour in some manner desired by the actor.

com estas ações como pretendemos demonstrar. E é este Estado, hoje considerado como aquele que continua a ter grande influência no sistema internacional e nas relações internacionais, que vai aqui ser tratado.

Dando especial atenção à prisão de Guantánamo, que se estreia enquanto prisão dentro de uma doutrina marcante de um presidente americano, George Bush, e a doutrina "War on terror" após o 11 de Setembro. Verificamos desta forma que as democracias liberais de hoje estão em risco e não conseguem seguir os seus princípios em momentos de crise, que se mostram cruciais à História da Humanidade. O que nos pode mostrar isto? O que podemos afirmar é que os nossos regimes políticos correm perigo, a era da democracia está em jogo, ao serviço dos interesses nacionais dos Estados na medida em que estes decidem como, quando e onde a utilizam (Stohl, 2006).

Um dos efeitos da globalização foi a evolução das ideias de forma tão rápida, e a dissipação destas da mesma forma, bem como a mudança para a "era da cronopolítica". A mudança é uma característica do mundo de hoje, e, por isso, não podemos dizer que os princípios das democracias liberais são imutáveis.

É importante referir que a história dos EUA revela que a sua política externa não foi linear. Também por razões geopolíticas, esta política externa dividia-se, apresentando uma dicotomia entre o idealismo e o realismo: ao idealismo podemos ligar a criação da Sociedade das Nações com Woodrow Wilson, e por outro lado, numa vertente realista realçamos o poderio militar e a instalação de bases militares espalhadas pelo globo. No entanto, também podemos ligar a política externa dos EUA a uma outra dicotomia: o isolacionismo vs intervencionismo; o isolacionismo no espectro continental e, por outro lado, o intervencionismo com a procura dos EUA na sua afirmação enquanto potência global e a sua presença marcante para garantir a relevância ao nível internacional, sendo exemplo o papel dos EUA na Europa após a Segunda Guerra Mundial.

Os EUA são, muitas das vezes, recorrentes na utilização deste uso ilegítimo do aparelho do Estado como, por exemplo, quando tentavam "impor" uma ideologia pró-capitalista pelo globo, como a ética do Macarthismo com medidas anticomunistas e como a alegada luta pela liberdade. No entanto, no caso da doutrina de George W. Bush, esta não teve menor expressão, pois a Autorização para o Uso da Força Militar (AUFM) de 2001 permitia aos EUA a detenção de qualquer indivíduo suspeito de práticas terroristas ou ligação a organizações deste tipo, por parte das forças armadas norte-americanas. Bem como, o encaminhamento destes mesmos indivíduos para bases navais que estavam espalhadas pelo território, uma com grande expressão neste período, como já foi referido, a prisão de Guantánamo em Cuba (Blakeley, 2009, p. 22).

Após os atentados do 11 de Setembro, o presidente Bush declarou emergência nacional, juntamente com a "permissão" do Congresso para a utilização de todos os recursos disponíveis. O uso destes recursos, incluíndo as detenções, mostravam que os EUA permitiam o uso ilimitado de poderes ao presidente e, para além disso, os suspeitos eram sujeitos a torturas sem possibilidade de terem advogados em sua defesa, o que representava uma violação dos direitos humanos e do Pacto Internacional dos Direitos Civis e Políticos, como iremos desenvolver adiante (Damin, 2009, pp.67-68).

Desta forma, conseguimos perceber que o terrorismo de Estado também está presente na história dos EUA, principalmente quando falamos da prisão de Guantánamo, e, tal como já nos disse Cícero, as leis são silenciosas em tempos de guerra (Damin, 2009, p. 117).

3.2. Terrorismo de Estado aplicado à Prisão de Guantánamo

A prisão de Guantánamo foi oficialmente instituída como um centro de detenções para suspeitos terroristas antes dos mesmos enfrentarem um julgamento militar; contudo, rapidamente ficou evidente que o seu objetivo primordial era o de extrair informações sobre possíveis ameaças terroristas (Birdsall, 2010).

Os EUA conseguiram criar com sucesso uma "área extralegal", onde negam os direitos humanos básicos. Contudo, o governo dos Estados Unidos tinha a hipótese de lidar com os ataques de 11 de Setembro de 2001 de uma forma diferente se tivesse optado por utilizar a cooperação global para resolver o problema. Inclusive, poderia ter apelado a uma sucessão de alianças que invocassem os direitos humanos, com o intuito de sinalizar a necessidade de uma solidariedade global (Schneider, 2004).

Graças ao estado legal incomum do território, os direitos dos detidos são limitados e Guantánamo acaba por ser classificado como uma das "zonas em que os regulamentos normais de um Estado não se aplicam e não são aplicados em sua totalidade, lugares em que a exceção aparece como a norma" (Moreno, 2005, citado por Damin, 2009). Ao longo dos anos tornou-se mais predominante a forma como o governo norte-americano tentou contornar as obrigações estabelecidas pela lei internacional e usá-las de acordo com os seus próprios propósitos, à medida que vários casos foram levados a tribunal com a intenção de contestar a prisão e negar procedimentos que permitiam o devido processo a prisioneiros em Guantánamo (Birdsall, 2010).

De acordo com o Artigo 3º da Convenção de Genebra (citado por Pearlman, 2014), o Estado está proibido de torturar, humilhar ou ter qualquer tratamento cruel e degradante para com os prisioneiros de guerra. Apesar do ponto de vista internacional e das ações dos Estados Unidos da América na prisão de Guantánamo estarem sob a vigência desta lei internacional, que exige que os seus prisioneiros sejam tratados de forma humanizada, o governo de Bush defendeu que as mesmas não se aplicam, justificando esta ação ao afirmar que, uma vez que os detidos violaram as leis da guerra, acabam por ser considerados combatentes inimigos, e não prisioneiros de guerra (Pearlman, 2014). Isto permitiu uma justificação para que os EUA utilizassem todas as formas possíveis para violar os direitos humanos dos presos em Guantánamo, o que justifica a tese de que os EUA espelharam uma forma de terrorismo de Estado em Guantánamo.

De acordo com a mesma fonte, os EUA foram criticados por reivindicar a sua atuação e desenvolver o seu próprio direito internacional no contexto desta guerra e ações contraterroristas. Apesar de defender a prisão de Guantánamo enquanto uma prioridade para a segurança nacional e contra o terrorismo, os próprios EUA legitimaram que se desenvolvesse, nesta zona, a prática de terrorismo de Estado. Sem apresentar regras claras ou proteções definidas para os seus inimigos estrangeiros que são atores não estatais,

acaba também por não ser considerado um conflito armado internacional reconhecido nem sob a Convenção de Genebra, nem sob os seus Protocolos Adicionais (Pearlman, 2014).

Rotulado como um "buraco negro legal" por vários autores, os prisioneiros são detidos em qualquer lugar por ordem militar ou executiva, não tendo direito a qualquer forma de julgamento ou audiência em tribunal (Fletcher, 2004, citado por Damin, 2009). Visto que o governo norte-americano não reconheceu os indivíduos detidos no Afeganistão como prisioneiros de guerra, a proibição de tortura nos Estados Unidos acaba ainda por não se aplicar aos seus interrogatórios em Guantánamo o que reforça, mais uma vez, a ideia aqui defendida que este tipo de prisão constitui uma forma de terrorismo de Estado.

De forma a percebermos como o terrorismo de Estado evoluiu na prisão de Guantánamo, no próximo capítulo iremos abordar os tópicos que marcaram o ano de 2022, refletindo a importância do tema ainda na atualidade e reforçando a necessidade de combater as violações que lá perduram.

4. A prisão de Guantánamo em 2022

O ano de 2022 marcou o 20º aniversário da prisão de Guantánamo, chamando a atenção para as questões acerca da existência do mesmo, sendo que é conhecido como um local que viola os direitos humanos e o Estado de direito. Começamos a ouvir falar no encerramento do estabelecimento logo após o fim do governo Bush, prometido por Barack Obama, acabando sempre por ser impedido pelo Congresso com os Republicanos. Após os EUA terem dado como terminada a chamada "Guerra ao Terror" no Afeganistão e retirado as suas tropas do país, com o acordo entre o Talibã e Donald Trump, em agosto de 2021, a criação, existência e manutenção da prisão perdeu a sua justificação primordial.

Por sua vez, Biden não escondeu que tem como objetivo fechar Guantánamo e Finkelstein, Biddle e Rishikof (2022), consideraram a possibilidade de que 2022 fosse o ano em que o centro de detenção seria finalmente encerrado. Durante os últimos anos os media cobriram vários protestos em que civis questionaram e pediram o fecho da prisão.

De acordo com Elsea (2016), para compreendermos melhor este facto é necessário analisarmos o tratado de 1934, que ainda se encontra em vigor, e que estipula que o acordo só pode ser modificado ou revogado a partir de uma negociação entre os Estados Unidos e Cuba. Apesar de não existir uma lei que proíba a negociação de modificações no tratado com o atual governo de Cuba, a Câmara dos Deputados aprovou a proibição de realizar tal modificação sem a aprovação do Congresso como parte da Lei de Autorização de Defesa Nacional, proibição esta que acabou por ser prolongada até o ano de 2022. Desta forma, mesmo não havendo proibições estatais contra o fecho da instalação militar, o Congresso tem imposto obstáculos práticos ao fecho da mesma, como também, por exemplo, restringido a transferência de reclusos de Guantánamo para países estrangeiros e proibido a sua transferência para os Estados Unidos (Elsea, 2016).

Elsea (2016) ainda menciona a Lei de Autorização de Defesa Nacional (NDAA), aprovada pelo Congresso em 2016 e também estendida a 2022, que proibiu o uso de fundos do Departamento de Defesa para fechar ou abandonar a Estação Naval, ceder o controlo da Baía de Guantánamo à República de Cuba ou ainda para implementar uma modificação material no Tratado entre os Estados Unidos da América e Cuba. Constitui um grande entrave ao fecho desta Base, visto que, a suspensão dessa restrição teria permitido que muitos detidos fossem julgados em tribunais nos Estados Unidos sob as regras tradicionais de provas e procedimentos judiciais (Finkelstein, Biddle e Rishikof, 2022).

Foi também no ano de 2022 que foi libertado o prisioneiro mais antigo de Guantánamo, preso pelas autoridades norte-americanas por uma suspeita de afiliação à Al-Qaeda, sendo a quarta pessoa libertada nesse ano. De acordo com Kim (2022), estas ações fazem parte dos esforços do presidente Biden para reduzir progressivamente o número de reclusos, de forma a que no futuro se consiga encerrar as instalações. Permanecem agora 35 detidos, dos quais a mesma autora afirma, vinte são elegíveis para transferência, três são elegíveis para um conselho de revisão, nove estão envolvidos no processo da comissão militar e três detidos foram condenados. Por outro lado, Farooq (2022), diz-nos que vários advogados de defesa criticaram o governo Biden, afirmando que este não está a fazer o suficiente. Mesmo tendo libertado reclusos e nomeado um funcionário para supervisionar as transferências restantes de Guantánamo, os advogados defendem que ainda não existiu nenhuma ação forte e reformista e demonstram, ainda, a sua preocupação com os cuidados médicos em Guantánamo que espelham uma situação precária.

Finkelstein, Biddle e Rishikof (2022) apresentam como solução o presidente Biden declarar publicamente a sua intenção de retirar as acusações contra todos os indivíduos restantes, com o objetivo de pressionar o Congresso a remover a proibição da NDAA e a permitir transferências para o tribunal de justiça, de forma que os reclusos não escapem completamente da punição.

Isto permite-nos comprovar que a prisão de Guantánamo ainda é um problema discutido atualmente na agenda internacional o que reforça a necessidade de se adotarem novas perspetivas para observar o fenómeno.

5. Terrorismo de Estado na Prisão de Guantánamo sob a lente teórica da Segurança Humana

Após termos refletido sobre a prática de terrorismo de Estado nos EUA, na prisão de Guantánamo até ao ano apresentado na delimitação temporal, 2022, este estudo propõe-se agora, como já referido, analisar o caso sob a lente teórica da Segurança Humana que nos irá ajudar a perceber de que forma o terrorismo de Estado na prisão de Guantánamo constitui uma violação dos direitos humanos.

O 11 de Setembro de 2001 teve um impacto sem precedentes no entendimento tradicional da segurança, na ameaça de atores não estatais e nas medidas necessárias para evitar ameaças à segurança nacional (Nyadera e Bincof, 2019). Os EUA, principalmente,

começaram a colocar as necessidades de direitos humanos em segundo lugar relativamente à sua segurança nacional, dando legitimidade a um sistema onde o terrorismo de Estado está bastante presente, em oposição à Segurança Humana enquanto doutrina protetora dos direitos humanos.

Quando George W. Bush, 43º presidente dos EUA, implementou a Guerra ao Terror como parte da sua estratégia global de combate ao terrorismo, os EUA agiram, sobretudo, de acordo com o seu interesse nacional. Aliás, a ênfase nos interesses nacionais deu o tom da política externa dos EUA, isto é, uma política totalmente unilateralista e isolacionista como já tínhamos observado (Birdsall, 2010). A segurança nacional no centro da agenda política pós 11 de Setembro serviu como justificação para que o terrorismo de Estado acontecesse e para a menor prioridade dada aos direitos humanos e à Segurança Humana. A 18 de setembro de 2001, o governo dos EUA aprovou a Autorização para Uso da Força Militar, que dava ao presidente o poder de usar toda a força necessária e apropriada contra nações, organizações ou pessoas que ele determinasse que estivessem comprometidas de alguma forma com os ataques terroristas, a fim de prevenir futuros atos de terrorismo contra os EUA. O centro de detenções para suspeitos de terrorismo na Baía de Guantánamo, em Cuba, foi uma das formas que os EUA arranjaram de encontrar uma lacuna legal para poderem deter indivíduos ligados à Al-Qaeda e aos acontecimentos do 11 de Setembro, onde os seus direitos humanos estão limitados pela soberania que os EUA detêm do território, e, portanto, onde a Segurança Humana não pode ser aplicável.

Apesar de Bush ter reconhecido a existência de leis humanitárias internacionais, ele determinou que as Convenções de Genebra, convenções que desenvolveram o Direito Internacional Humanitário (DIH), só se aplicavam aos Estados e não à Al-Qaeda enquanto organização terrorista. Os prisioneiros, como vimos, foram considerados como combatentes inimigos ilegais, não se qualificando como prisioneiros de guerra sob as Convenções de Genebra e, por conseguinte, foi-lhes negado o seu estatuto levando a que a Segurança Humana e os seus direitos inerentes não fossem cumpridos e, sim, constantemente violados. A verdade é que, como Birdsall (2010) nos diz, embora a Al-Qaeda apresentasse uma ameaça à segurança dos EUA, existiam outras formas de lidar com essa ameaça que não passassem pelo terrorismo de Estado, que não pusessem em causa a Segurança Humana dos indivíduos e que estivessem em harmonia com o DIH.

A Segurança Humana é um paradigma que, tal como já contemplamos, põe o indivíduo como unidade de referência da segurança. As estratégias antiterroristas assumidas pelos EUA ameaçaram a Segurança Humana ao usarem tortura contra os indivíduos na prisão de Guantánamo, ao não salvaguardar os direitos dos detidos a um julgamento justo e ao impedirem a liberdade de muitos presos injustamente. Sendo assim, ao usarem uma justificação de "segurança nacional", os EUA realizaram estas ações ilegítimas e inúmeras violações dos direitos humanos, adotando uma forma de terrorismo de Estado onde o indivíduo não foi colocado como o principal referente da segurança, mas sim os EUA e os seus interesses. A Segurança Humana ajuda a desenvolver a estrutura existente dos direitos humanos (Nyadera e Bincof, 2019) que, neste caso, não foi cumprida. A

ameaça à Segurança Humana foi perpetuada por um sistema onde a prisão de Guantánamo consistiu numa forma de terrorismo de Estado, apesar de os EUA negarem todas estas acusações tendo por base que os detidos não são prisioneiros de guerra, mas sim, combatentes inimigos ilegais.

A Segurança Humana só poderá existir quando o indivíduo tem possibilidade de possuir um padrão de vida adequado e quando não se sente ameaçado (Tărteață, 2021). Ora, os detentos na prisão de Guantánamo vivem num ambiente de constante ameaça sem direito a uma vida digna e é por essa razão que a Segurança Humana não existe para eles. A entidade de segurança em Guantánamo nunca foram os indivíduos, mas sim os EUA, o que contraria a tese da Segurança Humana que defende que os Estados não são mais os únicos objetos de segurança e reforça ainda mais a ideia, presente nesta pesquisa, que a prisão de Guantánamo constitui uma forma de terrorismo de Estado dos EUA em que os interesses do Estado são prioritários a quaisquer outros interesses, justificando práticas terroristas. A Segurança Humana não é uma segurança militar ou nacional pois o ser humano está no cerne da questão para esta doutrina e não o Estado (Tărteață, 2021). As atuais estratégias de segurança e política externas dos EUA não deveriam influenciar negativamente o indivíduo ao criar desigualdade e ao sacrificar os direitos fundamentais em nome dos interesses estatais, como aquilo que aconteceu e ainda acontece em Guantánamo.

Se os EUA tivessem adotado uma abordagem mais compreensiva da Segurança Humana em vez de Terrorismo de Estado, todos os detidos em Guantánamo teriam sido tratados com humanidade, com direitos a um julgamento justo e com respeito pela sua dignidade humana, ou seja, a Segurança Humana permitiria que a estratégia de combate ao terrorismo e segurança nacional que os EUA adotaram, fosse compatível com os direitos humanos (Paulussen e Scheinin, 2020). O facto de os EUA terem escolhido Guantánamo como o local para o efeito, sendo um "buraco legal", é em si, uma supressão da Segurança Humana pois foi onde se permitiu o uso de condutas terroristas. Uma abordagem que envolvesse a Segurança Humana poderia gerar um clima onde o foco recaía nas necessidades dos indivíduos presos em Guantánamo e não foi isso que realmente se verificou, pois, o foco sempre permaneceu nos EUA.

Ainda não se encontrou soluções para que a segurança individual seja uma prioridade na política internacional (Tărteață, 2021); mas o facto é que a Segurança Humana não contribui apenas para os indivíduos, também contribui para a segurança nacional, regional e internacional, ao proteger os direitos humanos e ao criar condições necessárias para uma paz sustentável que só pode ser alcançada quando as necessidades básicas e os direitos de todos os seres humanos forem atendidos (Nuhiu, 2017), incluindo aqueles que ainda estão sujeitos às condições da prisão de Guantánamo. Em Guantánamo, os EUA prejudicaram fisicamente os detidos e, desta forma, passaram a violar os seus direitos de segurança pessoal (Callaway e Harrelson-Stephens, 2006) um direito inerente à Segurança Humana. A violação destes direitos criou um ambiente propício para o desenvolvimento de doutrinas contrárias à Segurança Humana, uma delas, como já referido, o Terrorismo de Estado.

Podemos concluir que na ótica da Segurança Humana os interesses dos indivíduos que estão presos na prisão de Guantánamo estão em primeiro lugar, comparando com os interesses que os EUA têm em manter os presos em Guantánamo, mas neste panorama não é isso que se sucede. O que observamos é uma ideologia contrária à Segurança Humana, de Terrorismo de Estado, na tentativa de promover uma maior segurança nacional dos EUA, e é por esse motivo que presenciamos constantes violações dos direitos humanos neste lugar, algo que iremos analisar na seguinte secção.

5.1. Privação dos Direitos Humanos

Como já analisamos, os direitos humanos ficaram atrás das considerações de segurança nacional dos EUA depois do 11 de Setembro de 2001 e aquando da criação da prisão de Guantánamo em 2002. A segurança nacional importou mais que a Segurança Humana e subsequentemente que os direitos humanos.

A Segurança Humana veio mudar a perceção que os direitos humanos só existem em virtude de uma pessoa ser cidadão de um Estado, sendo que os direitos humanos devem existir independentemente dos Estados (Birdsall, 2010). Desde as Convenções de Genebra de 1949, as normas para as leis internacionais relativas ao DIH foram fundamentais para regular os direitos humanos, que, contudo, foram constantemente violados por alguns Estados. O caso que analisamos é um desses exemplos, observando-se um abuso do direito internacional e dos direitos humanos através da detenção de pessoas sob custódia dos EUA na Baía de Guantánamo.

Observámos anteriormente que os direitos dos detidos em Guantánamo não estavam protegidos pelas Convenções de Genebra devido ao seu estatuto de combatentes inimigos ilegais, o que permitia aos EUA uma maior margem para interrogá-los. Bush, no momento da criação da prisão, referiu que iria tratar os presos com humanidade de acordo com a "necessidade militar", mas esta necessidade militar é a palavra-chave para que os EUA pudessem fazer uso da força, na tentativa de eliminar as ameaças à sua segurança. Mesmo que estes prisioneiros não pudessem ser classificados como prisioneiros de guerra, eles ainda têm direitos básicos que não foram respeitados (Birdsall, 2010). Por exemplo, foram inúmeros os relatos de utilização de tortura por parte de militares dos EUA de forma a extraírem informações sobre possíveis ameaças terroristas. Logo aí se verificou que os EUA fizeram uso do terrorismo de Estado, intimidando os prisioneiros e praticando formas de interrogatórios abusivas. Ao longo dos anos foram surgindo mais queixas sobre a forma como os prisioneiros eram tratados nos interrogatórios, que claramente minavam as normas e leis dos direitos humanos e os esforços do contraterrorismo. Os casos podem ter incluído a negação de tratamento médico adequado a detentos que participaram em greves de fome (Tittemore, 2006) e, para além disso, Schneider (2004) menciona o uso de tortura leve e através da privação do sono, da exposição constante à luz intensa e também da proibição de falarem com detidos de outros blocos.

Mohamedou Slahi, um prisioneiro de Guantánamo de 2002 a 2016, já relatou muitas das condições em que viviam, muitas vezes sem comida ou água, sem acesso a cuidados de higiene básicos, e presos em celas frias e pequenas. Mohamedou Slahi lutou para sair

da prisão, alegando que não os EUA não tinham provas sobre a sua ligação à Al-Qaeda; no entanto, ao longo dos anos os pedidos foram negados pelos EUA. O jovem apenas teve ligações com a organização no início da década de 1990, quando esta ainda tinha o apoio dos EUA para a retirada do governo comunista no Afeganistão, não tendo, portanto, participado dos ataques terroristas de 2001. Mohamedou Slahi esteve preso durante 14 anos, pois nenhuma legislação o resguardou, nem a ele nem aos restantes detidos em Guantánamo e a alguns que ainda lá permanecem. Assim, os prisioneiros de Guantánamo permanecem detidos indefinidamente, sem poderem recorrer aos tribunais dos EUA para contestar a legalidade da sua detenção. Os esforços da comunidade internacional, especialmente de organizações de direitos humanos, em dar voz aos reclusos e retirá-los de Guantánamo ainda não foram suficientes, apesar de Biden estar a trabalhar para que isso aconteça.

Schneider (2004) afirma, além do mais, que se o governo norte-americano considerasse os detidos prisioneiros de guerra e não combatentes inimigos ilegais, teriam ocorrido inúmeras violações da Convenção de Genebra:

> Artigo 13: assim que os prisioneiros chegaram, eles foram exibidos, ajoelhados no chão, com as mãos amarradas nas costas, usando óculos escuros e fones de ouvidos – isso equivale a uma violação da proteção da curiosidade pública (essas fotos foram transmitidas em todo o mundo). Isso ofende a dignidade do indivíduo e é calculado para o humilhar. Também haveria uma violação do artigo 18 – os detidos foram despojados das suas próprias roupas e privados dos seus pertences. Foram internados numa penitenciária (artigo 22.º), onde lhes foram negados refeitórios adequados (artigo 26.º), cantinas (artigo 28.º), instalações religiosas (artigo 34.º), oportunidades de exercício físico (artigo 38.º), acesso ao texto da Convenção (artigo 41), liberdade de escrever para as suas famílias (artigos 70, 71) e pacotes de alimentos e livros (artigo 72). Eles não foram libertados e repatriados após a cessação das hostilidades ativas (artigo 118)[2] (Schneider, 2004, p. 426).

Infelizmente, como percebemos, as violações dos direitos humanos na Baía de Guantánamo não foram poucas nem raras, o que revela que os EUA desrespeitaram as normas internacionais ao adotarem práticas de terrorismo de Estado em nome da proteção da sua segurança nacional. Os EUA, a nação conhecida por ser uma das maiores defensoras das doutrinas de direitos humanos, cometeram as mesmas violações que tanto condenavam em outras áreas do mundo (Pearlman, 2014). Como já mencionamos, os EUA criaram uma zona extralegal negando os direitos humanos básicos dos indivíduos em vez de usarem a cooperação global para lidar com os ataques do 11 de Setembro

2 Tradução: Article 13: as soon as the prisoners arrived, they were displayed, kneeling on the ground, hands tied behind their backs, wearing blacked-out goggles and earphones – this amounts to a breach of the protection of public curiosity (these pictures were broadcast around the world). This offends the dignity of the individual and is calculated to humiliate. There would also be a breach of Article 18 – detainees had been stripped of their own clothes and deprived of their possessions. They were interned in a penitentiary (Article 22) where they were denied proper mess facilities (Article 26), canteens (Article 28), religious premises (Article 34), opportunities for physical exercise (Article 38), access to the text of the Convention (Article 41), freedom to write to their families (Articles 70, 71) and parcels of food and books (Article 72). They were not released and repatriated after the cessation of active hostilities (Article 118).

de maneira diferente. A prisão de Guantánamo é classificada como um emblema de abusos de direitos humanos, um local onde a subjetividade jurídica dos indivíduos é impugnada ou mesmo suspensa permanentemente (Zevnik, 2011).

Ao negarem os direitos fundamentais dos presos em Guantánamo, os indivíduos, em nome de uma segurança que não a sua, foram vistos numa luta que impediu que a Segurança Humana fosse viável. O aumento do nível de segurança nacional nem sempre é proporcional com o cumprimento dos direitos humanos como verificamos em Guantánamo; contudo, se aplicássemos uma doutrina em conformidade com a Segurança Humana, poderíamos dizer que o aumento do nível de Segurança Humana estava em harmonia com os direitos humanos e aí que se reflete a diferença fundamental entre a Segurança Humana e a segurança nacional propagada pelos EUA em forma de Terrorismo de Estado, mais militarizada e em proporcionalidade com agendas estatais (Nuhiu, 2017). É nesta diferença que se espelha a necessidade da adoção do paradigma da Segurança Humana em Guantánamo, para que os direitos humanos dos indivíduos que lá se encontram sejam a prioridade fundamental.

Conclusão

A base de Guantánamo mantém-se na jurisdição dos EUA desde 1903 até à atualidade. A partir da doutrina de Bush, o intuito principal com a manutenção da prisão foi encobrir as violações dos direitos humanos. O objetivo principal com estas violações continua a ser o de extrair informações de grupos terroristas, de forma a evitar futuros ataques como o 11 de Setembro. Contudo, os métodos utilizados são ineficazes.

Destacamos também o facto de o território de Guantánamo ter valor acrescentado para os EUA, pois é um território neutro, podendo estes aplicar de forma deliberada as leis mais convenientes, visto que não estão na alçada jurídica de nenhuma das partes envolvidas.

O terrorismo de Estado presente na prisão de Guantánamo constitui uma forma de violação dos direitos humanos pelos motivos já mencionados, designadamente a designação que foi atribuída aos reclusos, a recusa de um julgamento justo e as formas de tortura diária a que foram sujeitos. Os EUA, através do terrorismo de Estado em Guantánamo, violaram ainda os direitos humanos ao fazer uso ilegítimo do seu aparelho, dado que, abusaram do seu poder e influência através da mobilização de recursos económicos, militares, humanos, entre outros.

Ainda com a ajuda da lente teórica da Segurança Humana foi possível responder a esta pergunta de investigação e torna-se evidente o contraste existente entre o terrorismo de Estado praticado pelos EUA na prisão de Guantánamo e os ideais que o paradigma da Segurança Humana defende, ao valorizar a segurança do indivíduo acima da segurança do Estado.

Em suma, aquela que poderia ter sido a estratégia adotada pelos EUA para combater o terrorismo, de cooperação internacional, não aconteceu, acabando por originar um dos maiores flagelos praticados pelos norte-americanos apesar de os EUA serem considerados uma democracia liberal.

Bibliografia

Amaro, A., 2008. Segurança humana e protecção civil na sociedade do risco: a crise do modelo estatocêntrico na(s) segurança(s). *Territorium*, (15), pp.83–94. Doi: 10.14195/1647-7723_15_7.

Betts, A. e Eagleton-Pierce, M., 2005. Editorial Introduction: 'Human Security'. *St Antony's International Review*, [online] 1(2), pp.5–10. Disponível em: https://www.ingentaconnect.com/content/stair/stair/2005/00000001/00000002/art00002 [Consultado a 16 nov. 2022].

Birdsall, A., 2010. 'A monstrous failure of justice'? Guantanamo Bay and national security challenges to fundamental human rights. *International Politics*, 47(6), pp.680–697. Doi: 10.1057/ip.2010.25.

Blakeley, R., 2009. State Terrorism in the Social Sciences: Theories, Methods and Concepts. [online] kar.kent.ac.uk. Disponível em: http://kar.kent.ac.uk/30159/ [Consultado a 13 nov. 2022].

Brandão, A.P., 2005. A Segurança Humana em Debate: Human Security in Debate. *Perspectivas – Journal of Political Science*, pp. 106–116.

Bridge Initiative Team, 2020. Factsheet: The History and Evolution of Guantánamo Bay Detention Camp. [online] *Bridge Initiative*. Disponível em: https://bridge.georgetown.edu/research/factsheet-the-history-and-evolution-of-guantanamo-bay-detention-camp/ [Consultado a 13 nov. 2022].

Burgess, P., 2017. Posthuman security. *European Journal of Human Security*, (1), pp.63–76. Doi: 10.5937/ejhs1701063b

Callaway, R.L. e Harrelson-Stephens, J., 2006. Toward a Theory of Terrorism: Human Security as a Determinant of Terrorism. *Studies in Conflict & Terrorism*, 29(8), pp.773–796. Doi: 10.1080/10576100600701974a.

Damin, C.J., 2009. Democracia e poderes emergenciais: o caso da 'guerra contra o terrorismo' nos Estados Unidos. [online] Disponível em: http://hdl.handle.net/10183/21580 [Consultado a 11 nov. 2022].

De Lauri, A., 2020. Humanitarianism: Keywords. *Leiden: Brill.*

Elsea, J.K., 2016. Naval Station Guantanamo Bay: History and Legal Issues Regarding Its Lease Agreements. [online] *Congressional Research Service*. Disponível em: https://crsreports.congress.gov/product/pdf/R/R44137 [Consultado a 13 nov. 2022].

Farooq, U.A., 2022. Biden administration not taking 'concrete steps' to close Guantanamo, defence lawyers say. [online] Middle East Eye. Disponível em: https://www.middleeasteye.net/news/defence-lawyers-say-biden-administration-not-doing-enough-close-down-guantanamo [Consultado a 11 nov. 2022].

Finkelstein, C., Biddle, A. e Rishikof, H., 2022. Beyond Guantánamo: Restoring the Rule of Law to the Law of War. [online] *University of Pennsylvania: Center for Ethics and the Rule of Law*. Disponível em: https://www.penncerl.org/wp-content/uploads/2022/09/Beyond-Guantanamo--Restoring-the-Rule-of-Law-to-the-Law-of-War.pdf [Consultado a 11 nov. 2022].

Fukuda-Parr, S. e Messineo, C., 2012. Human Security: A Critical Review of the Literature. *Centre for Research on Peace and Development* 11.

Glasius, M., 2008. Human Security from Paradigm Shift to Operationalization: Job Description for a Human Security Worker. *Security Dialogue*, 39(1), pp.31–54. Doi: 10.1177/0967010607086822.

Guilherme Castelo Branco, 2017. Terrorismo de Estado. *Autêntica*.

Kaplan, A., 2005. Where Is Guantanamo? *American Quarterly*, 57(3), pp.831–858. Doi: 10.1353/aq.2005.0048.

Karlsrud, J., 2017. Towards UN counter-terrorism operations? *Third World Quarterly*, 38(6), pp.1215–1231. Doi: 10.1080/01436597.2016.1268907.

Kim, J., 2022. The U.S. releases the oldest prisoner in Guantánamo Bay. *NPR*. [online] 29 out. Disponível em: https://www.npr.org/2022/10/29/1132605483/oldest-prisoner-guantanamo-released-pakistan.

Kraft, E.C., 2013. A operacionalização de segurança humana no sistema jurídico e político internacional. [online] *Universidade Técnica de Lisboa*. Disponível em: http://hdl.handle.net/10400.5/6180 [Consultado a 11 nov. 2022].

Marco, D.G., 2016. Como e quanto os EUA pagam a Cuba pelo aluguel da baía de Guantánamo. [online] *BBC News Brasil*. Disponível em: https://www.bbc.com/portuguese/noticias/2016/03/160321_eua_cuba_guantanamo_dgm_cc [Consultado a 4 nov. 2022].

Martins, R.F.C., 2010. *Acerca de «Terrorismo» e de «Terrorismo»*. Instituto da Defesa Nacional. Lisboa. Disponível em: www.idn.gov.pt.

Nolen, J., 2019. Guantánamo Bay detention camp | United States detention facility, Cuba. *Encyclopædia Britannica*. [online] Disponível em: https://www.britannica.com/topic/Guantanamo-Bay-detention-camp [Consultado a 4 nov. 2022].

Nuhiu, B., 2017. Terrorism And Human Rights. *Pravne teme*, [online] 5(09), pp.177–185. Disponível em: https://www.ceeol.com/search/article-detail?id=607932 [Consultado a 16 nov. 2022].

Nyadera, I.N. e Bincof, M.O., 2019. Human Security, Terrorism, and Counterterrorism: Boko Haram and the Talibã. *International Journal on World Peace*, [online] 36(1), pp.4–15. Disponível em: https://www.academia.edu/38994786/HUMAN_SECURITY_TERRORISM_AND_COUNTERTERRORISM_BOKO_HARAM_AND_THE_TALIBAN?auto=citations&-from=cover_page [Consultado a 15 Nov. 2022].

Paiva, G.A.A. de e Digolin, K.A., 2022. A relação entre direitos humanos e segurança humana. *GEDES*. Disponível em: https://gedes-unesp.org/a-relacao-entre-direitos-humanos-e-seguranca-humana/ [Consultado a: 4 November 2022].

Paulussen, C. e Scheinin, M., 2020. Human Dignity and Human Security in Times of Terrorism. *The Hague: T.M.C.* Asser Press. Doi: 10.1007/978-94-6265-355-9.

Pearlman, S., 2014. Human Rights Violations at Guantanamo Bay: How the United States Has Avoided Enforcement of International Norms. *Seattle University Law Review*, [online] 38, pp.1109–1138. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/sealr38&div=42&id=&page= [Consultado a 11 Nov. 2022].

PNUD, 1994. *Relatório do Desenvolvimento Humano 1994*. [online] Oxford University Press. New York. Disponível em: https://hdr.undp.org/system/files/documents/hdr1994encompletenostatspdf.pdf

Ponto de Viragem: o 11 de Setembro e a guerra contra o Terrorismo, 2021. Netflix.

Rocha, R.M. de A., 2017. Segurança humana: histórico, conceito e utilização. [online] *Universidade de São Paulo*. Disponível em: https://teses.usp.br/teses/disponiveis/101/101131/tde-08092017-155459/pt-br.php [Consultado a 15 nov. 2022].

Schneider, D., 2004. Human Rights Issues in Guantanamo Bay. *The Journal of Criminal Law*, 68(5), pp.423–439. Doi: 10.1350/jcla.68.5.423.43228.

Silva, M.G.C., 2019. Segurança humana, responsabilidade de proteger e Direito Internacional: o caso de intervenção na Líbia. *repositorium.sdum.uminho.pt*. [online] Disponível em: http://repositorium.sdum.uminho.pt/handle/1822/58858 [Consultado a 12 nov. 2022].

Stohl, M., 2006. The State as Terrorist: Insights and Implications. *Democracy and Security*, 2(1), pp.1–25. Doi: 10.1080/17419160600623418.

Tadjbakhsh, S., 2015. Human Security: Concepts and Implications with an Application to Post-Intervention Challenges in Afghanistan. [online] *Les études du CERI*. Disponível em: https://www.sciencespo.fr/ceri/en/content/human-security-concepts-and-implications-application-post-intervention-challenges-afghanista [Consultado a 12 nov. 2022].

Tărteaţă, C., 2021. Human security, Terrorism and Organized crime in the Western Balkans. *Strategies XXI – National Defence College*, 1(72), pp.178–186. doi:10.53477/2668-5094-21-13.

Tittemore, B.D., 2006. Guantanamo Bay and the Precautionary Measures of the Inter-American Commission on Human Rights: A Case for International Oversight in the Struggle Against Terrorism. *Human Rights Law Review*, 6(2), pp.378–402. Doi: 10.1093/hrlr/ngl008.

Warren, A. e Grenfell, D., 2017. Rethinking Humanitarian Intervention in the 21st Century. *Edinburgh University Press*. Doi: 10.1515/9781474423823.

Wibben, A.T.R., 2008. Human Security: Toward an Opening. *Security Dialogue*, 39(4), pp.455–462. Doi: 10.1177/0967010608094039.

Zevnik, A., 2011. Becoming-Animal, Becoming-Detainee: Encountering Human Rights Discourse in Guantanamo. *Law and Critique*, 22(2), pp.155–169. Doi: 10.1007/s10978-011-9087-0.

Género, Segurança e Política Externa da União Europeia: uma Análise Crítica da Implementação da Resolução 1325

Francisca Martins Reina

Em outubro de 2020, o Parlamento Europeu adotou uma resolução sobre "igualdade de género na política externa e de segurança da UE" que apelava à União Europeia (UE) para incorporar os princípios da integração de género (*gender mainstreaming*) da/e interseccionalidade na sua política externa e de segurança (Parlamento Europeu, 2020). A resolução partiu da iniciativa da eurodeputada Hannah Neumann, que tem vindo a defender a adoção de uma Política Externa Feminista (PEF) na UE, à semelhança de alguns Estados-membros, como a Suécia, França, Espanha e, mais recentemente, Alemanha.

Até ao momento, a UE não desenvolveu nenhuma PEF comum, mas tem havido um esforço no sentido de integrar uma perspetiva de género na ação externa da UE. Foi também em 2020 que a UE lançou o seu terceiro Plano de Ação em matéria de Igualdade de Género nas relações externas (GAP III 2021-2025). Além disso, a agenda das Mulheres, Paz e Segurança (MPS) foi reconhecida como uma das principais áreas de intervenção do GAP III, na sequência da adoção, em 2019, do Plano de Ação da UE para implementar a agenda MPS a nível comunitário. É importante referir que a Europa é a região com o maior número de Planos Nacionais de Ação (PNAs) para a implementação da Resolução 1325 (2000) do Conselho de Segurança das Nações Unidas, a resolução histórica que inaugurou a agenda MPS a nível global.

Tendo em conta estes desenvolvimentos empíricos, é importante questionar a invisibilidade tanto das questões de género e da agenda MPS como das perspetivas feministas nos debates sobre *actorness* global da UE. A maioria dos estudos sobre políticas de género na UE preocupa-se com as dinâmicas políticas internas da UE e com os efeitos da adesão à UE sobre os regimes nacionais em matéria de igualdade de género (Thomson, 2022). Por outro lado, os poucos estudos sobre igualdade de género na política externa da UE relacionam-se com as políticas de cooperação, ajuda ao desenvolvimento e relações comerciais (Anagnostakis, 2021). Assim, as outras dimensões da ação externa da UE que se relacionam mais diretamente com os objetivos da agenda MPS, como a política de segurança, paz, ação humanitária ou migrações, permanecem nas margens da discussão.

Neste sentido, este artigo procura responder à seguinte questão: como é que a UE incorpora o princípio da integração de género (*gender mainstreaming*) e a agenda MPS na sua ação externa? Metodologicamente, o artigo apoia-se na revisão da literatura e na análise de documentos estratégicos sobre género e segurança no contexto da UE. De forma resumida, o artigo argumenta que a discrepância que se verifica entre a identidade de líder global em igualdade de género projetada pela UE, a sua abordagem estratégica para a agenda MPS e a implementação lenta e seletiva dos compromissos assumidos comprometem a afirmação da UE como ator global no âmbito da agenda MPS.

Conceptualizando a UE como um ator global

Para compreender a forma como as questões de género e a agenda MPS moldam a capacidade de a UE se posicionar como um ator global, é importante conhecer os diferentes contributos teóricos das Relações Internacionais (RI) para conceptualizar a *actorness* (agência) da União Europeia. Em particular, as abordagens construtivistas ocupam um lugar central nesta área de estudo, enfatizando o conjunto de normas, ideias e significados partilhados (isto é, a estrutura intersubjetiva) que constituem a identidade coletiva da UE como ator global (Rumelli e Cebeci, 2016).

Uma das formas de conceptualizar o papel internacional da UE destaca a importância do seu poder normativo. Neste caso, Manners (2002) conceptualiza a UE como um ator normativo, destacando o seu papel como promotora internacional de normas partilhadas no espaço europeu, incluindo os seus cinco valores fundamentais: paz, liberdade, democracia, Estado de direito, e respeito pelos direitos humanos. Reconhecendo "a sua evolução histórica particular, a sua política híbrida, e a sua configuração constitucional", Manners conclui que "a UE tem uma base normativamente diferente para as suas relações com o mundo" (p. 252).

De modo semelhante, Bretherton e Vogler (2006) entendem a capacidade de afirmação da UE como ator global a partir da interação entre três condições relacionadas entre si: oportunidade (*opportunity*), capacidade (*capability*), e presença (*presence*). Em primeiro lugar, o conceito de 'oportunidade' traduz o contexto estrutural que enquadra a ação da UE, mais concretamente "o ambiente externo de ideias e eventos que [a] constrangem ou viabilizam" (Bretherton e Vogler, 2006, p. 22). Em segundo lugar, o conceito de capacidade (*capability*), teorizado por Sjöstedt (1977), é determinado pelo ambiente político interno da UE, refletindo os entendimentos distintos sobre a capacidade de formular políticas eficazes (de acordo com critérios de coerência e consistência interna) e a disponibilidade de instrumentos adequados (de âmbito político, económico e militar) (Bretherton e Vogler, 2006, p. 28). Finalmente, a presença (*presence*), conceito formulado por Allen e Smith (1990), descreve a capacidade da UE, em virtude da sua existência, de exercer influência para além das suas fronteiras (Bretherton e Vogler, 2016, p. 22). Combina os entendimentos sobre o caráter e a identidade da UE, e as consequências externas (imprevistas) das políticas internas da UE.

Assim, ao constituir-se como comunidade de valores ou como 'poder normativo', a UE é colocada no papel específico de promotora e exportadora do conjunto de valores e normas que a diferenciam dos restantes atores – em particular, o valor da igualdade de género. No entanto, é importante contrariar a forma como a integração de género e a agenda MPS em particular estão muitas vezes ausentes nestes debates devido à marginalização recorrente das perspetivas feministas nos estudos da UE. Por exemplo, o institucionalismo feminista é particularmente relevante para compreender como é que as normas e políticas de género operam dentro das instituições (Thomson, 2018). O que estes estudos sublinham é o papel desempenhado por diferentes atores institucionais feministas no interior da União Europeia (Guerrina e Wright, 2016). A secção seguinte sublinha a importância destes contributos para compreender a forma como as questões de género são integradas na ação externa da UE.

Integração de género na política externa e de segurança da UE

As últimas décadas têm sido marcadas pela crescente difusão de normas e políticas sobre igualdade de género e empoderamento das mulheres na política externa. Dois desenvolvimentos são particularmente relevantes para o nosso argumento: primeiro, a política de integração de género (*gender mainstreaming*), que implica a integração da perspetiva da igualdade de género em todas as fases da formulação da política externa; segundo, a incorporação de uma perspetiva de género na governança da paz e segurança internacional, de acordo com os princípios da Resolução 1325 de 2000 do Conselho de Segurança das Nações Unidas, que estabelece a agenda das Mulheres, Paz e Segurança (MPS) (Aggestam e True, 2020).

A política de *gender mainstreaming* nasce nas conferências mundiais sobre a mulher organizadas pelas Nações Unidas, em particular na Conferência e Declaração de Pequim, em 1995, na sequência da qual os governos nacionais e as organizações internacionais passaram a adotar uma perspetiva de género nos seus processos de decisão (Hafner-Burton e Pollack, 2002). Deste modo, a ascensão da agenda global para a igualdade de género sob o impulso das Nações Unidas criou o contexto normativo propício à consagração do princípio da integração de género pela UE no Tratado de Amsterdão, adotado em 1997. Se a perspetiva de género já tinha sido incorporada noutras áreas de política interna da UE (como o emprego e a proteção social), as questões de género eram praticamente invisíveis no âmbito da política externa (Chappell e Guerrina, 2020). Ainda assim, a igualdade de género constitui um valor fundamental através do qual a UE projeta o seu poder normativo no plano global (Peto e Manners, 2006).

Uma explicação possível para a introdução tardia da perspetiva de género na política externa e de segurança relaciona-se com a própria natureza da UE como sistema de governação multinível. Em particular, a necessidade de equilibrar princípios de governação supranacional e intergovernamental em competição entre si coloca dificuldades ao reforço da integração no domínio da política externa e de segurança (Dover, 2010; Bretherton e Vogler, 2016). Por um lado, o ambiente político resultante do fim da Guerra

Fria e da eclosão dos conflitos violentos nos Balcãs era mais favorável ao reforço do papel da UE na política de segurança global. Neste contexto, o Tratado da União Europeia (TUE), adotado em 1992, instituiu a Política Externa e de Segurança Comum (PESC), que, a par da Estratégia Europeia de Segurança (EES) de 2003 (depois substituída pela Estratégia Global da UE de 2016), estabelece o enquadramento político para a ação externa da UE. Por seu turno, o Tratado de Lisboa, adotado em 2007, expandiu as capacidades de atuação da UE no domínio da política externa, segurança e defesa. Entre outras inovações, o tratado instituiu a Política Comum de Segurança e Defesa (PCSD) e o cargo de Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança e Vice-Presidente da Comissão (AR/VP), assistido pelo Serviço Europeu para a Ação Externa (SEAE), o recém-criado serviço diplomático da UE.

Por outro lado, a arquitetura institucional da PESC concentra a tomada de decisão em matéria de política externa e segurança nos Estados-membros (reunidos em Conselho da UE), seguindo o princípio do intergovernamentalismo, mantendo as barreiras já existentes a uma maior integração. De acordo com a estrutura em pilares consagrada no TUE, a cooperação em matéria de segurança e política externa está prevista no segundo pilar da UE, de natureza intergovernamental, pelo que a tomada de decisão no âmbito da PESC é feita por voto de unanimidade no Conselho da UE. Embora os três pilares tenham sido desmantelados, o carácter intergovernamental da PESC não foi revertido no Tratado de Lisboa. O Parlamento Europeu permanece excluído dos processos de decisão, enquanto a Comissão Europeia possui um papel limitado e indireto, por via do AR/VP e de domínios específicos da ação externa da UE (como as relações comerciais, por exemplo).

Assim, dentro da estrutura de governação multinível da UE, existe alguma variação no posicionamento e capacidade de atuação das diferentes instituições europeias, determinando o modo como a integração de género é concebida e implementada na prática. Por exemplo, o Parlamento Europeu – e, de forma menos significativa, a Comissão Europeia – tem manifestado uma posição mais favorável ao desenvolvimento de uma política externa sensível ao género do que os Estados-membros da UE.

Para uma análise crítica da integração da perspetiva género na UE é importante considerar os contributos do institucionalismo feminista, que sublinha a importância destas barreiras institucionais. O institucionalismo feminista estuda a interação das instituições políticas com as relações de género, atentando na operação das normas de género no interior da estrutura burocrática e institucional dos Estados e organizações internacionais (Thomson, 2018). Neste âmbito, Guerrina e Wright (2016), por exemplo, destacam o papel fundamental de atores institucionais feministas para o desenvolvimento do regime de igualdade de género da UE. Estes atores feministas incluem os 'femocratas'[1] dentro da Comissão Europeia, a Comissão dos Direitos da Mulher e da Igualdade dos

1 O termo 'femocratas' (no inglês, *femocrats*) refere-se a indivíduos posicionados dentro de uma estrutura burocrática que trabalham para efetuar mudanças transformativas em linha com os objetivos feministas (Guerrina and Wright, 2016, p. 296).

Géneros (FEMM) do Parlamento Europeu, e organizações da sociedade civil como o Lobby Europeu das Mulheres (LEM).

Todavia, os atores feministas distribuídos pelas diferentes instituições europeias enfrentam obstáculos maiores nos domínios onde a UE não detém competências claras, como é o caso da política externa e de segurança. Como notam Guerrina e Wright (2016, p. 305), "...são as instituições supranacionais – como o Parlamento Europeu, a Comissão e o Tribunal de Justiça da UE – que têm defendido consistentemente o papel da UE como *'gender actor'*. Os Estados-membros, contudo, mantêm um elevado nível de controlo sobre as questões de segurança e defesa, reduzindo assim as oportunidades para outras instituições atuarem como empreendedores políticos (*policy entrepreneurs*)." Não é, pois, surpreendente que a integração de género seja mais expressiva nos domínios da ação externa sob a competência da Comissão Europeia, como o comércio a ajuda ao desenvolvimento (Scneiker et al., 2020; Woodward e Van der Vleuten, 2014), por oposição aos domínios controlados pelos Estados-membros.

Mesmo em domínios como a ajuda ao desenvolvimento e cooperação internacional, onde a integração da perspetiva de género é mais significativa, permanecem alguns problemas que limitam a realização plena da política de empoderamento e igualdade de género na UE. Uma parte da literatura questiona os pressupostos subjacentes à política de integração de género, problematizando a instrumentalização e subordinação da agenda da igualdade de género a preocupações económicas mais amplas, alinhadas com o modelo neoliberal dominante. Estas críticas destacam o modo como a adoção de políticas neoliberais amplifica as desigualdades existentes e compromete o pleno empoderamento económico das mulheres, sobretudo nos países do Sul Global (Anagnostakis, 2021; Haastrup, Wright, e Guerrina, 2019). Além disso, Chappell e Guerrina (2020), por exemplo, questionam o verdadeiro potencial das políticas de integração de género em instituições predominantemente masculinas, como o SEAE, onde as mulheres continuam sub-representadas nas posições de gestão e liderança. Uma vez que as dinâmicas de género existentes no interior das instituições europeias e dos Estados-membros permanecem intactas, a integração de género tem um potencial de transformação muito limitado.

Situando a agenda das Mulheres, Paz e Segurança na UE

Numa tentativa de incorporar os princípios da integração de género no sistema de governação da paz e segurança internacional, o Conselho de Segurança das Nações Unidas aprovou a Resolução 1325 sobre Mulheres, Paz e Segurança (MPS) em outubro de 2000. Esta resolução constitui um marco histórico assinalável, sendo a primeira vez que o Conselho de Segurança reconhece o impacto desproporcional e específico dos conflitos armados nas mulheres e raparigas.

Assim, a agenda MPS (que, além da Resolução 1325, inclui nove resoluções adicionais) estabelece um quadro normativo internacional dividido em três pilares fundamentais: primeiro, a participação e representação das mulheres em todas as fases da tomada de decisão; segundo, a proteção dos direitos e necessidades específicas das mulheres e

raparigas durante os conflitos; e terceiro, a incorporação de uma perspetiva de género nos processos de resolução de conflitos, construção da paz e reconstrução pós-conflito (Kirby e Shepherd, 2016). Os Estados-membros são responsáveis pela implementação da Resolução 1325, nomeadamente através do desenvolvimento de Planos Nacionais de Ação (PNA), que traduzem a abordagem e estratégia dos governos nacionais para concretizar a agenda MPS a nível nacional. Até ao momento, cerca de oitenta países publicaram PNA, incluindo vinte e quatro Estados-membros da UE.

Nos últimos anos, as organizações regionais também têm vindo a assumir responsabilidades específicas na implementação da agenda MPS, abrindo uma janela de oportunidade para a UE desenvolver uma abordagem integrada. Além do Parlamento Europeu, países como a Suécia, a Áustria e a Bélgica têm pressionado as instituições europeias para desenvolver uma ação conjunta neste âmbito (Barnes, 2011; Guerrina, e Wright, 2016).

No entanto, os primeiros passos nesse sentido surgiram apenas durante as presidências eslovena e francesa do Conselho da UE em 2008, com a aprovação da *Abordagem global da implementação pela UE das Resoluções 1325 e 1820 do Conselho de Segurança das Nações Unidas sobre as mulheres, a paz e a segurança* (de agora em diante, *Abordagem global*). No documento, a UE adota uma abordagem tripartida assente na incorporação da agenda MPS no diálogo político com países terceiros, a integração do género nas suas políticas e atividades, e o apoio de ações estratégicas direcionadas para a proteção e o empoderamento das mulheres (Conselho da UE, 2008, p. 11).

Desde então, o Conselho adotou um conjunto de medidas concretas para promover a integração de género na PCSD. Em particular, estabeleceu um grupo de trabalho informal sobre a Resolução 1325 (*Informal Task Force on UNSCR 1325*) para assegurar a consistência e coordenação interna entre as diferentes instituições europeias. Este grupo de trabalho era composto por membros do SEAE, do secretariado do Conselho e da Comissão, estando ainda aberto à participação dos Estados-membros e de Organizações Não Governamentais (ONG). Contudo, as instituições da UE careciam de experiência no âmbito da agenda MPS, pelo que o grupo de trabalho dependeu, em grande medida, dos contributos da ONU Mulheres, a agência das Nações Unidas para a Igualdade de Género e Empoderamento das Mulheres (Scheniker et al., 2020).

Além disso, em 2015, o SEAE introduziu o cargo de Assessor Principal de Género (*Principal Gender Advisor*), responsável pela coordenação da UE com outros atores internacionais, regionais e nacionais na ação política relacionada com género e Resolução 1325. No entanto, o seu potencial de transformação é limitado pela posição marginal ocupada pelo Assessor dentro do SEAE, sobretudo quando comparado ao papel do Representante Especial da NATO para as Mulheres, Paz e Segurança. De um modo geral, os Estados-membros têm concentrado os seus esforços no âmbito da agenda MPS nas instituições da NATO, um aspeto que levanta algumas questões relacionadas com o próprio papel da UE como ator global no domínio da segurança e defesa, como discutimos anteriormente (Guerrina, e Wright, 2016).

No âmbito específico da PCSD, a integração de género tem evoluído de forma gradual, sobretudo ao nível das missões e operações civis e militares (Chappell, e Guerrina,

2020). Além da criação de Assessores de Género e da formação em igualdade de género (Martinelli, 2014), a representação das mulheres nas missões e operações da UE subiu ligeiramente: nas vinte e seis missões e operações conduzidas pela UE entre 2008 e 2017, as mulheres representavam 5,9% do pessoal militar, 10,9% da polícia, e 27,8% do pessoal civil internacional (SIPRI, 2018).

Apesar desta evolução positiva, o desenvolvimento de uma política comum para a implementação da agenda MPS ao nível da UE surge tardiamente, em dezembro de 2018, com a adoção das *Conclusões do Conselho sobre as Mulheres, Paz e Segurança* e da respetiva *Abordagem Estratégica para as MPS*, que substitui a anterior *Abordagem global* de 2008. A nova *Abordagem Estratégica*, coordenada pelo SEAE, descreve a visão e os objetivos da UE para a implementação plena da agenda MPS. Concebida com o propósito de colocar a agenda MPS no centro da Política Externa e de Segurança Comum (PESC) da UE e de traduzir os compromissos europeus em ações concretas e holísticas, a Abordagem Estratégica é operacionalizada no *Plano de Ação da UE para as Mulheres, Paz e Segurança* (2019-2024) aprovado em 2019. Tanto a *Abordagem Estratégica* como o *Plano de Ação* que detalha a sua implementação estão estruturados ao longo de quatro áreas de intervenção fundamentais – prevenção, proteção, assistência e recuperação –, sendo informados por dois princípios transversais, a integração de género e a participação.

A *Abordagem Estratégica* aplica-se aos vários domínios da ação interna e externa da UE, sendo reforçada pelo quadro normativo europeu sobre igualdade de género, nomeadamente o terceiro *Plano de Ação em matéria de Igualdade de Género nas relações externas* (GAP III). O documento realça que a implementação da agenda MPS não é responsabilidade única dos Estados-membros, mas também das próprias instituições da UE, incluindo o SEAE, as delegações da UE, os serviços da Comissão, e as missões e operações da PCSD. Além disso, reforça a importância de incorporar a *Abordagem Estratégica* da UE no desenvolvimento dos PNA dos Estados-membros, de forma a reforçar a sua coerência e consistência interna (Conselho da UE, 2018, p. 4).

Neste sentido, um dos princípios básicos desta *Abordagem Estratégica* é a sua aplicabilidade universal e o carácter vinculativo da sua implementação para todos os atores da UE e Estados-membros, bem como nas relações com países terceiros. Em particular, o documento sublinha o compromisso da UE em "agir como um líder global quando se trata de implementar plenamente a agenda MPS" (Conselho da UE, 2018, p. 17). Ainda assim, a UE contraria as abordagens tradicionais dos Estados-membros de implementação maioritariamente externa da agenda MPS (isto é, aplicada apenas a situações de conflito como a prevenção de conflitos, resolução de conflitos e construção). Nesta nova abordagem, a UE reconhece e a necessidade de implementação também na dimensão interna, nomeadamente através do apoio a organizações de mulheres (incluindo associações de mulheres migrantes e refugiadas e defensoras de direitos humanos), e da integração da perspetiva de género na agenda de prevenção e combate ao terrorismo e extremismo violento (Conselho da UE, 2018, p. 21).

Por um lado, estes desenvolvimentos representam um progresso importante na UE, reforçando a sua capacidade de afirmação como ator global no âmbito da agenda MPS.

Como destacam Haastrup, Wright e Guerrina (2019, p. 68), a *Abordagem Estratégica* reflete uma visão mais holística e detalhada do que as abordagens anteriores, procurando dotar a UE de agência própria no âmbito da agenda MPS e sublinhando a confiança das instituições europeias em desenvolver e apropriar-se desta agenda política. De facto, até 2018, a implementação da agenda MPS na UE tinha um carácter fragmentado, na medida em que a maioria das iniciativas e programas se desenvolviam nos setores da segurança e defesa, sem coordenação com as ações tomadas nos restantes domínios da ação interna e externa da UE.

Por outro lado, esta preferência por uma abordagem holística e inclusiva não se traduziu em medidas concretas destinadas a transformar o significado e a prática da segurança pela UE, respeitando o propósito original da Resolução 1325. Esta não é, contudo, uma característica exclusiva da UE. Como argumenta Shepherd (2016), a cooptação da agenda MPS pelos governos nacionais e organizações de segurança, que a subordinam às suas políticas securitárias e militaristas (reduzindo-a ao esforço de 'tornar a guerra segura para as mulheres' ao invés de construir uma paz sustentável), é um dos principais obstáculos à realização do potencial transformativo da Resolução 1325.

Esta reprodução dos significados e práticas dominantes de segurança limita significativamente a capacidade de a UE se afirmar como um ator global distinto no que diz respeito à agenda MPS (Scheniker et al., 2020). Como argumentam Deiana e McDonagh (2018) no seu estudo sobre a implementação da agenda MPS no planeamento das missões da PCSD, uma conceção minimalista e tradicional de segurança, gestão de crises e estabilidade prevalece frequentemente sobre as preocupações com as questões de género. Como consequência, a incorporação da agenda MPS na PCSD é crescentemente limitada a questões como a representação feminina nas missões de manutenção da paz e a violência sexual durante os conflitos, contrariando os compromissos mais amplos expressos nos documentos estratégicos da UE sobre a agenda MPS.

De modo semelhante, a implementação da agenda MPS no SEAE reflete uma visão limitada e instrumental sobre o princípio da integração de género. Chappell e Guerrina (2020) criticam o princípio '*add women and stir*' subjacente à abordagem da UE, cujo objetivo único é assegurar a paridade de género nas estruturas institucionais da SEAE. Na sua perspetiva, a preocupação com o aumento da representação feminina nas instituições existentes não é acompanhada do esforço de desconstrução das relações de género no seu interior e que determinam a forma como a segurança e defesa são pensadas e praticadas. Pelo contrário, a UE tem demonstrado uma estratégia de cooptação e despolitização da igualdade de género como forma de promover os seus interesses como organização.

Conclusão

Como tentei demonstrar ao longo deste artigo, existe um grande fosso entre os compromissos normativos da UE com a agenda MPS e a sua implementação plena ao longo de todos os domínios da ação interna e externa da UE, comprometendo a sua capacidade de se afirmar como ator global em matéria de igualdade de género.

Por um lado, a aprovação da Resolução 1325 em 2000, num contexto político pós-Guerra Fria, tornou a estrutura de oportunidades mais favorável à afirmação da UE como ator global no âmbito da agenda MPS. De facto, os primeiros países a desenvolver PNAs para implementar a Resolução 1325 eram Estados-membros da UE e, atualmente, a Europa é a região com o maior número de PNA aprovados. Além disso, a igualdade de género é um dos valores fundamentais através dos quais a UE constrói a sua identidade como 'poder normativo' na sua ação externa (Woodward & Van der Vleuten, 2014), na qual a agenda MPS poderia ocupar uma posição mais central.

Por outro lado, e apesar destas condições favoráveis, a integração da agenda MPS na ação externa da UE surge de forma tardia e fragmentada, através da *Abordagem Global* em 2008, posteriormente substituída pela *Abordagem Estratégica* e o respetivo *Plano de Ação* em 2018. Se esta nova *Abordagem* representa um avanço significativo na forma como a agenda MPS é articulada no discurso da UE, na prática, a Resolução 1325 continuou a existir nas margens da ação externa da UE e o seu potencial transformativo não foi encarado com seriedade.

Há várias explicações possíveis para a marginalização e subordinação da agenda MPS às prioridades políticas mais amplas da UE como ator global. Primeiro, a conceptualização da agenda MPS como pertencendo somente ao domínio da segurança e defesa (na sua conceção mais restrita e moldada pela visão militarista dos Estados), e não como uma agenda de transformação social e política que atravessa todas as dimensões da ação europeia, limita significativamente a capacidade da UE se afirmar como ator global neste âmbito. Se é verdade que, do ponto de vista discursivo, a nova *Abordagem Estratégica* propõe uma visão mais holística da agenda MPS, ancorada numa abordagem *rights-based*, na prática, a sua implementação permaneceu limitada e subordinada aos objetivos da política de segurança e defesa da UE.

Segundo, e como consequência desta estratégia de securitização e militarização da agenda MPS, as capacidades limitadas da UE no domínio da segurança e defesa constituem um obstáculo ao desenvolvimento de uma política comum de integração de género neste domínio, contribuindo para esta dupla marginalização da agenda MPS na UE. Como tentei demonstrar, a natureza intergovernamental da PESC e da PCSD coloca os Estados-membros numa posição dominante no que diz respeito à definição do significado e prática de segurança na UE. Em particular, a preferência por uma conceção militarizada de segurança exclui as preocupações e objetivos de mudança social que estão na origem da aprovação da Resolução 1325, em que a construção de uma paz sustentável está dependente da transformação das relações de género existentes.

Um dos principais desafios para a investigação futura será tentar compreender os significados atribuídos à integração de género e à agenda MPS pelas diferentes instituições da UE e o modo como cada uma procura influenciar a tomada de decisão neste domínio. Além disso, é necessário alargar a análise a outros atores institucionais importantes, como os grupos de interesse, as organizações da sociedade civil e outras organizações internacionais (como a NATO) que interagem frequentemente com a UE no âmbito da agenda MPS. Em todo o caso, a investigação sobre a implementação da agenda

MPS beneficiaria significativamente se fosse prestada maior atenção aos contributos valiosos das abordagens feministas nas Relações Internacionais e nos estudos de segurança, bem como se fossem levadas a sério as experiências e estratégias de atores feministas que tentam colocar a agenda MPS no centro das prioridades europeias.

Referências

Aggestam, K. e True, J., 2020. Gendering Foreign Policy: A Comparative Framework for Analysis. *Foreign Policy Analysis*, 16(2), pp. 143–162.

Allen, D., e Smith, M., 1990. Western Europe's Presence in the Contemporary International Arena. *Review of International Studies*, 16(1), pp. 19–37.

Anagnostakis, D., 2021. EU Foreign Policy and Gender: How Does the EU Incorporate Gender in Its External Relations? In: R. Süleymanoglu-Kürüm, e F. M. Cin, ed. *Feminist Framing of Europeanisation: Gender Equality Policies in Turkey and the EU*. Palgrave Macmillan. pp. 41–61.

Barnes, K., 2010. Turning policies into action? The European Union and the implementation of UNSCR 1325. In: F. Olonisakin, K. Barnes, e E. Ikpe, eds. *Women, Peace and Security: Translating Policy into Practice*. Routledge. pp. 211–222.

Bretherton, C., e Vogler, J., 2006. *The European Union as a Global Actor*, ed. 2006. Routledge.

Chappell, L., e Guerrina, R., 2020. Understanding the gender regime in the European External Action Service. *Cooperation and Conflict*, 55(2), pp. 261–280.

Comissão Europeia, 2020. Joint Communication to the European Parliament and the Council: *EU Gender Action Plan (Gap) III – an Ambitious Agenda for Gender Equality and Women's Empowerment in EU External Action*.

Conselho da UE, 2008. *Abordagem global da implementação pela UE das Resoluções 1325 e 1820 do Conselho de Segurança das Nações Unidas sobre as mulheres, a paz e a segurança*, adotada a 1 dezembro de 2008.

Conselho da UE, 2018. *Council Conclusions on Women, Peace and Security*, adopted on 10 December 2018.

Conselho da UE, 2019. *EU Action Plan on Women, Peace and Security (WPS) 2019-2024*, adopted on 5 July 2019.

CSNU – Conselho de Segurança das Nações Unidas, 2000. *Security Council resolution 1325 (2000) on women and peace and security*. S/RES/1325 (2000).

Davies, S. E., e True, J., 2019. *The Oxford Handbook of Women, Peace, and Security*. Oxford University Press.

Deiana, M.-A., e McDonagh, K., 2018. 'It is important, but…': Translating the Women Peace and Security (WPS) Agenda into the planning of EU peacekeeping missions. *Peacebuilding*, 6(1), pp. 34–48.

Dover, R., 2010. From CFSP to ESDP: the EU's Foreign, Security, and Defence Policies. In: M. Cini, e N. P.-S. Borragán, eds. *European Union Politics*. Oxford University Press.

Guerrina, R., e Wright, K. A. M., 2016. Gendering normative power Europe: Lessons of the Women, Peace and Security agenda. *International Affairs*, 92(2), pp. 293–312.

Haastrup, T., Wright, K. A. M., e Guerrina, R., 2019. Bringing Gender In? EU Foreign and Security Policy after Brexit. *Politics and Governance*, 7(3), pp. 62–71.

Hafner-Burton, E., e Pollack, M. A., 2002. Mainstreaming Gender in Global Governance. *European Journal of International Relations*, 8(3), pp. 339–373.

Kirby, P., e Shepherd, L. J., 2016. Reintroducing women, peace and security. *International Affairs*, 92(2), pp. 249–254.

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

Martinelli, M., 2014. Gender Protection in the Context of EU's External Relations. In: S. Lucarelli, ed. *Gender and the European Union*. Firenze University Press. pp. 51–69.

ONU, 2021. *Report of the Secretary-General on women and peace and security* (S/2021/827).

Parlamento Europeu, 2020. European Parliament resolution of 23 October 2020 on *Gender Equality in EU's foreign and security policy* (2019/2167(INI)).

Peto, A., e Manners, I., 2006. The European Union and the value of gender equality. In: S. Lucarelli, e I. Manners, eds. *Values and Principles in European Union Foreign Policy* Routledge. pp. 97–113.

Rumelili, B., e Cebeci, M., 2016. Theorizing European identity: Contributions to constructivist international relations debates on collective identity. In: V. Kaina, I., P. Karolewski, e S. Kuhn, eds. *European Identity Revisited: New approaches and recent empirical evidence*. Routledge. pp. 31–43.

Schneiker, A., Jenichen, A., e Joachim, J., 2020. Situating the Gender Mainstreaming Norm in Regional Organisations: Comparing the Incorporation of UN Security Council Resolution 1325 in the EU and OSCE. In: L. Engberg-Pedersen, A. Fejerskov, e S. M. Cold-Ravnkilde, eds., *Rethinking Gender Equality in Global Governance: The Delusion of Norm Diffusion*. Palgrave Macmillan. pp. 97–120.

Shepherd, L. J., 2016. Making war safe for women? National Action Plans and the militarisation of the Women, Peace and Security agenda. *International Political Science Review*, 37(3), pp. 324–335.

SIPRI, 2018. *Trends in Women's Participation in UN, EU and OSCE Peace Operations* [Policy Paper]. Stockholm International Peace Research Institute.

Sjöstedt, G., 1977. *The external role of the European Community*. Saxon House.

Thomson, J., 2018. The Women, Peace, and Security Agenda and Feminist Institutionalism: A Research Agenda. *International Studies Review*, 21(4), pp. 598-613.

Thomson, J., 2022. Feminist Foreign Policy Studies in Europe. In: M. Stern, e A. E. Towns, eds. *Feminist IR in Europe: Knowledge Production in Academic Institutions*. Palgrave Macmillan. pp. 115–132.

Villellas, M., Urrutia, P., Villellas, A., e Fisas, V., 2016. *Gender in EU Conflict Prevention and Peacebuilding Policy and Practice* [WOSCAP Orientation Paper]. Escola de Cultura de Pau.

Woodward, A. E., e Van der Vleuten, A., 2014. EU and the Export of Gender Equality Norms: Myth and Facts. In: A. Van der Vleuten, A. Van Eerdewijk, e C. Roggeband, eds. *Gender Equality Norms in Regional Governance: Transnational Dynamics in Europe, South America and Southern Africa*. Palgrave Macmillan. pp. 67–92.

Capítulo II
AMEAÇAS E RISCOS

Climate Security and Security Governance beyond the Central State: Moving the Debate Forward

Ana Raquel Almeida Dias

Introduction

Considering the accelerated rate at which climate change is occurring and its implications for global security, i.e., climate security, the current security governance system will need to adapt (Hoffmann, 2013, p.15; Newell, 2013, p.377). However, this adaptation poses pressing challenges at two distinctive levels: first, at the theoretical level – i.e., on how climate security should be framed – and second, at the practical level – i.e., on how security governance should be implemented and who should be responsible for its provision.

Climate change is widely recognized as a "threat multiplier" (Floyd, 2015, p.124) that poses considerable repercussions for the security of individuals and states (Barnett, 2003; Floyd, 2008; McDonald, 2018). In a context of increased climate risks, climate security emerges, today, as the "condition of not being exposed to dangers" (Dower, 1995) caused by sources of climate change (greenhouse gases – GHG) (Barnett, 2003: 7). Yet, the significant challenge relies on the fact that sources of insecurity are virtually everywhere, spread around the globe (Hoffmann, 2013, p.3).

In a context where no international actor can individually provide climate security (Falkner, 2013, p.252), especially in the absence of a global government (Rosenau, 1992), this paper envisions climate security as a 'global public good', i.e., as a universal, non-rival and non-excludable benefit (Kaul, Grunberg and Stern, 1999, p.11). Additionally, in the absence of clear 'governing solutions' to mitigate sources of climate insecurities, a security governance approach framed within a multilevel system will allow us to shed a new light on alternative dynamics of effectively providing climate security.

Having said that, the contribution of this article towards the literature on climate security and security governance is intended in two complementary ways. The first contribution concerns the conceptualization of climate security as a global public good by looking beyond traditional debates on threat management and discussions on military connotations *versus* human security (Barnett, 2003). The second contribution deals with practical issues of global governance, claiming that climate security requires a security governance approach grounded on a multilevel framework (multilevel governance or

MLG) where states work along other actors in the provision of a global public good, as it is already being conceived under the Paris Agreement. In sum, this article is guided by two objectives: first, the reconceptualization of climate security as a global public good by looking at GHG as sources of insecurity; and second, the framing of climate security governance under MLG rationales (type I), as to understand the prominent role of other institutional actors who, along the state, may work towards the provision of climate security.

The remainder of this article is divided in three parts, corresponding to two different stages of the analysis and a conclusion. To this end, the first part will offer a theoretical debate on climate security by pointing out its limitations and why such deadlock can be overcome through a global public good understanding that is, consequentially, in need of a security governance framework. The second part will first take the lens of MLG I to analyze security governance as a suitable approach for the provision of climate security as a global public good, but it will also signal how some steps are already being taken towards such framework, within the Paris Agreement. Finally, the third and final part of the article will summarize its major arguments.

1. Climate Change and Security Governance: Moving the Debate Forward

Consideration of environmental problems as security concerns is well known in policymaking, yet little research explores the relation between climate change and security (McDonald, 2018). At a time where the provision of climate security is put to the test by the intensification of climate risks (Deere-Birkbeck, 2009, p.1173), the following section acknowledges the need to improve the conceptual understanding of climate security as an essential first step for its effective provision through security governance.

Starting with the scientific phenomenon of climate change, its direct relation to security affairs pertains to its effect as a threat multiplier, by compounding a wide set of dangers to both individuals and states (Dalby, 2013). According to the United Nations Environment Programme (UNEP), the linkage between climate change and security results from the former's impact on food, water, and energy supplies; increased competition over natural resources; loss of livelihoods; and climate-related disasters (2022). By the end of this chain reaction, these risks may result in forced migration and displacement, but also insurgencies, violent conflicts, extremism, and even global terrorism (Deere-Birkbeck, 2009, p.1185). However, more important than making clear the security threats posed by climate change is to highlight the actual sources of such insecurities: the presence and increasing emission of GHG into the atmosphere which is, ultimately, shared by humanity as a whole and has no consideration for national borders (Page, 2013, p.237). Overall, the effective provision of climate security is challenged by the fact that sources of insecurity are spread around the globe (Hoffmann, 2013, p.3).

Since sources of climate risks and threats are virtually everywhere (Page, 2013, p.237), in terms of GHG, no actor in the international system can manage them alone

(Dalby, 2013, p.167; Falkner, 2013, p.252). From this argument, the paper looks at climate security as a global public good, that is, universal, non-rival and non-excludable (Kaul, Grunberg and Stern, 1999, p.11). In sum, the following section aims to bring together the phenomenon of climate change with the notions of global public goods and security governance. The idea is to highlight why climate security should be understood as a 'global public good' while underlining the major difficulties in its provision.

1.1. Conceptual security debates: a deadlock for climate security

In empirical terms, climate change is perceived to be a security issue (Barnett, 2003; McDonald, 2018), acknowledging a connection between global warning resulting from the emission of GHG and security concerns (Floyd, 2008, p.61). Yet, conceptually speaking, climate security is still framed within the general debate on environmental security, firstly inaugurated after the Cold War, with regard to shortages of natural resources and natural disasters (Ulman, 1983). Briefly put aside during the period of "war on terror", the relation between global warming and security came to renew the old debates on environmental security, now under the label of climate security (Floyd, 2008, p.51).

As a contested subfield of International Relations, security has no agreed definition (Walt, 1991; Baldwin, 1997). Different positions within the discipline perceive very differently *who* or *what* is to be secured, *against what it is to be secured* and, also, *the nature of the threat,* which should be considered (Baldwin, 1997). As a natural result, the same questions and divergences apply to environmental security, as a whole, and climate security, specifically. However, the last decades have witnessed a changing perception of humanity's role in the biosphere, resulting from a growing scientific understanding of the effects of general human activity, therefore, highlighting the need for policies to deal with changing circumstances (Steffen, 2013).

This context requires a very careful reflection on the very meaning of security. As noted by Dalby (2013, pp.174-175), current understandings rely on a security system of political institutions, modern sates, and a political economy of carbon-fueled industrialism. If such tendencies remain in the face of mounting disruptions, global security may end up in a situation that Paul Rogers (2010) has called "keeping the violent peace", whereby military forces are used to repress insurrections and maintain the existing political and economic arrangements. Alternatively, the United Nations Framework Convention on Climate Change (UNFCCC) suggests the facilitated participation of a much larger portion of humanity in the decision-making process. Moreover, it is a sustainable economic system that makes a stable climate system the basis for global security grounded on a much less militarized version of the future (*Ibidem*).

On the other hand, in what concerns to the literature, there is a marked division between the dominant position of a (1) military security perspective and the (2) individual security point of view (Floyd, 2008, p.54). The first is focused on (1) national security concerns, physical processes occurring within a sovereign delimited territory which pose security risks, such as sea-level rise, and the consequential violence proliferation – climate effects and/or disasters which may lead to violent conflict (Gleditsch,

1998; Barnett, 2000; Busby, 2007). The second approach relates to (2) human security, a vision focused on the impacts of climate change on individual and community welfare, as well as their livelihoods (Barnett, 2003, p.14; Barnett *et al.*, 2010). The existence of such different visions in framing the climate change-security nexus ultimately gives rise to different security discourses on: whose security is at stake; what is threatening security; who is responsible for the provision of security; and what means should be used (McDonald, 2018).

Despite the traditional cleavages that characterise conceptual debates, it is possible to argue that the nature of climate change may cross military and human security conceptions, being posed as a much broader phenomenon (Barnett, 2003). Coined by Goodman in 2007 as a "threat multiplier", climate risks and threats are pervasive regarding *who* and *what* they affect, being far-reaching in their nature. Although there is no agreement on specific climate threats in the literature (Barnett, 2003, p.7), storms, flooding, and sea-level rises, that reduce crop stability, damage infrastructure, cause food scarcity and induce migration, are just a few examples of the effects of climate change pointed out by authors (Brown, 1977; Brown, 1989; Shaw, 1996; Barnett and Dovers, 2001). To put it simply, an instable long-term weather pattern, experienced in a specific location, and caused by the presence of greenhouse gases in the atmosphere (climate change), may, directly or indirectly, induce the emergence of new risks and threats or aggravate existing ones by destabilising states, societies, and the overall human livelihood, thus leading to a heightened risk of conflicts.

Despite differences in opinion, proponents of major security approaches unquestionably promote climate change as a security concern (Floyd, 2008). Based on this statement, efforts may be endorsed towards the achievement of a common conceptual ground, which may be of significant policy value.

1.2. (Re)conceptualising climate security as a 'Global Public Good'

Aside from traditional security debates which ultimately lead to a deadlock with no agreement in sight, this paper acknowledges that regardless of what environmental and climate issues are to be considered as threats, and what security perspective is adopted, either military or human, a common ground may be found if one envisions climate security as a 'global public good'.

Developed by the well-known economist Paul A. Samuelson (1954), the concept of public good is defined as a "collective consumption good", one in which "all enjoy in common in the sense that each individual's consumption of such good leads to no subtractions from any other individual's consumption of that good" (Samuelson, 1954, pp.387-389). Essentially, the central properties of a public good rely in its non-rivalry and non-excludability or, in other words, in the fact that the consumption by one element does not limit the actual and potential consumption by another (Cottier and Ahmad, 2021). As such notion does not refer to a geographic area of production or consumption, the term has also been used as 'global public good' (Kaul, 2012) to reflect a public good which is non-rival and non-excludable with a worldwide reach, therefore

being different from the ones that exist in a specific national domain (Cottier and Ahmad, 2021). When applied to the global level, public goods remain in possession of their two essential qualities, non-rivalry and non-excludability, while noting that these are assumed to be *quasi*-universal in terms of geographic, demographic, and generational access. In the end, humanity in general is the ultimate beneficiary of global public goods (*Ibidem*).

Bearing in mind the mentioned definition, the existence of sustainable climate conditions which fade climate-related risks and threats caused by the presence and continuous emission of greenhouse gases (GHG) into the atmosphere, *i.e.,* climate security, clearly corresponds to a global public good. Framing climate security in these terms implies a mitigation-based view focused not only on the sources of insecurity as the problem, but essentially on its universal condition of being non-excludable and non-rival: (1) security threats are caused by global and generalized (non-rival) emissions of GHG (insecurity source) into the atmosphere; (2) GHG are spread around the globe with effects in terms of risks and threats, from which no state or individual is excluded (non-excludable). All in all, seeing that the sources of climate insecurity are globally spread with equally global effects, regarding the consequential security threats, climate security may be conceptually understood as a global public good.

Such view is justified by the fact that it allows a broader conception of the climate change phenomenon in terms of the magnitude of risks and threats but, most importantly, it gives a clear direction on what types of strategies are better suited to provide climate security, as will be explained. The very fact that climate change is, in many ways, objectively undefinable means that how a problem is perceived defines the kind of solution applied (Hoffmann, 2013, p.7). Regarding this case, adopting a global public good conceptual framework allows us to directly consider the problem's source, *i.e.*, the presence and continuous emission of GHG into the atmosphere (source of insecurity risks and threats), as universal in its nature.

Acknowledging the fact that causes of climate insecurity are everywhere, arising from nearly all kinds of human activity (agriculture, transportation, manufacturing, energy use, land use), with effects that are felt across the globe (Hoffmann, 2013, p.6), three major arguments may be drawn from climate security's condition as a global public good: (1) no state, individual, or any single actor in the international system is capable of providing it alone; (2) there is no overreaching global authority (Rosenau, 2007, p.93) to proceed with an enforced distribution of shares to reduce sources of insecurity (GHG) and guarantee the overall provision of climate security; (3) if sources of security risks and threats are globally produced, security needs to be globally provided (Uitto, 2016, p.108).

By way of conclusion, one may argue that looking at climate security as a global public good, beyond the debate on military *versus* human security lenses, is a first step towards a common ground for discussion. According to such understanding, climate security as a global public good denotes a universal condition of sustainable climate patterns shared by all states, individuals, and generations, in the absence of or with reduced emissions of greenhouse gases into the atmosphere, which diminishes climate-related risks and threats.

1.3. Governing the Ungovernable? Security Governance of Climate Security

The perception of climate security as a 'global public good' is essentially grounded on the idea that sources of insecurity are globally spread (Hoffmann, 2013, p.3; Page, 2013, p.237). In this sense, a set of GHG emitted anywhere results in the same amount of climate changing potential being exerted everywhere, which poses the complex problem of how to govern through a multidimensional approach, in order to manage insecurities which are all around (Stripple and Stephan, 2013).

The problem with the provision of climate security is that climate change does not consider borders, therefore it needs to be dealt with at the international level, where sovereign authority and territoriality dominate the system. An overall problem with the provision of global public goods brings up the question of *who* should manage the problem of climate change and provide climate security in the absence of a global government (*Ibidem*, 149). Until recent times, the management of global public goods consisted primarily of 'traffic rules' between countries and at-the-border issues as 'tariffs', yet, due to the effects of globalization and the need for international cooperation, global concerns have integrated national agendas, and national concerns became subject of international debate but also policy coordination and harmonization (Kaul, Grunberg and Stern, 1999, p. 450).

As the world population certainly does not negotiate the supply of these goods directly among themselves, such a task is undertaken by governments on their behalf which still correspond to a large number of parties, when it comes to creating cooperative arrangements for goods provision. Similarly, in terms of beneficiaries, global public goods do vary from other public goods: not only are the beneficiary groups extremely large, but they are also highly diverse, being composed of developing and industrial states, poor and rich, with different cultures and different historical backgrounds. In such a context, the interests and concerns of the involved parties will vary considerably in terms of policy priorities and, therefore, cooperation in terms of supplying global public goods becomes difficult to achieve (Kaul, Grunberg and Stern, 1999, pp.14-15).

A first step forward is indeed the recognition of a security governance framework to deal with changing security challenges as a result of transnational risks and threats (Ehrhart, Hegemann and Kahl, 2014, p.119). The idea is that, in the absence of a world government, a set of 'routinised arrangements' are able to sustain 'global life' (Webber *et al.*, 2004, p.5), grounded on mechanisms of collective coordination (Rosenau, 2007, p.93), here understood in the context of MLG. Although there is a wide set of assumptions on the definition of security governance, Ehrhart, Hegemann and Kahl (2014, p.120) note that most definitions converge in the idea of a "pluri-centric coordination in which national governments are one central, but not necessarily the only actor; a combination of formal and informal structures among interdependent but autonomous actors operating beyond formal hierarchies" in the provision of security. Yet, it should be noted that security governance is embedded in broader notions of security analysis, the widening and deepening debate (Buzan and Hansen, 2009) which implies not only

the consideration of a wider range of security threats, such as climate change, but also security actors above (international) and below (sub-state and local) the central state (Krause and William, 1996, p.230; Krahmann, 2003, p.10).

The provision of public goods such as stable climate patterns, *i.e.*, climate security, (Page, 2013, p.237), demands indeed a multi-actor, multi-structure, and a multi-level response (Rosenau, 1997, p.64), in terms of politics, policymaking, and policy implementation towards the direct or indirect reduction of GHG (Hoffmann, 2013, pp.13-15). As noted by Prins and Rayner (2007), there is a call for a "buckshot" approach rather than a "silver bullet" one. The response must encompass various types of activities taking place at many levels, in order to be effective (Hoffmann, 2013, p.15); much beyond a traditional state-centric approach grounded on military concerns and means (Krahmann, 2003, p.10).

In short, climate security governance is here understood as climate mitigation efforts in which governments are the central authority in the coordination of formal and informal policy implementation structures, where interdependent institutional actors autonomously work towards the reduction of greenhouse gases as sources of climate risks and threats. According to this conception, different institutional actors *below* (regional and local) and *above* (international) the state, under a broad institutional framework, may combine formal and informal dynamics in the production of climate security as a global public good: a universally shared condition of sustainable climate patterns in the absence (or reduced emission) of greenhouse gases which significantly reduces (or eliminates) climate-related risks and threats.

This is not to say that the overall solution is achieved through a security governance approach. In fact, many gaps are found in this approach, such as lack of effective coordination between participants (Hoffmann, 2013, p.15), free-riding incentives and the prisoner's dilemma where parties find incentives to not cooperate (Kaul, Grunberg and Stern, 1999, pp.7-8). Starting out with the (1) lack of effective coordination, many responses taking place and involving many actors at various levels may have its pitfalls. Although this means that action is taking place everywhere around the globe and with the participation of various actors, scaling up individual initiatives will not be an easy task and neither will be to achieve a centralized process in the absence of 'global monitoring'. In the end, there is a possibility of it resulting in the fragmentation of climate security governance (Hoffmann, 2013, p.14.). Secondly, in accordance with the (2) free-riding formulation, there is an incentive for parties to free themselves from their loads while relying on others in order to avoid the contribution of personal resources towards common ventures (Kaul, Grunberg and Stern, 1999, p.7). The last aspect arises from game theory, more precisely the (3) prisoner's dilemma, which highlights that parties will be better off cooperating in a situation under which the different parts face incentive to refrain from cooperation (*Ibidem*).

A central aspect to the provision of global public goods is that they face a double danger: (1) market and (2) government failure, given its incapacity to improve cooperation conditions or inability to use its coercive power to achieve optimal outputs (possible

at the national level) (*Ibidem*). In such cases, cooperation may be triggered by additional actors taking a role in the process chain through advocating on behalf of the public concerns (*Ibidem*). Looking at climate change as a local but also global phenomenon, it is of critical importance to analyze the role of institutional players, below and above the state, in the production of global public goods and in climate security governance.

2. Climate change and security governance: a MLG approach to global public goods

Having emphasised climate change as a security concern and its framing as a global public good, which can be better provided in a security governance context (Ehrhart, Hegemann and Kahl, 2014, p.120), this paper also identifies multilevel governance (MLG) as an approach to frame this reality. Such acknowledgement is grounded on the premise that the Paris Agreement has given the first signs of how dealing with climate challenges might require a much broader institutional approach.

In doing so, attention is drawn to the interconnection between supranational, national, regional and local political arenas (Betsilll and Bulkeley, 2006, p.149), in the face of increasingly complex security concerns. Although broad theories of international relations, such as transnationalism or international regimes, could also be indicated as being capable of framing global public goods provision, their capacity to reflect the empirical reality is narrow. While transnationalism is limited to understanding the emergence of the context where action is taking place beyond the central state (Paris's opportunity), Krasner's (1982) theory of international regimes is mainly focused on the creation of international standards by international organizations through the interaction of states. Such approaches are not clear in explaining how the security governance of climate change occurs through processes running at and between different levels, among an array of actors with different degrees and forms of authority.

Against such background, the following section highlights the features of multilevel governance (MLG) that make it a plausible framework for security governance in the provision of climate as a global public good. Furthermore, the Paris Agreement is presented as having created a precedent for the emergence of multilevel governance dynamics in the management of climate affairs and, specifically, in the efforts to reduce GHG.

2.1. MLG and security governance: A framework for global public good provision?

Having mentioned climate change as a security concern and its framing as a global public good, it is time to turn our attention to the crucial need for more security governance in the provision of security, beyond the sole action of the central state (Ehrhart, Hegemann and Kahl, 2014, p.120), under the framework of MLG (Hooghe and Marks, 2003). Looking at the scattered nature of climate change which calls for globally and locally coordinated efforts between different actors in the provision of a global public good, states may find the need to cooperate by reaching out to supranational and subna-

tional authorities (regional and local) considering the challenges posed by climate-related risks and threats.

Theoretically speaking, multilevel governance conceives the "dispersion of authority denoting the existence of a clear hierarchy between different layers of governance who have independent agency not in a context of governance *above* the state but rather governance *beyond* the state within a specific institutional arrangement" (Hooghe and Marks, 2003). The framework broadly translates into two types of relationship dynamics: MLG type I, vertical coordination among (institutional) public actors (international, national, regional and local governments); but also, MLG type II, horizontal coordination between both public and private actors (*Ibidem*). Yet, as this paper is solely focused on the role of public actors, due to the needed legal and institutional action capacity, only MLG type I is going to be considered. Therefore, as greenhouse gas emissions are the result of local processes with a worldwide reach in terms of effects, a climate security governance approach needs to be based on an international framework of national mandates which coordinates and promotes vertical arrangements for a multitude of institutional actors to autonomously act as facilitators of climate security governance provision in a multilevel context.

Resulting from a plethora of worldwide economic activities with equally worldwide effects (non-rival and non-excludable), climate change is undeniably a global matter, and a sphere where only central states can intervene. Yet, it is also true that insecurity sources are regionally and locally produced. Having this in mind, climate security as a global public good necessarily connects the international, national, regional and local governance dimensions. In fact, Kaul, Grunberg and Stern (1999) notice that public goods provision is related with multilevel governance frameworks which seek to allocate regulatory powers with the intention of producing public goods commensurate with the level of governance. In accordance with such understanding, a security governance strategy, aimed at producing climate conditions as global public goods, needs to relate international, national, regional, and local spheres by calling for effective responses at the appropriate governance levels as conceived under a MLG I approach (Cottier and Ahmad, 2021).

An important point of consideration is that climate change is a problem with different layers, with significant differences in its production and the way its effects are felt by the involved dimensions (international, national, regional and local) (*Ibidem*). Each level has the capacity to endorse different answers (different provision means) to a problem which exceeds a single governance sphere. In other words, a multilevel governance approach provides a starting point for a deeper understanding of how a climate security governance framework may be configured for the provision of climate as a global public good, through a dynamic interface of vertical coordination between institutional actors.

2.2. Emerging patterns of MLG type I under the Paris Agreement

The Paris Agreement, signed in 2015 as part of the UNFCCC, is well known for its combination of a bottom-up and a top-down approach that generates a complementary

synergy between activities undertaken by international, national, regional and local authorities. The result is a sequential enhancement of international, but mainly, regional and local entities as essential elements in rising climate action.

For the purpose of this article, the essential feature of the Paris Agreement is reflected on its article 7 (2015), which states that climate change is a "global challenge faced by all with local, subnational, national, regional and international dimensions, and that it is a key component of and makes a contribution to the long-term global response to climate change" (United Nations, 2015, p.9). In sum, the treaty acknowledges the broadening universe of international affairs as complex, fragmented and unstructured (Aldecoa and Keating, 1999, p.6), an official departure towards an agency space that crosses vertical (local, regional, national and international) boundaries (Hoffmann, 2013, p.12).

From such premise, and considering the already mentioned framework of MLG I, one can apprehend that such approach is suitable to understand how climate politics have evolved under the Paris Agreement: acknowledging the magnitude of the climate challenges, central states have found the need to institutionalize the matter at the international level under the UNFCCC, in 1992, which, in 2015, also came to recognize other institutional actors as important players in the long-term global response to climate change and the goal of reducing GHG. This is not to say that central states have seen their role devalued, in fact they have gained a new strategic role within the much broader institutional framework of climate action, which they not only coordinate (as the only signatory parties of the institutional arrangement formalized under the UNFCCC) but also use to cooperate with other entities based on a functional need: the duty to implement global governance goals in climate matters.

What the Paris Agreement comes to acknowledge is that, in the realm of climate change, other actors in the system may play that role, not only because they are closer to the sources of insecurity (GHG) (Brown, 2012, p.322), but also because they are crucial in the implementation and monitoring of policies (Webber *et al.*, 2004, pp. 5-6). According to Hale (2016, p. 14), such role is made explicit by acknowledging these actors not as an alternative to the UNFCCC process, or as merely a helpful addition, but as a core feature of long-term global action. The importance of these actors in the new agreement is by no means innocent or unexpected, in fact, Keohane and Oppenheimer (2016, p.150) state that "the Paris Agreement is less of an accomplishment than part of an already ongoing process" of global governance.

In this respect, Falkner (2016, p.1111) frames the Paris Agreement as a formalization of an already ongoing process which has built the momentum for an agreement in Paris's terms. It was throughout the 2000s that a gradual transformation started taking place within international climate politics (*Ibidem*; Hale, 2016, p.15) for the emergence of a global climate governance beyond the sole action of central states through the progressive pull of authority upwards and downwards. In Paris's terms, climate governance has been recognized as "all purposeful mechanisms and measures aimed at steering social systems toward preventing, mitigating, or adapting to the risks posed by climate change"

(Jagers and Stripple, 2003, p.385). This definition reflects the encompassing nature of global governance, here redirected towards concerns of climate change.

In short, the Paris Agreement can be considered as a dynamic of MLG type I. In the sense that MLG I focuses on the formal distribution of power between levels of authority, downwards and upwards, it is precisely the dynamics of upward delegations from central states to a supranational authority that come to explain how international, subnational, and local authorities may be part of the new framework established by the Paris Agreement.

Conclusion

Climate change is everywhere, not necessarily the physical phenomenon itself, which is indeed an almost daily presence, but, instead, it is an inescapable lens through which the world is observed. As such, this article has sought to bring together climate change, security, and security governance. In doing so, it has sought to move the debate on climate security by conceiving it as a global public good, while highlighting a MLG I approach to climate security governance.

Known to be a threat-multiplier, not only does climate change generate its own risks and threats but it also aggravates already existent ones which may destabilize states, societies, and the overall human livelihood. Importantly, climate change is a direct result of GHG emissions into the atmosphere, which are globally spread (Page, 2013) but, simultaneously, locally produced (Brown, 2012). In the end, no actor alone is capable of reducing GHG (Falkner, 2013; Uitto, 2016) and, therefore, of providing climate security.

Against this backdrop, and although there is no literature consensus on what type of threats are to be considered (Barnett, 2003), this article has adopted a middle ground based on the concept of global public goods. Climate security is here conceived as a universal condition, *i.e.*, non-rival and non-excludable, shared by all states, individuals, and generations, of sustainable climate patterns in the absence (or reduced emission) of greenhouse gases in the atmosphere, which diminishes climate-related risks and threats. By looking directly at the problem, the causes of insecurity (GHG), the paper intends to overcome the conceptual deadlock and move beyond traditional debates on security as a contested concept. The reason for perceiving climate security as a global public good resides in the fact that while sources of insecurity are worldwide produced and its effects are far-reaching in their nature, the provision of stable climate patterns (*i.e.*, climate security) needs to be globally shared as well.

As there is no global government in charge of providing global public goods and no actor can do it on its own, the argument pursued in this paper is that only security governance is able to do so: an arrangement where institutional actors *below* (regional and local) and *above* (international) the state, under a broad institutional framework, may combine formal and informal dynamics in the production of climate security. To capture this reality in further detail, the paper assumes MLG I as a framework for climate secu-

rity governance based on vertical coordination among public actors at the international, national, regional and local levels who autonomously act towards the reduction of GHG, under an institutionally coordinated mandate led by central states.

As a final note, the presented framework is by no means distant or abstract considering that the Paris Agreement has, in 2015, taken its first steps towards the adoption of such model of climate action. After all, climate change is a phenomenon that is shaping, in various ways, traditional concepts, ideas and the world itself.

References

Aldecoa, F., and Keating, M., 1999. *Paradiplomacy in Action: The Foreign Relations of Sub-state Governments*. New York: Routledge.

Balwin, D., 1997. The Concept of Security. *Review of International Studies*, 23 (1), pp.52.

Barnett, J., 2000. Destabilising the Environment-conflict Thesis. *Review of International Studies*, 26 (2), pp.271-288.

Barnett, J., 2003. Security and Climate Change. *Global Environmental Change*, 13 (1), pp.7-17.

Barnett, J., and Dovers S., 2001. Environmental Security, Sustainability and Policy. *Pacifica Review*, 13 (3), pp.157-169.

Betsill, M., and Bulkeley, H., 2004. Transnational Networks and Global Environmental Governance: The Cities for Climate Protection Program. *International Studies Quarterly* 48 (2), pp.471-493.

Betsill, M., and Bulkeley, H., 2006. Cities and the Multilevel Governance of Global Climate Change. *Global Governance* 12 (2), pp.141-159.

Brown, L., 1989. Redefining National Security. *Worldwatch Paper* 14, pp.2-46.

Brown, M. D., 2012.Comparative Climate Change Policy and Federalism: An Overview. *Review of Policy Research* 29 (3), pp.322-333.

Brown, N., 1989. Climate, Ecology and International security. *Global Politics and Strategy* 31 (6), pp.519-532.

Busby, J., 2007. *Climate Change and National Security: An Agenda for Action*. New York: Council on Foreign Relations Press.

Buzan, B., and Hansen, L., 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Cottier, T., and Ahmad. Z., 2021. *The Prospects of Common Concern of Humankind in International Law*. Cambridge: Cambridge University Press.

Dalby, S., 2013. Global Environmental Security. In: R. Falkner, ed. 2013. *The Handbook of Global Environmental Climate and Environmental Policy*. New Jersey: John Wiley & Sons, pp.163-178.

Deere-Birkbeck, C., 2009. Global Governance in the Context of Climate change: The Challenges of Increasingly Complex Risk Parameters. *International Affairs* 85 (6), pp.1173-1194.

Dower, N., 1995. Peace and Security: Some conceptual Notes. In: Salla, M., Tonetto, W., Martinez, E., eds. 1995. *Essays on Peace: Paradigms for Global Order*. Rock-hampton: Central Queensland University Press, pp.18-23.

Ehrhart, H. Hegemann, H. and Kahl, M., 2014. Putting Security Governance to the Test: conceptual, empirical, and normative challenges. *European Security* (2), pp.119-125.

Falkner, R., 2013. The Nation-State, International Society, and the Global Environment. In: R. Falkner, ed. 2013. *The Handbook of Global Environmental Climate and Environmental Policy*. New Jersey: John Wiley & Sons, pp.251-267.

Falkner, R., 2016. The Paris Agreement and the New Logic of International Climate Politics. *International Affairs* 92 (5), pp.1107-1125.

Floyd, R., 2008. The Environmental Security Debate and its Significance for Climate Change. *The International Spectator* 3 (3), pp.51-65.

Gleditsch, N., 2001. Armed conflict and the Environment. In: P. Diehlm, and N. Gleditsch, ed. 2001. *Environmental Conflict: An Anthology*. New York: Routledge, pp. 251-272.

Goodman, S., 2007. National Security and The Threat of Climate Change. *The CNA Corporation*, [online] Available at: https://www.cna.org/archive/CNA_Files/pdf/national%20security%20and%20the%20threat%20of%20climate%20change.pdf. [Accessed 1 January 2022].

Hale, T., 2016. All Hands on Deck: The Paris Agreement and Nonstate Climate Action. *Global Environmental Politics* 16 (3), pp.12-22.

Hoffmann, M., 2013. Global Climate Change. In: R. Falkner, ed. 2013. *The Handbook of Global Environmental Climate and Environmental Policy*. New Jersey: John Wiley & Sons, pp 3-18.

Hooghe, L., and Marks, G., 2003. Unraveling the Central State, but How? Types of Multilevel Governance. *American Political Science Review* 97 (2), pp.233-243.

Hulme, M., 2001. You've Been Framed. *The Conversation*, [online] Available at: http://theconversation.edu.au/youve-been-framed-six-new-ways-to-understand-climate-change-2119. [Accessed 21 October 2022]

Jagers, S., and Johannes, S., 2003. Climate Governance Beyond the State. *Global Governance* 9 (3), pp.385-399.

Kaul, I., 2012. Global Public Goods: Explaining their underprovision. *Journal of International Law* 15 (3), pp.729-750.

Kaul, I., Grunberg, I., and Stern, M., 1999. *Global Public Goods: International Cooperation in the 21st Century*. New York: Oxford University Press.

Krahmann, E., 2003. National, Regional and Global Governance. *Global Governance* 9 (3), pp.23-346.

Krasner, S.D., 1982. *International Regimes*. New York: Cornell University Press.

Krause, K. and Williams, C. M., 1996. Broadening the Agenda of Security Studies: Politics and Methods. Mershon International Studies Review (40 (2), pp.229-254.

McDonald, M., 2018. Climate Change and Security: Towards Ecological Security? *International Theory* 10 (2), pp.153-180.

Newell, P., 2013. Globalization. In: R. Falkner, ed. 2013. *The Handbook of Global Environmental Climate and Environmental Policy*. New Jersey: John Wiley & Sons, pp.163-178.

Page, E., 2013. Climate Change Justice. In: R. Falkner, ed. 2013. *The Handbook of Global Environmental Climate and Environmental Policy*. New Jersey: John Wiley & Sons, pp.231-247.

Prins, G., and Rayner, S., 2007. Time to Ditch Kyoto. *Nature* 449, pp.973-975.

Rogers, P., 2010. *Losing Control: Global Security in the 21st Century*. London: Pluto.

Rosenau, J., 1992. Governance, Order, and Change in World Politics. In: J. Rosenau, and E. Czempiel, ed. 1992. *Governance without Government: Order and Change in World Politic*. Cambridge: Cambridge University Press, pp.1-29.

Rosenau, J., 1997. *Along the domestic-foreign Frontier: Exploring Governance in a Turbulent World*. Cambridge: Cambridge University Press.

Rosenau, J., 2007. Governing the Ungovernable: The Challenge of a Global Disaggregation of Authority. *Regulation & Governance* 1 (1), pp.88-97.

Samuelson, A. P., 1954. The Pure Theory of Public Expenditure. *The Review of Economics and Statistics* 36 (4), pp.387-389.

Shaw, B., 1996. When are Environmental Issues Security Issues? *Woodrow Wilson Center Environmental Change and Security Project Report* 2, pp.39-44.

Steffen, B., 2013. Strengthening the United Nations. In: R. Falkner, ed. 2013. *The Handbook of Global Environmental Climate and Environmental Policy*. New Jersey: John Wiley & Sons, pp.220-338.

Stripple, J. and Stephan, H., 2013. Globalization. In: R. Falkner, ed. 2013. *The Handbook of Global Environmental Climate and Environmental Policy*. New Jersey: John Wiley & Sons, pp.146-162.

Uitto, J., 2016. Evaluating the Environment as a Global Public Good. *Evaluation* 22 (1), pp.108-115.

Ullman, R., 1983. Redefining Security. *International Security* 8 (1), pp.129-153.

United Nations, 2015. *Paris Agreement*.

Walt, S., 1991. The Renaissance of Security Studies. *International Studies Quarterly*, 35 (2), pp.211-39.

Webber, M., Croft, S., Howorth, J., Terriff, T., and Krahamann, E., 2004. The Governance of European Security. *Review of International Studies* 30, pp.3-26.

Capítulo III

DEFESA NACIONAL: CONTEXTOS, POLÍTICAS E ATORES

O Combate às Alterações Climáticas pelos Órgãos de Defesa Nacionais e Europeus

Constança José Almeida de Queirós
Hugo Alves Quarteu
Joana Pereira Pires
Maria Francisca Veloso Volta

Alterações Climáticas: uma questão de defesa

As alterações climáticas refletem-se em diferenças estatísticas em diversas variáveis meteorológicas, como a temperatura, a precipitação, o nível do mar, etc., registadas num longo período de tempo. O aumento da temperatura média no planeta, comummente chamado aquecimento global, provocado pela emissão de gases com efeito de estufa, é um dos sintomas dessas mesmas alterações. Esta situação, que traz como consequências, também, a maior frequência e gravidade dos fenómenos meteorológicos extremos (secas, vagas de calor, incêndios florestais, inundações, entre outros), afigura-se como uma ameaça global, embora o risco seja maior para algumas partes do mundo. Este é o caso de Portugal, cujas particularidades geográficas constituem vulnerabilidades num contexto de crise climática, tornando-a um problema da Defesa Nacional, ameaçando o território português e a sua população.

Efetivamente, pela posição costeira do país, tanto o continente como os arquipélagos se encontram vulneráveis ao aumento do nível das águas do mar. Para além disso, os estudos preveem, num cenário de 1.5 °C de aquecimento global, uma situação de escassez de água para a região sul da Europa. De facto, Portugal já tem vindo a sentir as consequências das alterações climáticas, verificando-se temperaturas crescentemente elevadas e longos períodos de seca durante a época do verão, que se traduzem num problema de incêndios florestais. Estes, por sua vez, agravam a ocorrência e dimensão de cheias e inundações provocadas pelas precipitações extremas, também elas um sintoma das alterações climáticas. Estão também previstas, neste contexto, dificuldades na produção agrícola e perturbações nos ecossistemas terrestres e marinhos. Finalmente, em todos os casos, é de se esperar um aumento na mortalidade e na morbilidade.

É neste sentido que o *Conceito Estratégico de Defesa Nacional 2013* (CEDN, 2013) aponta os "riscos de natureza ambiental" como "principais riscos e ameaças à segurança global" – referindo-se às possíveis migrações em massa que advêm da degradação da qualidade da água e da sua disponibilidade, da degradação das terras para produção agrícola, e consequente perda de alimentos, e ainda dos já citados fenómenos.

Portugal e a União Europeia no combate à crise climática

Para além disso, Portugal vê-se influenciado e afetado pelos acontecimentos ao redor do globo, nomeadamente pela sua participação na NATO e na União Europeia. Assim, e tendo em conta que os fenómenos meteorológicos extremos e as restantes consequências das alterações climáticas já se afiguram como importantes causas de conflito e crises geopolíticas, Portugal ver-se-á obrigado a fazer um maior destacamento das Forças Armadas para operações de resolução dos mesmos. Neste sentido, e no contexto da Presidência Portuguesa do Conselho da União Europeia em 2021, o combate às alterações climáticas foi estabelecido como uma das principais prioridades na ação da União, pelo que se teve como objetivo trazer de volta, à agenda da Política Comum de Segurança e Defesa (PCSD), o foco no impacto das mudanças climáticas, e na prevenção e mitigação dos efeitos das futuras crises provocadas por essas mesmas mudanças.

O Instituto da Defesa Nacional divulgou, em 2021, um *brief* a analisar o roteiro publicado, anteriormente, neste contexto, pelo Serviço Europeu de Ação Externa (EASS), o qual será abaixo mais amplamente descrito, acerca desta relação entre as alterações climáticas e a defesa, bem como a necessidade de ter essa mesma relação em conta na Presidência Portuguesa do Conselho da União Europeia. Nesse documento, assinado pelo assessor do IDN, Carlos Coutinho Rodrigues, sublinha-se a incompreensão que os decisores políticos e os órgãos de apoio à decisão e de planeamento estratégico apresentam face às consequências das mudanças climáticas e às operações, recursos e infraestruturas necessárias no futuro que estas implicam. De facto, a maior frequência e intensidade desses eventos acarreta consequências para a PCSD, que passa a ter de ser planeada diferentemente e fica afetada no desenvolvimento das suas capacidades militares. O *brief* alerta ainda para perigos como o agravamento de tensões já existentes e o surgimento de extensos territórios inóspitos em que, com o Estado impossibilitado de exercer o seu controlo, ganham poder grupos ligados ao tráfico e ao crime organizado, o que, por sua vez, significa um grande fardo para as Forças Armadas dos Estados-membros da União Europeia, que ficaram encarregues de solucionar estas crises complexas.

Para além disto, os conflitos e as crises que surgem neste contexto diferem dos tradicionais e pressupõem operações em condições climáticas extremas e, consequentemente, mais perigosas à condição biológica humana, que carecem de uma preparação adicional e de tecnologia mais eficiente. O *brief* em questão apontava, aliás, para uma infraestrutura militar energeticamente ineficiente, o que remete para a necessidade de aumentar a resiliência energética e a eficácia operacional, bem como reduzir as emissões das operações da PCSD.

Destaca-se ainda que, uma vez que as alterações climáticas são um assunto global, as ações a tomar para as reverter devem ser também elas globais, e não apenas regionais. É por isto que a União Europeia tem procurado apresentar uma resposta conjunta e uma ação coerente de todos os Estados-membros. No entanto, o European Green Deal destaca a necessidade de estabelecer uma ação conjunta a par das restantes organizações internacionais e parcerias multilaterais, nomeadamente a ONU e a OTAN, e bilaterais

(com países parceiros). É também apontada a importância de planear as ações a curto, médio e longo prazo, assegurou o roteiro supracitado.

Estes documentos denotam então, para toda a UE, e particularmente para Portugal, tendo em conta o CEDN 2013, a necessidade de desenvolver a capacidade de agir para prevenir e responder aos acontecimentos que se colocam no contexto das alterações climáticas.

Mais recentemente, em setembro de 2022, o *IDN Brief* foi subordinado ao tema "Segurança, Sustentabilidade e Autonomia Energética da Europa", aprofundando aquela que foi a temática desenvolvida numa conferência online a 15 de junho pelo IDN. Este *brief* conta já com os impactos da guerra russo-ucraniana – assinala-se, por exemplo, a necessidade de desenvolver as energias renováveis, tendo em conta a rutura com o principal fornecedor energético da Europa. No entanto, as tecnologias necessárias ao desenvolvimento de energia verde trazem também os seus dilemas, nomeadamente a concorrência e a disputa pelos recursos necessários (como o cobalto). O *brief* aponta, também, para as dimensões que se associam ao abastecimento energético (climática, económica e securitária), referindo a redução e o abandono dos combustíveis fósseis, conforme pressupõe a Lei Climática Europeia. A ação que tem vindo a ser tomada, no sentido de alcançar este objetivo, traduz-se a nível da regulação e do investimento e acabou por ser acelerada pela guerra na Ucrânia, tendo-se verificado a dependência energética da UE. É, pois, nesse contexto que se encaixa o plano REPowerEU, apresentado pela Comissão, que tem como fim reduzir a importação dos combustíveis fósseis russos, apostando nas energias renováveis e no aumento da eficiência energética. Fica, portanto, exposta (através do contexto geopolítico atual e da apresentação deste tema no referido *brief*) a necessidade de considerar todas as implicações que a energia tem, não separando os domínios supracitados do clima, segurança e economia. Numa parte final, da autoria de Carlos Coutinho Rodrigues, o *IDN Brief* foca-se na relação entre a energia e a defesa, e alerta para o investimento na ciência e na inovação, bem como para a inclusão das questões ambientais no contexto da Lei de Programação Militar.

No entanto, apesar da provada necessidade de uma ação, no presente, para mitigar os efeitos das alterações climáticas e da prioridade que estas têm assumido nos diversos documentos e legislação já referidos, pode-se apontar uma falta de referências concretas ao CEDN 2013 ao longo dos quase 10 anos desde a sua publicação. Ainda assim, ações têm sido tomadas, mas sobretudo porque a União Europeia tem vindo a defini-las como prioridades. De facto, a política adotada , neste âmbito, por Portugal depende das linhas definidas pela UE.

Ainda no âmbito da União Europeia, e antes de passar às ações concretas, importa mencionar o evento virtual: "Climate Change, Defence and Crisis Management: from Reflection to Action" (Alterações Climáticas, Defesa e Gestão de Crises: da Reflexão à Ação). Este teve lugar em 2020 e foi organizado, conjuntamente, pelo Instituto de Estudos de Segurança da União Europeia (EUISS) e pelo Serviço Europeu de Ação Externa (EEAS). Foi neste evento que o Alto Representante Josep Borrell apresentou o supraci-

tado roteiro, "Climate Change and Defense Roadmap", que conta com medidas concretas a tomar, não só para gerir as consequências das alterações climáticas, mas também no sentido de consciencializar a população para a problemática, de preparar as Forças Armadas para lidar com os eventos que surgirão, de estabelecer parcerias para assegurar a segurança na gestão desses mesmos eventos e, finalmente, de garantir o cumprimento dos objetivos do Acordo Verde Europeu. As medidas apresentadas por este roteiro dividem-se em três áreas-chave: a dimensão operacional (mais envolvida na consciencialização e prevenção), o desenvolvimento de capacidades (que visa garantir a eficiência militar e a segurança energética face aos desafios futuros) e a abordagem diplomática (nomeadamente na procura de novos parceiros, incluindo as Nações Unidas e a NATO, para lidar com a crise climática).

Ação da União Europeia quanto às alterações climáticas

Reunião do Conselho Europeu de 2019 – conclusões e Pacto Ecológico Europeu

O Conselho Europeu deixou definido, em 2019, o objetivo de alcançar o impacto climático neutro até 2050 (Conclusões da Reunião do Conselho Europeu a 12 de dezembro de 2019, ponto 1 do tópico das alterações climáticas), o que implica uma redução da emissão de gases com efeito de estufa e compensação daquelas que se revelam incontornáveis. O organismo prevê que isto, através de estratégias inovadoras baseadas em investigação e desenvolvimento, beneficie o crescimento económico, emprego, mercados comerciais e desenvolvimento tecnológico dos Estados-membros (ponto 2). A par disto, explica-se igualmente a criação de um plano de transição – "quadro facilitador" – que permita que esta transformação contemple a contenção de custos e equidade social, e que seja adequado às especificidades de cada país (ponto 3).

Esta ação precisará de englobar uma totalidade do setor o que será possibilitado por um significativo investimento tanto público como privado. Tal implica também alterações no orçamento europeu de 2021–2027, projetando-se que no mínimo 30% deste seja canalizado para projetos da área, desta forma demonstrando o enfoque na neutralidade ambiental. O financiamento restante será coberto pelo Plano de Recuperação do Next Generation EU.

Este objetivo implica a verificação de políticas coordenadas em todos os Estados, o que pode levar a ajustes legislativos por parte da Comissão, relativamente a ajudas e acordos estatais, a par de relatórios focados nas consequências sociais, económicas e ambientais que a "neutralidade climática" comporta. Note-se o conjugar desta última questão com a competitividade da união (ponto 7). Entre medidas que contribuam para a redução da pegada de carbono, menciona-se a criação de um engenho capaz de controlar as emissões de CO_2 nos setores mais poluentes, sendo que as infraestruturas de países terceiros colaboradores deverão seguir estritas regras de segurança ambiental, estabelecidas no sistema internacional. Por outro lado, levanta-se a questão da energia nuclear e do seu papel no panorama económico de alguns países (ponto 6).

Estas propostas estão sob a alçada daquele que é conhecido como o Pacto Ecológico Europeu. A entidade supra-estatal europeia prevê que a transição para a utilização da energia verde possa significar uma terceira revolução industrial, capaz de criar mercados de produtos e tecnologias verdes. Com isto, estima-se a criação de 160.000 novos postos de trabalho e a renovação de 35 milhões de edifícios. De forma a evitar concorrência desigual vinda de países terceiros, propõe-se que estes estejam sujeitos ao pagamento de uma taxa de carbono quando exportando para a União Europeia. O passo mais recente tomado no sentido deste objetivo deu-se em outubro de 2022, altura em que o Parlamento e Conselho Europeu chegaram a um acordo provisório e mais concreto quanto às emissões de CO_2 de novos automóveis. Em 2030, espera-se que haja uma redução do nível de emissão de dióxido de carbono de pelo menos 55% em relação à década de 1990, e em 2050 a neutralidade climática.

Acordo de Paris e política externa ambiental da UE

O Acordo de Paris – tratado internacional a respeito do problema global das alterações climáticas – foi assinado em 2015 por vários líderes mundiais e apresenta um conjunto de medidas e objetivos que permitem travar o aquecimento global (especificamente, procurando evitar que a temperatura média global suba mais de 2ºC). Nesta conferência cada Estado apresentou um plano de ação nacional – também conhecido como NDC – Nationally determined contribution – que deve ser revisto a cada cinco anos, e comprometeu-se a manter uma postura de transparência informacional quanto à questão. De apontar, também, o papel que os países desenvolvidos assumiram, prestando apoio financeiro aos países em vias de desenvolvimento neste âmbito. Esta contribuição monetária é focada no fenómeno de mitigação da emissão de gases, conseguida através de grandes investimentos, e na adaptação das infraestruturas e tecnologias. Todos os países da União Europeia ratificaram o acordo que viria a vigorar a partir de 4 de novembro de 2016. Atualmente, as alternativas verdes estão a ganhar competitividade no mercado energético, representando 25% do total mundial das emissões. Em 2030, espera-se que este número cresça até aos 70%, no entanto este esforço está, mais recentemente, em risco perante o cenário internacional atual, que realoca as atenções para o plano da segurança estatal.

Objetivos climáticos e política externa da UE

A UE representa 8% das emissões globais de gases de estufa, pelo que a ação interna no combate às alterações climáticas é complementada com a sua política externa. Nas relações bilaterais que estabelece, o organismo de integração procura fazer do clima um tema central, onde a partilha de conhecimentos e apoio financeiro e científico são priorizados. Em congruência com este cenário, elabora-se a proposta de Lei Europeia do Clima.

Proposta de Lei Europeia do Clima

A Comissão Europeia anunciou esta nova Estratégia da UE, onde destaca a matéria de adaptação às alterações climáticas na sua Comunicação sobre o Pacto Ecológico Europeu, na sequência de uma avaliação da Estratégia de 2013, realizada em 2018, e de uma consulta pública efetuada entre maio e agosto de 2020. A proposta de Lei Europeia do Clima lança as bases para um reforço das políticas alinhadas em matéria de adaptação. Isto é, a proposta integra, no Direito da UE, o objetivo global em matéria de adaptação previsto no artigo 7.º do Acordo de Paris e a ação a título do Objetivo de Desenvolvimento Sustentável n.º 13. Nos termos da proposta, a UE e os Estados-membros deverão realizar progressos contínuos para aumentar a capacidade de adaptação, reforçar a resiliência e reduzir a sua vulnerabilidade às alterações climáticas. A nova estratégia de adaptação contribuirá para que estes progressos se tornem realidade. Paralelamente, não são referidos subtópicos concretos que cada Estado deva assumir o compromisso de adotar, o que faz com que, em certa medida, o documento fique aberto a interpretações subjetivas dos governos nacionais, podendo, em última instância, dar azo a diferentes procedimentos e políticas, em vez de uma ação coesa.

Climate-ADAPT

O Climate-ADAPT- em português, a Nova Estratégia da UE para a adaptação para as alterações climáticas – é uma estratégia que entrou em vigor em fevereiro de 2021. Esta plataforma deriva do Pacto Verde Europeu (2019), do documento inicial EU Adaptation Strategy (2013) e da subsequente avaliação do mesmo em 2018, e de uma consulta ao público entre maio e agosto de 2020. Assim, visa uma adaptação sistémica e internacional às novas condições climatéricas através de um conjunto de medidas a serem implementadas globalmente, não só pelos Estados-membros europeus, como também pelos Estados terceiros com que estes se relacionam na arena internacional. Os quatro objetivos principais subdividem-se em 14 pontos, todos focados na adaptação de meios e costumes para a diminuição do risco ambiental, e em garantir a potabilidade da água e a segurança das populações em todos os níveis socioeconómicos e em todos os setores da economia. Identifica-se ainda a prioridade da adaptação ser feita ao nível local, com soluções de base natural, e de ser integrada no cenário da política macro fiscal da União Europeia. No plano internacional, a política externa passará por um auxílio reforçado aos países, com provisão de recursos, mais injeção fiscal, e um diálogo sobre troca de informações e meios a nível global.

The EU's Climate Change and Defense Roadmap

Em março de 2022, foi publicado o documento The EU'S Climate Change and Defence Roadmap – Addressing the Implications of Climate Change for Security and Defence, no âmbito do Pacto Ecológico Europeu. Do ponto de vista da análise política, a justificação dada para a elaboração deste guia prende-se com o facto de as alterações climáticas representarem uma nova e imprevisível categoria de ameaça à paz e segurança

a nível nacional e internacional, nomeadamente o aumento da instabilidade em fenómenos como o aumento dos níveis da água do mar ou as secas. A maior frequência destes eventos é diretamente proporcional à maior necessidade de intervenção das Forças Armadas junto da sociedade civil, prestando auxílio no combate a fogos florestais, cheias, etc. Adicionalmente, refere-se que as infraestruturas terão de ser reestruturadas, de forma a estarem adaptadas a um ambiente em constante mutação. Mais uma vez, esta noção estende-se ao corpo do exército, que terá também de investir em tecnologias mais ecológicas, de tal modo que estas constituam a base da sua capacidade de inventário e de estrutura.

O projeto consiste em 30 medidas nas áreas das infraestruturas, indústria, tecnologia, desenvolvimento e pesquisa na defesa do território. Como anteriormente referido, estas estão inseridas em parcerias, dimensão operacional e desenvolvimento de capacidades. No que toca a parcerias, a cooperação com a NATO, Nações Unidas e parceiros bilaterais permite uma ação coesa e global no sentido de encontrar e internacionalizar soluções. Denota-se a atenção colocada no papel das Forças Armadas na prossecução dos pontos, tanto a nível do desenvolvimento de capacidades como da dimensão operacional. Com efeito, para que o plano alcance o seu fim, deverá haver uma "cooperação cívico-militar" que ajude a preparar respostas para eventuais catástrofes naturais e humanas. Para além disso, mencionam-se 133 milhões de euros canalizados para o desenvolvimento de tecnologia e equipamento de defesa mais eficazes e menos dependentes de combustíveis fósseis, melhoria dos meios de transporte dos corpos de proteção, estudos sobre os gastos dos mesmos e consequente reajustamento.

Finalmente, é deixada a indicação de que os grupos militares dos 27 Estados-membros usam atualmente a energia equivalente àquela que seria esperada de um Estado-membro de pequena dimensão. Ora, com todos estes dados, é possível sugerir que a criação do hipotético exército europeu – ideia apoiada por 55% dos europeus, segundo o estudo especial do Eurobarómetro sobre segurança e defesa em 2017 – seria benéfica, se o mesmo se viesse a encarregar de missões ligadas à sensibilização, preparação e combate às alterações climáticas nos Estados. Adicionalmente, a criação deste corpo viria a demonstrar-se como uma possível solução acima apresentado no *brief* do IDN de 2021, pois poderia encarregar-se de mitigar as eventuais ascensões ao poder de grupos ligados ao narcotráfico, naqueles países em que a posição de influência do governo se visse diminuída.

Ação do Governo Português

Projeto LIFESHARA

O projeto LIFESHARA "Sensibilização e conhecimento para a adaptação às alterações climáticas" teve como objetivo o reforço da governação em relação às mudanças criadas pelas alterações climáticas e a melhoraria da capacidade de resistência na Península Ibérica. Com um orçamento de 1,5 milhões de euros e uma duração de cinco anos, o projeto terminou em outubro de 2021.

Este fez aumentar o conhecimento sobre o tema através da comunicação, consciencializando a população sobre as mudanças que devem ser feitas. Para isso, deu-se o reforço da coordenação entre os agentes, promovendo seminários sobre setores particularmente vulneráveis e estabelecendo a cooperação entre Portugal e Espanha para identificar prioridades e ações comuns. A promoção de acordos público-privados para a adaptação do setor privado foi igualmente incentivada.

Em forma de conclusão das atividades do LIFESHARA, decorreu em novembro de 2021 uma conferência que contou com a presença de ministros dos dois países. Foi um evento para dialogar, trocar experiências e boas práticas entre toda a população. O encontro permitiu o reforço da cooperação para avançar no combate à crise climática.

Roteiro Nacional para a Adaptação 2100 – Avaliação da vulnerabilidade do território português às alterações climáticas no século XXI (RNA 2100)

O Roteiro Nacional para a Adaptação 2100 tem como função a definição de medidas para a evolução das vulnerabilidades territoriais e humanas e os impactos das alterações climáticas, assim como analisar as necessidades de investimento e precisar os custos socioeconómicos da inatividade. O projeto pretende responder a exercícios de política pública; já os seus organizadores esperam que este atue de forma a consciencializar e educar para a mudança de comportamentos relativos às alterações climáticas.

Tendo os últimos estudos sobre as referidas vulnerabilidades sido realizados em 2002 e 2006, foi necessário voltar a fazer investigações a nível nacional e regional para garantir a resiliência socioecológica do território português.

No decurso da realização do Programa de Ação para a Adaptação às Alterações Climáticas (P-3AC), identificou-se os impactos e vulnerabilidades mais proeminentes, nomeadamente o aumento da periodicidade e da intensidade dos incêndios rurais, a evolução das ondas de calor, o aumento da desertificação, os períodos de seca e a escassez de chuva, as cheias, a subida do nível das águas do mar e a intensidade dos fenómenos extremos. Posto isto, o P-3AC procura expor os impactos sociais e económicos que não são estudados de maneira eficiente e que exigem a criação de metodologias adequadas.

O projeto apoiará, então, as ações da Estratégia Nacional de Adaptação às Alterações Climáticas (ENAAC 2020); contribuirá para a implementação do PNPOT, na caracterização e cartografia dos territórios mais suscetíveis aos fenómenos extremos; e terá um papel público e mediático nas ações de comunicação e sensibilização deste tema.

A mudança de mentalidade ambiental coletiva tem de ser completada com a criação de medidas concretas, que possam ser postas em prática. O projeto começou em 2020 e prevê o fim da sua atuação em 2023, pelo que ainda resta algum tempo para se manifestarem consequências concretas.

O papel do Ordenamento do Território na mitigação e adaptação às Alterações Climáticas

O ordenamento do território tem um papel no combate às alterações climáticas, isto porque os usos e ocupações do solo têm impactos no clima, e as alterações climáticas, por sua vez, terão influência nas futuras utilizações dos solos.

Segundo Susana Gomes (2017), é necessário promover uma diminuição do grau de exposição às alterações climáticas e, ao mesmo tempo, desenvolver capacidades para reduzir as situações que as geram. Na opinião de vários autores (Füssel, 2007; Biesbroek et al., 2009) isto pode ser conseguido através da proatividade, isto é, atuar antes que as catástrofes aconteçam, pois é mais económico e seguro do que lidar com as consequências que destas advêm.

As ações devem ser estruturadas e desenvolvidas de maneira a que a sua praticabilidade seja simples. A mitigação das alterações climáticas deve também ser complementada por uma estratégia de adaptação (Hurlimann e March, 2012). No entanto, apesar de referida em várias políticas nacionais e internacionais, ainda não se encontra integrada nas práticas de planeamento municipal.

A elaboração do projeto de adaptação climática compreende duas aplicações diferentes: por um lado, a ação reativa, que tem lugar depois do evento; por outro, a ação de antecipação. A adaptação deve determinar medidas para os dois casos, isto é, se eventualmente a ação de antecipação não resultar no processo de assimilação dos efeitos provocados pelo fenómeno climático, o plano tornar-se-á elaborar linhas de ação reativas, não descurando os planos de emergência municipais.

Em relação à mitigação, a redução dos gases com efeito de estufa é a medida principal. Todavia, a relação entre esta e o ordenamento do território pode não ser clara. A lógica é que uma infraestrutura verde é notória pela capacidade de eliminar o dióxido de carbono da atmosfera; como tal, definir usos do solo que aumentam as áreas verdes e permeáveis promove a mitigação. No entanto, Portugal tem uma limitação que afeta muito a sua ação, e que se relaciona com o modo arcaico, muito estático, como o país continua a introduzir estas estratégias (Torres e Pinho, 2011).

Assim sendo, o planeamento de mitigação das alterações climáticas representa um tópico da agenda dos governos locais, pois torna-se necessário fazer uma inventariação das emissões de gases com efeitos de estufa e um estudo de projeções de impactos locais.

No que diz respeito à ação que pode ser posta em prática, as medidas de mitigação relacionadas com o ordenamento de território passam pela redução da distância entre os locais de residência e os locais de trabalho; a criação de um estrutura de transportes públicos consistente e eficiente, impondo um limite à dispersão urbana; o desenvolvimento das energias renováveis, com a criação de parques de produção de fontes renováveis e estabelecendo um plano de transição do tipo de energia dos edifícios e dos espaços públicos; e por último, mas não menos importante, a revalorização e proteção dos ecossistemas e a criação de espaços verdes (Pinto; 2014).

Por sua vez, as medidas de adaptação devem ter em conta os riscos de incêndio, ondas de calor e seca, inundações, ponderando os seus impactos e salvaguardando as

pessoas e os seus bens; os novos edifícios e os espaços públicos têm de ser planeados de forma a que sejam resistentes às alterações climáticas, nomeadamente ondas de calor; é imperativa a criação de Estruturas Ecológicas Municipais e Urbanas e uma gestão competente dos recursos hídricos (Pinto; 2014).

O que resta fazer

A Ferrovia como alternativa ecológica

A Revolução Industrial aproveitou o potencial energético dos combustíveis fósseis, desde o carvão ao petróleo e gás natural, apropriando-se destes para o desenvolvimento das diversas indústrias de mercadorias, assim como de transportes. A invenção e subsequente produção em massa dos meios de transporte trouxe ao mundo progresso, proximidade e um aceleramento do fenómeno de globalização. No entanto, esta indústria tem sido também um dos principais catalisadores do aquecimento global (Michaelis, 1993). Segundo estudos da Universidade Técnica Chalmers, localizada em Gotemburgo, na Suécia, a indústria dos transportes é responsável por sensivelmente 17% da totalidade das emissões de gases de efeito de estufa resultantes das atividades humanas (Larsson e Kamb, 2019).

No entanto, os diferentes meios de transporte apresentam também diferentes níveis de impacto ecológico. De entre todos, destaca-se o comboio pelos seus reduzidos custos ambientais. Segundo os estudos de Chalmers, a estimativa de emissões de gases de efeito de estufa de uma viagem de comboio encontra-se no valor de 34 gramas de CO_2 por passageiro por quilómetro percorrido. Em comparação, o valor da estimativa para a viagem de carro é 63 gramas de CO_2 por passageiro, também por cada quilómetro. O contraste entre o comboio e outros meios de transporte como o avião (298), a balsa (170) ou a autocaravana (106) é ainda maior (Larsson e Kamb, 2019).

O comboio é, portanto, em comparação com os principais meios de transporte, aquele que apresenta um menor impacto ambiental no transporte de passageiros. Com o intuito de averiguar se a mesma conclusão poderia ser aplicada ao ramo do transporte de mercadorias, uma equipa de investigadores noruegueses dedicou-se a analisar a possibilidade e dimensão da diminuição de emissões de dióxido de carbono, no caso de 50% das mercadorias transportadas por camiões passarem a ser transportadas por comboios (Ager-Wick Ellingsen e Bjordal, 2021).

A distribuição da mercadoria total transportada por tipo de transporte, na Noruega, corresponde a: 46% por transporte marítimo, 49% por transporte rodoviário e apenas 5% por transporte ferroviário, segundo os dados de 2019 da Statistics Norway. O estudo em questão, realizado em 2021, focou-se no transporte de mercadorias entre as cidades de Oslo e Bergen.

Para averiguar a diferença entre os impactos ecológicos do transporte rodoviário e ferroviário, a equipa de investigadores analisou dois cenários distintos. No primeiro cenário, 50% da carga total atual transportada por camiões passaria a ser transportada

por comboios. No segundo cenário, todo o transporte terrestre de mercadorias passaria a ser efetuado pelos camiões. As emissões de ambos os cenários seriam medidas por um período de 30 anos. Os resultados do primeiro cenário demonstram que, após este período de três décadas, quase 300.000 toneladas de CO_2 seriam economizadas. Quanto ao segundo cenário, a quantidade de CO_2 libertada rondaria as 600.000 toneladas.

Segundo Ager-Wick Ellingsen, uma das autoras do artigo relativo ao estudo efetuado: "Seria definitivamente benéfico para o ambiente transferir mais mercadorias dos camiões para os comboios".

A situação atual da ferrovia norueguesa assemelha-se à portuguesa. Comparando com a fração de 5% de mercadorias transportadas por comboios na Noruega, em Portugal o valor é inferior, chegando a cerca de 4%, segundo os dados de 2019, conforme apresentados no Relatório do Estado do Ambiente. Quanto à quantidade de carga transportada por via marítima, os valores são maiores no país escandinavo do que no luso (46% e 34%, respetivamente). Assim, conclui-se também que a carga transportada pela rodovia é superior percentualmente em Portugal – cerca de 61% – comparativamente à Noruega – 49%.

Dadas as semelhanças entre os valores do peso da via ferroviária, no transporte de mercadorias, nos dois países, e tendo em atenção a maior utilização do transporte rodoviário de mercadorias em território português, os resultados do estudo podem ser projetados para a realidade de Portugal, assinalando ainda uma possibilidade de maior redução de emissões de CO_2 no cenário de transferência de 50% da carga transportada por camiões para comboios. Para além disso, Portugal apresenta também um valor inferior de transporte de passageiros por via ferroviária – 4,6% do transporte total – quando comparado com a média dos países da União Europeia – 8,1%. Estes resultados, é claro, representam emissões de gases de efeito estufa acrescidas.

Estes dados ilustram uma deficiência efetiva de investimento na via ferroviária portuguesa. De facto, Portugal é, em 2022, o único país da União Europeia que dispõe de uma rede de autoestradas mais extensa do que a ferroviária. Aliás, regista-se o contínuo investimento nas autoestradas de 1991 a 2011, em comparação com aquele efetuado para a malha ferroviária no mesmo período. Segundo a Pordata, a extensão total da rede de autoestradas passou de cerca de 500 km em 1991 para cerca de 3.000 km em 2011. A realidade da rede de ferrovia é distinta. No mesmo período, e apesar de a extensão total ter aumentado (de 3.546 km passou para 3.622 km), a linha ferroviária explorada diminuiu, passando de 3.117 km a 2.527 km.

Em suma, é importante considerar o investimento no desenvolvimento e expansão da ferrovia, na luta contra as alterações climáticas. De facto, tanto o transporte de passageiros, como o transporte de mercadorias são menos impactantes a nível ambiental quando realizados por comboios. Assim, na defesa do território e na preservação do bem-estar dos portugueses, a utilização da via ferroviária pode oferecer uma opção mais sustentável do que a rodovia.

A Indústria Pecuária e o Aquecimento Global

A indústria pecuária é um dos setores de atividade a registar maiores níveis de emissões de gases de efeito de estufa globalmente (Twine, 2021), equiparando-se mesmo a toda a indústria dos transportes. A contribuição deste setor de atividade resulta em cerca de 14,5% da totalidade da libertação destes gases, destacando-se pela emissão de gases como metano, que causam um efeito de estufa superior ao do dióxido de carbono. Trata-se, portanto, de um dos principais catalisadores (se não o principal catalisador) das alterações climáticas e dos fenómenos que a estas vêm ligados, como, por exemplo, a crise crónica dos incêndios florestais em Portugal (Lourenço e Cunha Lopes, 2004).

Segundo um estudo efetuado por investigadores da Universidade de Oxford em 2018, e publicado na revista *Science*, a pecuária é responsável por 60% da emissão de gases de efeito de estufa resultante da totalidade da atividade agrícola, apesar de produzir 18% das calorias e 37% das proteínas a nível mundial (Poore e Nemecek, 2018). No decorrer deste estudo, foram recolhidos dados de quase 40.000 explorações agropecuárias em 119 países. Após terem analisado uma variedade de 40 produtos alimentícios, sobre os quais se baseia 90% da alimentação mundial, os investigadores concluíram que os produtos com o maior custo ambiental de produção são as diversas carnes, incluindo as de peixe, assim como os laticínios. O estudo revela ainda que, deixando de consumir este tipo de produtos, poderemos reduzir o nosso consumo individual de carbono até 73%.

Para além da libertação direta de gases nocivos à vida na Terra, a pecuária exige a neutralização da tecnologia mais eficaz no combate ao aquecimento global, isto é, as árvores (Manning, 2020). As árvores, produzindo o seu alimento, consomem dióxido de carbono e libertam oxigénio, num processo conhecido como fotossíntese. Para além disto, são fulcrais para o equilíbrio dos ecossistemas, para a manutenção da biodiversidade, para a retenção de água, entre outros.

A causa destacada para a desflorestação global é a agricultura (Allen e Barnes, 1985). Segundo a Organização das Nações Unidas para a Alimentação e a Agricultura, todos os anos milhões de hectares de zonas florestais são transformados em campos agrícolas ou pastos para gado (26% da superfície terrestre). Destes campos agrícolas, um terço serve o propósito de produzir ração para a indústria pecuária, sendo consumidos pelos humanos indiretamente, ou seja, após processos que resultam em perdas do seu aproveitamento calórico e nutricional. O abandono do consumo de carnes ou laticínios permitiria a libertação e consequente reflorestação de 75% da área global reservada à atividade agrícola (Poore e Nemecek, 2018). Isto corresponde a uma área equivalente à soma dos territórios dos Estados Unidos da América, da China, da Austrália e dos países da União Europeia.

Segundo Joseph Poore, autor principal do artigo: "Uma dieta vegana (sem recurso ao consumo de produtos de origem animal) é provavelmente a maior forma de reduzir o seu impacto no planeta Terra, não apenas os gases com efeito de estufa, mas também a acidificação global, eutrofização, uso da terra e uso da água".

Em Portugal, o impacto da pecuária na constituição gasosa da atmosfera continua a crescer. Em 2022, a associação Zero chamou à atenção para as emissões de gases de

efeito de estufa no setor agropecuário, que, em contraste com a tendência geral das restantes indústrias, não só não atinge a meta de redução de emissões estabelecida para 2020 (uma redução de 8% em relação 2005), como demonstra um crescimento contínuo, tendo ultrapassado os valores de 2008 logo em 2017.

Deste modo, tendo em atenção a pressão que a pecuária exerce sobre o ambiente, em Portugal e em todo o mundo, importa considerar as implicações que esta indústria tem na saúde e na segurança do território, assim como analisar possibilidades para a redução do seu impacto, como a promoção da redução do consumo de produtos de origem animal, ou fiscalização restritiva desta área de produção.

Conclusão

Tendo em conta os diversos contornos que a questão das alterações climáticas assume e a forma como as suas consequências se fazem sentir nos diversos setores da vida, em particular no nosso país, torna-se evidente a sua ligação à defesa nacional e, como tal, a necessidade de tornar prioritárias todas as iniciativas e as políticas que visem prevenir o agravamento da atual situação e mitigar os efeitos da mesma.

Neste sentido, ações e alterações ao nível da legislação têm sido levadas a cabo, tanto no panorama português, como no contexto da União Europeia, levando a crer que existe, efetivamente, uma vontade comum de priorizar a ação climática e de liderar a transição ecológica no mundo, de forma a evitar o pior cenário traçado pelas previsões dos cientistas. Não obstante, a análise dos projetos e das iniciativas que se têm vindo a desenvolver, particularmente em Portugal, revela que os mesmos têm sido não apenas insuficientes, como também ineficazes, baseando-se numa abordagem teórica e de consciencialização que, embora importante, acaba por não significar a obtenção dos resultados práticos necessários.

Por outro lado, identificaram-se áreas que importa explorar no combate às alterações climáticas, destacando-se a importância dos setores do transporte e da agropecuária, pelo seu impacto na crise que atravessamos, e pela relativa escassez de ação desenvolvida até agora neste sentido.

Resta, portanto, investir e canalizar os esforços no sentido de desenvolver soluções mais práticas e eficazes para o problema global que se põe.

Referências

Ager-Wick Ellingsen, L. e Bjordal, K. (2021). LCA of freight transport track and road. *Asplan Viak*.

Allen, J.C. e Barnes, D.F. (1985). The Causes of Deforestation in Developing Countries. *Annals of the Association of American Geographers*, 75(2), pp.163–184. doi:https://doi.org/10.1111/j.1467-8306.1985.tb00079.x.

apambiente.pt. (n.d.). Projetos em Adaptação | Agência Portuguesa do Ambiente. [online] Available at: https://apambiente.pt/clima/projetos-em-adaptacao [Accessed Nov. 2022].

Biesbroek, G.R., Swart, R.J. e van der Knaap, W.G.M. (2009) *The mitigation–adaptation dichotomy and the role of spatial planning*.

Climate Change and Defence Roadmap. (2020). [online] p.13. Available at: https://data.consilium.europa.eu/doc/document/ST-12741-2020-INIT/en/pdf [Accessed Nov. 2022].

europa.eu. (n.d.). Eurobarometer. [online] Available at: https://europa.eu/e THE EU 'S CLIMATE CHANGE AND DEFENCE ROADMAP ADDRESSING THE IMPLICATIONS OF CLIMATE CHANGE FOR SECURIT Y AND DEFENCE. (2022). [online] Available at: https://www.eeas.europa.eu/sites/default/files/documents/2022-03-28-ClimateDefence-new-Layout.pdf [Accessed Nov. 2022].

European Commission (2019). *A European Green Deal*. [online] European Commission. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.

Füssel, H.-M. (no date) "Adaptation Planning for Climate Change: Concepts, Assessment Approaches and Key Lessons." Available at: https://www.researchgate.net/publication/215677053_Adaptation_Planning_for_Climate_Change_Concepts_Assessment_Approaches_and_Key_Lessons.

Gomes, S. (2017) *O PAPEL DO PLANEAMENTO URBANO NA MITIGAÇÂO DAS ALTERAÇÕES CLIMÁTICAS*. dissertation. Available at: https://repositorio-aberto.up.pt/bitstream/10216/108133/2/224102.pdf

Hurlimann, A.C. e March, A.P. (2012) *The role of spatial planning in adapting to climate change*.

Kamb, A. e Larsson, J. (2019). *Climate footprint from Swedish residents' air travel*. [online] Available at: https://research.chalmers.se/publication/508693/file/508693_Fulltext.pdf [Accessed 23 Feb. 2023].

Lourenço, L. e Cunha Lopes, N. (2004). Incêndios florestais, consequência e razão de ser de novas Mudanças Globais. *GeoLNova – Revista do Departamento de Geografia e Planeamento Regional*.

Manning, W.J. (2020). *Trees and Global Warming: The Role of Forests in Cooling and Warming the Atmosphere*. [online] Google Books. Cambridge University Press. Available at: https://books.google.pt/books?hl=pt-PT&lr=&id=x1DuDwAAQBAJ&oi=fnd&pg=PA1&dq=how+trees+reduce+global+warmth&ots=cSgb8VdIdw&sig=m0sa2-WHAPLQonc_47wAmU7ONXE&redir_esc=y#v=onepage&q=how%20trees%20reduce%20global%20warmth&f=false [Accessed 23 Feb. 2023].

Michaelis, L. (1993). Global warming impacts of transport. *Science of The Total Environment*, 134 (1-3), pp.117–124. doi:https://doi.org/10.1016/0048-9697(93)90344-6.

Pina, C., Pereira, L. e Alvarenga, M. (2019). O Ordenamento Do Território Na Resposta Às Alterações Climáticas. [online] Available at: https://www.ohchr.org/sites/default/files/2022-03/portugal-nhri-annex-I.pdf [Accessed Nov. 2022].urobarometer/screen/home [Accessed Nov. 2022].

Pinto, R.S.B.F.F. (2014) *O papel do ordenamento do território na adaptação às alterações climáticas no estuário do Rio Minho*. dissertation.

Poore, J. e Nemecek, T. (2018). Reducing food's environmental impacts through producers and consumers. *Science*, [online] 360(6392), pp.987–992. doi:https://doi.org/10.1126/science.aaq0216.

rna2100.apambiente.pt. (n.d.). Programa Ambiente, Alterações Climáticas e Economia de Baixo Carbono | rna2100. [online] Available at: https://rna2100.apambiente.pt/pagina/programa-ambiente-alteracoes-climaticas-e-economia-de-baixo-carbono [Accessed Nov. 2022].

Torres, M. e Pinho, P. (2011) "Encouraging low carbon policies through a Local Emissions Trading Scheme (LETS)."

"Transporte de Mercadorias | Relatório Do Estado Do Ambiente." Rea.apambiente.pt, 12 Nov. 2021, rea.apambiente.pt/content/transporte-de-mercadorias.

Twine, R. (2021). Emissions from Animal Agriculture—16.5% Is the New Minimum Figure. *Sustainability*, 13(11), p.6276. doi:https://doi.org/10.3390/su13116276.

United Nations (2017). UNFCCC. [online] Unfccc.int. Available at: https://unfccc.int/.

www.consilium.europa.eu. (n.d.). Objetivos climáticos e política externa da UE. [online] Available at: https://www.consilium.europa.eu/pt/policies/climate-change/climate-external-policy/ [Accessed 23 Nov. 2022].

www.eeas.europa.eu. (n.d.). *Towards a climate-proof security and defence policy: a Roadmap for EU action | EEAS Website*. [online] Available at: https://www.eeas.europa.eu/eeas/towards-climate-proof-security-and-defence-policy-roadmap-eu-action_en.

www.europarl.europa.eu. (2019). Defesa: está a UE a criar um exército europeu? | Atualidade | Parlamento Europeu. [online] Available at: https://www.europarl.europa.eu/news/pt/headlines/security/20190612STO54310/defesa-esta-a-ue-a-criar-um-exercito-europeu [Accessed Nov. 2022].

Capítulo IV

TRANSFORMAÇÃO DIGITAL E NOVAS TECNOLOGIAS MILITARES

Quando a Ciberconflitualidade Desafia as Regras Cinéticas – as Ciberoperações Militares e a Noção de Ataque Constante no Artigo 49.º do Primeiro Protocolo Adicional às Convenções de Genebra

Anabela Paula Brízido

1. Introdução, Delimitação do Objeto e Metodologia

1.1. Enquadramento

Literatura vária aponta para a importância da Sociedade da Informação cujo centro de gravidade é a informação. Ela constitui um importante ativo/valor passível de alienação, transmissão e troca[1]. Aceder-lhe e controlá-la é, por isso, sinónimo de poder, o que a torna, como se compreenderá, num alvo apetecível no ciberespaço, mesmo em situações de conflitualidade armada.

1.2. Delimitação do objeto

Elegemos, como questão principal, saber quais as operações de informação, nas operações militares[2], designadas por ciberoperações, suscetíveis de serem enquadradas na expressão de ataques constante no artigo 49.º/1 do I PA (I Protocolo Adicional) às CG (Convenções de Genebra). Neste particular importa, por isso, avançar conclusões e delimitar o objeto.

O preceito jurídico integra o I PA às CG cujo objeto é reger, nos termos do seu artigo 1.º/2/3/4, os CAI (conflitos armados internacionais), sendo a sua noção, por sua vez, posta pelo artigo 2.º comum às CG. pelo que, a nossa centralidade irá incidir sobre os CAI, em detrimento dos CANI (conflitos armados não internacionais).

O objeto do nosso estudo é, por isso, o DIH (Direito Internacional Humanitário),

1 Para as diferentes noções sobre sociedade da informação, remetemos para: WEBSTER, F. 2014. *Theories of the Information Society,* London, Routledge, Taylor & Francis Group.

2 NUNES, P. F. V. 2006. Operações de Informação: Enquadramento e Impacto Nacional. *Revista Militar*, s/pag.

cuja finalidade é, por um lado, proteger os civis, população civil, objetos civis – princípio da humanidade – em conflitos armados e, por outro lado, reger, ainda, a própria condução das hostilidades, ou seja, os meios e métodos a serem empregues – princípio da necessidade militar –, no caso, num CAI[3].

Por sua vez, a qualificação de dado conflito, em conflito armado e internacional assenta, por norma e com interesse para este trabalho, tem dois pressupostos: interestadualidade e componente armada. Se o primeiro atende à natureza de determinado sujeito – Estado –, já o segundo reconduz-se, perante uma determinada situação concreta, à verificabilidade de certa factualidade – conceito factual e objetivo – não estando, por isso, dependente do reconhecimento daquele estado de conflitualidade, pelas partes do conflito, como se depreende do artigo 2.º/1 comum às CG[4].

As ciberoperações militares quando executadas, no caso, em CAI no ciberespaço têm uma natureza anónima, ubíqua e sem fronteiras[5] o que as distinguem das operações convencionais. Por assim suceder, a doutrina colocou a seguinte questão: O Direito Internacional Público e o DIH, como sua *lex specialis*[6], regem o ciberespaço[7]?

Importa, neste contexto, esclarecer que partimos do pressuposto, por ser na atualidade doutrina pacífica, o Direito Internacional Público e o DIH regerem aquele espaço[8]. Por sua vez, encontramo-nos no campo do *jus in bellum* e, por isso, distinto do *jus ad bellum* em que o DIH se aplica independentemente das questões de licitude/ilicitude do uso da força[9].

Por sua vez, e apesar da natureza não cinética das ciberoperações, por integrarem o mundo virtual (do ciberespaço), e a violência, do mundo real, ser, na generalidade, associada à violência física e cinética, importa, todavia, esclarecer que a noção de conflito armado não é inconciliável, com o ciberespaço. Parte-se, por isso, do pressuposto que as

3 Para a noção de DIH e sem pretensão de exaustão PEREIRA, M. D. A. D. V. 2014. *Noções fundamentais de direito humanitário,* Coimbra, Coimbra.

4 Para a noção e qualificação de CAI: AKANDE, D. 2012. Classification of Armed Conflicts: Relevant Legal Concepts. *In:* WILMSHURST, E. (ed.) *International Law and the Classification of Conflicts.* Oxford: Oxford University Press, SCHMITT, M. N. 2013a. Classification of Cyber Conflict. *International Law Studies US Naval War College,* 89º, 233-251.

5 SCHMITT, M. 2018. Introduction. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

6 Parecer Consultivo do TIJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ; Reports 2004, p. 136.

7 BARLOW, J. P. 1996. A Declaration on the Independence of Cyberspace. *How to fix the Internet* [Online]. Available from: https://www.eff.org/cyberspace-independence [Accessed 08.02.1996. e POST, D. G. 2008. Governing Cyberspace: Law. *Santa Clara High Technology Law Journal,* 24, 883-913.

8 TSAGOURIAS, N. 2018. The legal status of cyberspace. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing. e, ainda, o recente entendimento no CICV 2020. International humanitarian law and cyber operations during armed conflicts, November 2019. *International Review of the Red Cross,* 102, 482-492.

9 KOLB, R. & HYDE, R. 2008. *An Introduction to the International Law of Armed Conflicts,* Oxford, Hart SASSÒLI, M. 2007. Ius ad Bellum and Ius in Bello – The Separation between the Legality of the Use of Force and Humanitarian Rules to be respected in Warfare : Crucial or Outdated? *In:* SCHMITT, M. N. & PEJIC, J. (eds.) *International Law and Armed Conflict : Exploring the Faultlines : Essays in Honour of Yoram Dinstein.* Leiden, Boston: Martinus Nijhoff.

ciberoperações podem estar na origem de um CAI[10], ainda que não combinados com meios convencionais da conflitualidade, e, naturalmente, durante todo o decurso até à cessação do conflito e a ocorrerem, conjuntamente, com os meios tradicionais[11].

Não perderemos de vista que o ciberespaço ocupa, ao lado do mar, terra, ar e espaço, um novo domínio operacional. Contudo com Clapham[12] esclarecemos que, não obstante as novas conflitualidades existentes e designações atribuídas pela literatura, importa não perder de vista que o DIH dispõe de conceitos jurídicos específicos que, por isso, determinam e enquadram quais as ciberoperações a serem reconduzidas à noção de ataque colocada pelo art.º 49.º/1 do I PA comum às GG.

1.3. Metodologia e estrutura

A metodologia utilizada assenta numa revisão da literatura, tendo por referência textos jurídicos, costume, jurisprudência, doutrina jurídica e militar e *soft law* com relevância para o DIH e com um raciocínio dedutivo. Por último, o trabalho está dividido em cinco partes:

Parte I: Introdução, delimitação do objeto e metodologia utilizada;
Parte II: Definição terminológica e operacional relevantes;
Parte III: Noção de ataque à luz do art.º 49.º/1 do I PA e diferentes posicionamentos doutrinários;
Parte IV: Conclusão;
Parte V: Bibliografia.

2. Definição Terminológica e Operacional

2.1. Ciberoperações militares

Uma das dificuldades com que nos deparamos ao tratar das matérias do ciberespaço é a ausência de um glossário universal[13]. Importa, por isso, sem pretensão de exaustão, explicar a terminologia utilizada.

---

10 Designados na literatura por *standalone attacks* e que até à data ainda não fizerem desencadear um CAI por falta de intensidade. GILL, T. D. 2018. International Humanitarian Law applied to cyber-warfare: Precautions, proportionality and the notion of "attack" under humanitarian law. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing, DOSWALD BECK, L. 2002. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *Computer Network Attack and International Law.* Newport: Naval War Collete.

11 Acórdão do TIExJ, *Prossecutor c. Tadic (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)*, IT-94-1, (02.10.1995), § 70.

12 CLAPHAM, A. 2021. *War,* Oxford, Oxford University Press.

13 DROEGE, C. 2012. Get off my cloud: cyber warfare, international humanitaria law, and the protections of civilians. *International Review of the Red Cross,* 94, 533-578.; DINNISS, H. H. 2012. *Cyberwarfare and the Laws of War,* Cambridge, Cambridge University Press.;TURNS, D. 2012. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict & Security Law,* 17, 279-297. e ROSCINI, M. 2014. *Cyber Operations and the Use of Force in International Law,* Oxford, Oxford University Press.

O objeto do nosso estudo são as ciberoperações militares conhecidas também, na doutrina anglo-saxónica, por *Military Cyber Operations* (MCO). Reportamo-nos, assim, àquelas operações de informação que ocorrem no/e através do ciberespaço (ciber) e, por prosseguirem uma finalidade militar, visam decerto concretizar aqueles objetivos empregando, para esse efeito, as competentes cibercapacidades (meios e métodos) aí desenvolvidas[14].

Dentro deste universo das ciberoperações militares pretendemos averiguar quais as que são subsumíveis no conceito de ataque constante no artigo 49.º/1 do IPA. Importa, por isso, com relação aos CAI, identificar, em primeiro lugar, as diferentes tipologias e explicar no que consistem para, em passo subsequente, ver as subsumíveis na noção de ataque.

Essa categorização não é, de resto, estranha aos diferentes entes privados e particulares, já que, sob o ponto de vista operacional e tático, todos os intervenientes no ciberespaço se socorrem dos mesmos meios e métodos de intervenção para alcançar os fins pretendidos. O que efetivamente muda é a estratégia e os objetivos/fins a atingir. Como se compreende, um grupo de *hackers* criminosos não comunga do mesmo objetivo de, por exemplo, uma equipa CERT (Computer Emergency Response Team) ou de uma unidade de comando militar como a US CYBERCOM (*United States Cyber Command*)[15].

Na literatura, mais antiga, fala-se em ciberguerra[16] e que é definida pela seguinte fórmula:

CW[17]= CNO[18] Sendo que o CNO = CND[19]+CNA[20]+CNE[21].

Verifica-se a importância ocupada pelas CNA (ataques) e as CNE (exploração ou *exploitation*) identificadas, então, como as atividades mais relevantes (ataque e exploração)[22].

---

14 Seguimos, por isso, de perto a terminologia de *Ducheine* e *Roscini* que, por sua vez, seguem a doutrina militar dos EUA ROSCINI, M. 2014. *Cyber Operations and the Use of Force in International Law,* Oxford, Oxford University Press, DUCHEINE, P. 2018. The notion of cyber operations. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing, DUCHEINE, P. A. L. 2015. Miltary Cybe Operations. *In:* GILL, T. D. & FLECK, D. (eds.) *The Handbook of the International Law of Military Operations.* 2ª ed. ed. Oxford: Oxford.

15 DUCHEINE, P. 2018. The notion of cyber operations. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing, SINGER, P. W. & FRIEDMANN, A. 2014. *Cybersecurity and Cyberwar : What Everyone needs to Know,* Oxford, Oxford University Press.

16 Evitamos este termo por o termo guerra ter, como já referido, um conceito jurídico específico.

17 Cyberwarfare.

18 Computer Network Operations.

19 Computer Network Defense.

20 Computer Network Attack.

21 Computer Network Exploitation. TURNS, D. 2012. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict & Security Law,* 17, 279-297.

22 O *Commentary to the HPCR Manual on International Law Applicable to Air and Missile Warfar* AAVV 2013. *Commentary to the HPCR Manual on International Law Applicable to Air and Missile Warfare : Elaborated by the Drafting Committee of the Group of Experts under the supervision of Professor Yoram Dinstein,* Cambridge, Cambridge University Press.

Estas ideias, como se verá, não se encontram totalmente afastadas, mas preferimos acompanhar a recente alteração ocorrida na doutrina militar dos EUA. Nela a designação de *Computer Network* (CN), que antecedia os termos *attack* e *exploitation* (CNA e CNE), foi substituída pela de *Cyberspace*, ficando agora a designar-se por *Cyberspace attack* e *Cybersapce exploitation*. Entendeu-se que o termo de CN era muito restritivo, por deixar de fora importantes ativos[23].

2.2. Terminologia adotada

Face ao exposto, importa, por isso, aderir ao pensamento de Roscini[24] que identifica as ciberoperações de exploração (*exploitation*) e os ciberataques (ataques), propriamente ditos como sendo as importantes, nesta matéria.

Nas atividades de ciberexploração, o objetivo é aceder, ilicitamente, a computadores, sistemas de computadores ou redes com o objetivo de exfiltrar a informação sem, todavia, colocar em causa a funcionalidade do sistema ou, sequer, a integridade dos próprios dados neles alojados[25].

Trata-se, por isso, de um acesso indolor, ou seja, sem repercussões para a funcionalidade do próprio sistema e para a integridade dos dados por se pretender um determinado acesso, sem que o respetivo titular se aperceba da presença, indevida, do terceiro e, ainda, como refere Roscini[26], não ser destrutivo.

Já nos ciberataques incluem-se todas aquelas ciberoperações, defensivas ou ofensivas, com a intenção de alterar, apagar, corromper ou negar acesso aos dados do computador ou *software* com o propósito de: a) propaganda ou deceção; e/ou b) disromper, parcial ou totalmente, o funcionamento do computador alvo, o sistema de computador ou a rede e, ainda, a existirem, afetar as próprias infraestruturas físicas operacionais; e/ou c) a produção de danos físicos exteriores ao computador, sistema de computadores ou rede[27].

Trata-se, assim, de um acesso doloroso por existir uma percetibilidade, pelo titular, da intrusão do terceiro, deixando este último um rasto de destruição, como também refere Roscini[28].

A nossa alusão às ciberoperações inclui aquelas duas modalidades sempre que não seja necessário proceder à sua distinção.

---

23 STAFF, U. D. O. D.-T. J. 2021. *DOD Dictionary of Military and Associated Terms,* Washington DC, US Department of Defense. Agradeço ao meu Colega do mestrado de Guerra da Informação, Carlos Pires, pelas explicações dadas.

24 ROSCINI, M. 2014. *Cyber Operations and the Use of Force in International Law,* Oxford, Oxford University Press.

25 *Idem.*

26 *Ibidem.*

27 *Ibidem.*

28 *Ibidem.*

3. Da Noção de Ataque

3.1. Dados estatísticos

Em 2020, houve um aumento de 435% nos ciberataques por *ransomware*[29]. De acordo com o relatório da Microsoft (2021), foram identificadas, como principais ameaças aos Estados, a espionagem e os ciberataques às infraestruturas críticas tais como, eletricidade, comunicações e saúde. Neste último particular, foram alvo de maior interesse os setores da administração pública (governo | 48%); organizações não governamentais e *think tanks* (31%), educação (3%), *Information Technology* (2%), *media* (1%), energia (1%), saúde (1%). Quanto aos países mais cobiçados, aparecem-nos, entre outros, os EUA (46%); Ucrânia (19%), Reino Unido (9%), Japão (3%) e a Alemanha (3%). Ainda segundo aquele mesmo relatório, os ataques tiveram origem na Rússia (58%); Coreia do Norte (23%); Irão (11%), China (8%); Coreia do Sul (1%), Vietname (1%) e Turquia (1%)[30].

A espionagem e os ciberataques também têm estado presentes no conflito armado entre a Ucrânia e a Rússia, para além do sofrimento de inocentes civis. Considerado o primeiro conflito de maior dimensão a envolver ciberoperações em larga escala, por semelhança do que sucedeu na Geórgia[31], a Rússia precedeu a invasão da Ucrânia com a exploração, disrupção de serviços (e do próprio satélite KA-SAT da Viasat Inc) e instalação de *software* maligno – com recurso ao *phishing* e *Distributed Denial of Services* nas redes ucranianas. Os alvos privilegiados foram, como referido, as infraestruturas críticas ucranianas, tais como sites governamentais, energia, redes operadoras de comunicação e instituições financeiras[32].

Decerto que contribuirão para o risco do escalar da conflitualidade a atuação dos *hacktivistas* patriotas[33] e, ainda, a própria retaliação da Rússia com relação aos países apoiantes da causa ucraniana[34].

29 FORUM, W. E. 2022. *The Global Risks Report 2022,* Suíça, World Economic Forum.

30 MICROSOFT 2021. Microsoft Digital Defense Report. s/local: Microsoft.

31 Na Geórgia, foi, ao que parece, pela primeira vez, coordenado um conjunto de operações no domínio do ciberespaço com outras operações militares ocorridas nos domínios operacionais em terra, mar e ar. HOLLIS, D. 2011. Cyberware Case Study: Georgia 2008. *Small Wars Journal*, 1-10.

32 LEWIS, J. A. 2022. Cyber War and Ukraine. *Center for Strategic and International Studies*, 1-14.

33 CORERA, G. 2022. Ukraine War: Don´t underestimate Russia cyber-threat, warns US. *BBC News*: acedido em 20.06.2022. Pense-se, ainda, com relação aos incidentes de 2007, na Estónia no papel desempenhado pelos *hacktivistas* patriotas russos OTTIS, R. 2008. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective,* Tallin, Cooperative Cyber Defence Centre of Excellence.

34 Não será, decerto, exagerado afirmar que o mundo está em alerta máximo, mais concretamente, os EUA e seus aliados JASPER, S. 2022. The Risk of Russian Cyber Retaliation for the United States Sending Rockets to Ukraine. *Europe and Eurasia – Ukraine* [Online]. Available from: https://www.cfr.org/blog/risk-russian-cyber-retaliation-united-states-sending-rockets-ukraine acedido em 20.06.2022.

3.2. Limitações do teste por equivalência dos efeitos cinéticos

A natureza do ciberespaço[35] – ubíquo, anónimo, sem fronteiras[36] – e, principalmente, dos próprios ciberataques, tem vindo a desafiar o DIH. Apesar da natureza não violenta ou não cinética dos ciberataques, os agentes que os praticam pretendem, no entanto, valer-se da sua aptidão para a produção de efeitos indiretos cinéticos e com repercussões negativas, por danos físicos ou perdas de funcionalidades de dado objeto, no mundo real[37].

O principal desafio colocado neste particular ao DIH, por isso, prende-se com a necessidade de "transmutar" esta realidade virtual para o mundo físico e à luz do qual foram criadas as regras. Com os olhos postos na conflitualidade com violência física, uso de força física e de armas cinéticas a produzirem diretamente os seus efeitos com relação aos alvos pretendidos[38]. A violência física direta era, por isso, a finalidade pretendida.

Com o advento das armas químicas e biológicas, este paradigma da violência física altera-se e o DIH não lhe fica indiferente. Desta feita, passamos a ter substâncias químicas e bacteriológicas nocivas que, pese embora não provocarem explosões físicas, não deixam, quando empregues, de ser qualificadas como ataques pelas graves repercussões tidas para as vítimas[39].

Imperativos da humanidade exigiam que, independentemente dos meios empregues e a natureza do ato (violento/ou não violento), se olhasse também para os efeitos por ele produzidos[40].

Este importante pensamento foi transposto, pelo DIH, para o ciberespaço. O ato (ciberoperação), em si, não passando a ser irrelevante, fica, assim, mais diluído, "desmaiado" por a centralidade assentar, agora, nos efeitos por si produzidos. Por sua vez, a

---

35 Várias são as noções do ciberespaço, no entanto, adotamos a constante no Dicionário do Departamento de Defesa dos EUA sobre termos militares e a eles associados STAFF, U. D. O. D.-T. J. 2021. *DOD Dictionary of Military and Associated Terms,* Washington DC, US Department of Defense.

36 SCHMITT, M. 2018. Introduction. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing. GILL, T. D. & FLECK, D. 2015. The Handbook of the International Law of Military Operations. *In:* GILL., T. D. & FLECK, D. (eds.) *Private Contractors and Security Companies.* 2ª ed. Oxford.

37 APPLEGATE, S. D. 2013. The Dawn of Kinetic Cyber. *In:* PODINS, K., STINISSEN, J. F. & MAYBAUM, M. (eds.) *5th International Conference on Cyber Conflict.* Tallin: NATO CCD COE Publications.

38 DUNANT, H. 1939. *A Memory of Solferino,* Geneva, International Committee of the Red Cross.. Ao DIH, não são desconhecidos os atos de natureza psicológica, devido à proibição constante no art.º 51/2 do I PA.

39 SCHMITT, M. N. 2013b. *Tallinn Manual on the International Law Applicable to Cyber Warfare : Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Cambridge, Cambridge University Press. SCHMITT, M. N. 2011. Cyber Operations and the *Jus in Bello*: Key Issues. *In:* PEDROZO, R. A. P. & WOLLSCHLAEGER, D. P. (eds.) *International Law and the Changing Character of War.* Newport, Rhode Island: Naval War College, SCHMITT, M. N. 2012. "Attack" as a Term of Art in International Law: The Cyber Operations Context. *In:* C. CZOSSEC, R. OTTIS & ZIOLKOSKI, K. (eds.) *Social Science Research Network.* Tallin: NATO CCD COE Publications.

40 DÖRMANN, K. 2004. Applicabiltiy of the Additional Protocols to Computer Network Attacks. *In:* BYSTRÖM, K. (ed.) *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law: Proceeding of the Conference* Stockholm: Swedish National Defence College.

Golden Gate, para a conversão de uma realidade não cinética para cinética, faz-se à luz dos efeitos cinéticos produzidos, lançando-se mão do teste da equivalência, conhecido na literatura anglo-saxónica por *Kinetic Effects Equivalence test*[41] (KEE) ou *effects based approach*[42]. Ficarão, assim, habilitados no teste todas aquelas ciberoperações que causem a destruição e/ou danos materiais em objetos e, ainda, os que causem ferimentos e a morte de pessoas. Nisso passando a assentar, para um mundo virtual, o que designamos, agora, pelo credo da fisicalidade do mundo cinético.

Percebe-se a solução assim encontrada; no entanto, ela conduz inevitavelmente a alguns constrangimentos, o que é resultante de uma conceção, por vezes forçada à imagem e semelhança de um mundo real, algo que não obstante ter ainda alguma territorialidade, é eminentemente virtual. Ou seja, a conceção de uma *imago digitalis,* com relação a algo, que não foi concebido à imagem e semelhança de uma realidade espacial clássica, concretamente, o ciberespaço e a internet.

Esta é uma das razões, como o demonstrarão a doutrina, pelas quais o teste por equivalência dos efeitos cinéticos fica aquém das necessidades sentidas por: a) nem sempre as ciberoperações produzirem efeitos cinéticos[43]; b) os efeitos pretendidos pelos seus autores serem, mais das vezes, os indiretos ou colaterais e c) por certas realidades, no mundo real, não serem consideradas objetos materiais – como, por exemplo, para alguma doutrina, os dados – e, por isso, insuscetíveis de destruição material pense-se, por exemplo, no apagar, manipulação de dados armazenados ou a inserção destes últimos, num sistema informático do adversário, sem causar dano ao equipamento[44].

No futuro e, com o advento da inteligência artificial e do *machine learning* na conflitualidade, previmos a probabilidade de as limitações inerentes a esta teoria ainda serem mais notórias devido aos contornos específicos e desafios postos por estas novas realidades. Julgamos, por isso, ser preferível ir ao encontro do futuro com teorias inovadoras e, por isso, mais conformes com a essência da *Information Technology*, do virtual, imaterial e da própria relação entre o mundo virtual e real que tendem, cada vez mais, a se apresentarem como dois mundos convergentes, intrincados e indissociáveis[45].

Um agarrar excessivo ao mundo cinético, com relação a uma realidade virtual, pode causar indesejáveis contradições e até conduzir, em última análise, a uma realidade proibida no mundo cinético, por comportar uma destruição física do objeto, não o seja no mundo virtual por não ser acompanhada do dogma da fisicalidade por nós identificado.

41 BANNELIER-CHRISTAKIS, K. 2018. Is the principle of distinction still relevant in cyberwarfare? *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

42 DINSTEIN, Y. 2002. Computer Network Attacks and Self-Defense. *In:* MICHAEL N. SCHMITT & O´DONNELL, B. T. (eds.) *International Law Studies.* United States: U.S Naval War College.

43 KOH, H. H. 2012. International Law in Cyberspace. *Harvard International Law Journal,* 54, 1-12.

44 WOLTAG, J.-C. 2014. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law,* Cambridge, Intersentia, SASSÒLI, M. 2019. *International Humanitarian Law: Rules, Controversies and Solutions to Problems Arising in Warfare,* United Kingdom, Edward Elgar Publishing Limited.

45 MARTINS, M. 2012. Ciberespaço: uma Nova Realidade para a Segurança Internacional. *idn nação e defesa*, 32-49.

Pense-se, por exemplo, nas ciberoperações que manipulam infraestruturas civis, tornando-as disfuncionais, sem, no entanto, causar qualquer dano imediato no objeto ou, até, ferimentos nas pessoas[46]. O DIH não pode, decerto, distanciar-se desta discussão apesar de alguns resultados positivos já alcançados com a KEE.

3.3. Divergências doutrinárias em relação à noção de ataque do artigo 49.º/1 do I PA – o debate entre Schmitt/Dörmann

Apesar do artigo 49.º/3 do I PA apenas se reportar à conflitualidade no mar, terra e ar, importa referir que o ciberespaço não está excluído do seu âmbito de aplicabilidade. O principal objetivo deste preceito foi clarificar, em relação aos ataques aéreos dirigidos contra objetivos em terra, se passariam a ser regidos pelas regras da conflitualidade aérea ou terrestre e, não propriamente, apresentar uma lista exaustiva sobre os seus domínios operacionais. Neste sentido, uma interpretação atualista ao I PA não é, por isso, impeditiva de o aplicar a qualquer "ciber-operação militar que possa afetar, em terra, a população civil, os civis e os bens de caráter civil", interpretação, de resto, conforme com o princípio da humanidade subjacente[47].

A noção de ataque é suscitada pelo artigo 49.º/1 do I PA que o define como atos de violência contra o adversário, independentemente, da natureza ofensiva ou defensiva do próprio ato. Para o DIH a distinção entre aquelas duas modalidades do ato (ofensivo e defensivo) é, por isso, irrelevante por ambas serem subsumíveis na noção de ataque[48].

Contudo, no que respeita à noção de violência, ela encontra-se muito acoplada à ideia de atos que envolvam danos físicos, sendo, por isso, excluída do âmbito do conceito da violência todas as ações típicas das guerras psicológica (ações psicológicas não destrutivas contra civis por força do artigo 51.º/2 do I PA), económica e política[49].

Neste contexto, entendem Partsch e Bothe, ciberataques "praticados através de vírus, bombas lógicas etc… e que produzam danos físicos a pessoas ou objetos e que vão para além do programa ou dados alvo de ataques, podem ser qualificados como atos de violência e, consequentemente, como ataques"[50].

A alusão à violência naquele preceito, interpretada nos termos suprarreferidos, socorrendo-se, ainda, dos entendimentos doutrinários daqueles autores, leva Schmitt a defender serem subsumíveis no conceito de ataque apenas aquelas operações militares

46 DROEGE, C. 2012. Get off my cloud: cyber warfare, international humanitaria law, and the protections of civilians. *International Review of the Red Cross,* 94, 533-578.

47 ROSCINI, M. 2014. *Cyber Operations and the Use of Force in International Law,* Oxford, Oxford University Press. e DORNBUSCH, J. 2018. *Das Kampfführungsrecht im internationalen Cyberkrieg,* Baden Baden, Nomos Verlagsgesellschaft.

48 WOLTAG, J.-C. 2014. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law,* Cambridge, Intersentia. E, ainda, SANDOZ, Y., SWINARSKI, C. & ZIMMERMANN, B. 1987. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949,* Martinus Nijhoff, International Committee of the Red Cross.

49 BOTHE, M., PARTSCH, K. J. & SOLF, W. A. 2013. *New Rules for victims of armed conflicts: commentary on the two 1977 protocols additional to the Geneva Conventions of 1949 – Vol I.,* Leiden, Martinus Nijfhoff Publishers.

50 *Idem.*

em relação às quais seja expectável de, com razoabilidade, causarem danos ou a destruição de objetos ou ferimentos ou morte das pessoas[51].

Segundo o autor, apenas seria em relação a estas que se aplicariam as proibições e restrições decorrentes do artigo 48.º do I PA, resultantes da aplicabilidade do princípio da distinção e, ainda, as vertidas no título IV do I PA (no qual se insere aquela norma), tais como, por exemplo, as constantes do artigo 51.º/2/4/7 do I PA, por apenas se reportarem ao termo de ataques e não ao de operações.

Consequentemente, todas as restantes operações militares que não se enquadrem neste conceito de ataque por não alcançarem o grau de violência física exigido, são permitidas. Por não se encontrarem, ainda, abrangidas pelo DIH, não existe nenhum impedimento, podendo, por isso, ter como objeto os civis e a população civil.

Para Schmitt, ataque e operações militares são conceitos sinónimos e reconduzidos ao próprio termo de operações constante do artigo 48.º do I PA, que apenas contemplam, no âmbito da sua previsibilidade, as operações militares conforme o conceito de violência posto pelo artigo 49.º/1 do I PA[52]. Com efeito, no seu entendimento, disposições jurídicas como os artigos 49.º/1 e 51.º/2/4/6 e 7 do I PA por aludirem, expressamente, ao termo "ataque" constituem preceitos especiais que, na qualidade de *lex specialis*, interpretam ou até modificam a regra geral vertida no artigo 48.º do I PA[53] referente ao princípio da distinção, garantindo, assim, uma harmonização entre os diferentes preceitos em presença.

Perante esta noção restrita de ataque colocada por Schmitt, vir-se-ia, contudo, a insurgir Dörmann. Com o argumento alicerçado nas operações de neutralização previstas no artigoº 52.º/ 2 do I PA, defende que nem todas as operações militares têm de ter como resultado a destruição física, total ou parcial, leia-se um dano físico[54]. Nesse sentido, aponta como exemplo o "mero desativar do objeto como, por exemplo, o desligar de uma rede elétrica, sem a destruir", dever também ser enquadrado na noção de ataque[55].

A questão não é simples, e ambos os posicionamentos são passíveis de críticas. Com relação a Dörmann, aderimos aos argumentos chave levantados por Dinniss. Não nos parece feliz entroncar um raciocínio, cuja preocupação passa pela proteção de civis e a população civil, num artigo em que apenas caem no âmbito da sua previsibilidade os

51 SCHMITT, M. N. 2019. Wired warfare 3.0: Protecting the civilian population during cyber operations. *International Review of the Red Cross*, 1-13, SCHMITT, M. N. 2002. Wired warfare: Computer network attack and *jus in bello*. *International Review of the Red Cross,* 84º, 365-399, SCHMITT, M. N. 2012. "Attack" as a Term of Art in International Law: The Cyber Operations Context. *In:* C. CZOSSEC, R. OTTIS & ZIOLKOSKI, K. (eds.) *Social Science Research Network*. Tallin: NATO CCD COE Publications.

52 SCHMITT, M. N. 2011. Cyber Operations and the *Jus in Bello*: Key Issues. *In:* PEDROZO, R. A. P. & WOLLSCHLAEGER, D. P. (eds.) *International Law and the Changing Character of War*. Newport, Rhode Island: Naval War College.

53 *Idem* e DINNISS, H. A. H. 2018. Attacks and Operations – The debate over network "attacks". *Paper for the Minerva Centre Conference, Jerusalem, Israel*, 1-9.

54 DÖRMANN, K. 2004. Applicabiltiy of the Additional Protocols to Computer Network Attacks. *In:* BYSTRÖM, K. (ed.) *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law: Proceeding of the Conference* Stockholm: Swedish National Defence College.

55 *Idem*.

objetos civis. Fazê-lo seria apenas garantir, à luz justamente do princípio da distinção previsto no artigo 48.º do I PA (argumento invocado pelo autor), metade de uma equação protetora que, em si mesma, deve ser incindível.

Entendemos, ainda, com Dinniss, que o posicionamento de Dörmann não ajuda na concretização do que seja um ataque. A alusão à neutralização confunde, por um objeto também poder ser neutralizado por ataques convencionais e suscetíveis de produzir danos físicos. O exemplo clássico apontado é a colocação de minas, em dado território, para impedir que o adversário lhe aceda[56].

Para além destas questões operacionais, acrescentamos ainda uma outra, assente na experiência, concretamente, a da própria dificuldade em determinar o que seja uma operação militar. Como assentar, por isso, uma solução numa base conceitual controvertida – operações militares – e, ainda, adversa à própria hermenêutica do DIH. Com efeito, para o DIH, mais importantes do que as categorizações ou tipologias é, efetivamente, a função ao abrigo do critério da funcionalidade em que assenta[57].

No advento das novas tecnologias e a sua rápida evolução, principalmente, com relação aos métodos e meios utilizados, pensamos que a atendibilidade de tipologias operacionais não é um critério habilitador para poder corresponder com os novos desafios colocados. Uma categorização e tipologia das operações militares assim posta, decerto asfixiaria o seu necessário ajustamento a estas novas realidades, condicionado, em muito, a sua arte militar à qual o DIH também atende, pela consagração do princípio da necessidade militar. Prova do exposto é que o próprio conceito de objetivos militares não se destina, tão só, a determinar o que pode ou não ser alvo de ataques. Para além disso, como suscitado por Dinniss, ele tem ainda como importante missão, em outras disposições, contextualizar e enquadrar as operações militares num todo[58].

Por último, a noção levantada por Dörmann é muito ampla nela, incluindo ciberoperações militares que as práticas estaduais entendem não serem proibidas. Nesse sentido, ela passaria, por exemplo, a abranger ataques Distributed Denial of Services e de desfiguração (*defacement*), como os praticados em 2008, no conflito entre a Rússia e a Geórgia, ocorridos antes, durante e após o conflito nos sites da Geórgia[59].

Já os argumentos avançados por Schmitt, com relação à noção de ataque, pecam por serem restritivos. A sua consequência é poder deixar os civis, população civil e objetos civis sem proteção, o que contraria a própria natureza do DIH.

Com efeito, nem todas as ciberoperações militares, como já referido, enquadram a noção de ataque e, por isso, o DIH não proíbe a deceção, operações de propaganda nem,

56 DINNISS, H. A. H. 2018. Attacks and Operations – The debate over network "attacks". *Paper for the Minerva Centre Conference, Jerusalem, Israel*, 1-9.

57 TOUGAS, M.-L. 2014. Commentary on Part I of the Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict. *International Review of the Red Cross,* 96º, 305-358.

58 Artigos 48.º e 51.º/7 todos do I PA.

59 DINNISS, H. A. H. 2018. Attacks and Operations – The debate over network "attacks". *Paper for the Minerva Centre Conference, Jerusalem, Israel*, 1-9.

em princípio, a ciberexploração (*exploitation*). Nesse sentido, também não exige, com relação a estas, a distinção entre combatentes e civis. Todavia, não deixa de ser um argumento que a destruição ou dano podem ser obtidos sem efeitos físicos violentos, como o demonstram as situações com relação a objetos, que perdem apenas a sua funcionalidade[60].

Contudo, importa, por ser válido, aproveitar, em relação à teoria dos efeitos cinéticos por equivalência, um consenso já alcançado. Efetivamente, quando uma ciberoperação produz danos físicos em relação a objetos e ferimentos ou morte das pessoas, há que, sem dúvida, reconduzi-lo à noção de ataque constante no artigo 49.º/1 do I PA e, por isso, sujeitá-lo às proibições e restrições constantes no artigo 48.º do I PA.

Por sua vez, uma visão realista também leva a defender não serem enquadrados, na noção de ataque, aqueles danos ou destruições mínimas, incomodativos para a vida dos civis, população civil e objetos civis que, por isso, não farão desencadear a aplicabilidade do DIH, por não reunirem o grau de intensidade exigido. Com efeito, o DIH é o último reduto a ser aplicado, em situações extremas, o que, naquele caso, não sucede[61]. Nesse contexto, uma ciberoperação que se limita a impedir o acesso da população à internet, sem causar qualquer efeito violento não fará, por isso, desencadear a aplicabilidade do DIH[62].

Não podemos perder de vista, neste particular, que o DIH tem sempre a árdua missão de conciliar dois princípios contraditórios: por um lado, a necessidade militar defendida, maioritariamente, por aqueles Estados com maiores capacidades militares, e o da humanidade, pela consideração da proteção dos civis, população civil e objeto posta, ainda, pelos Estados, com menor capacidade, por ser, também, uma forma de limitar o poder dos Estados mais fortes[63].

Contudo, entendemos que existem situações em que, por um lado, não só a exigibilidade de uma fisicalidade excessiva, como a constante na regra 98 do Manual de Tallin[64], conduz a contradições insanáveis e intoleráveis, como também, por outro lado, há, ainda, a necessidade de alargar, efetivamente, o conceito de ataque constante no artigo 49.º do I PA para se garantir, como referido, a proteção de civis, população civil e objetos civis.

Entendemos, por isso, ser uma fisicalidade excessiva na matéria referente às ciberoperações que interfiram com a funcionalidade de determinado objeto – de resto controvertida entre os próprios peritos – por apenas enquadrarem, na noção de ataque, aquelas

60 SASSÒLI, M. 2019. *International Humanitarian Law: Rules, Controversies and Solutions to Problems Arising in Warfare,* United Kingdom, Edward Elgar Publishing Limited, DINNISS, H. A. H. 2018. Attacks and Operations – The debate over network "attacks". *Paper for the Minerva Centre Conference, Jerusalem, Israel*, 1-9.

61 SCHMITT, M. N. & VIHUL, L. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations : Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Camdridge, Cambridge University Press.

62 SASSÒLI, M. 2019. *International Humanitarian Law : Rules, Controversies and Solutions to Problems Arising in Warfare,* United Kingdom, Edward Elgar Publishing Limited.

63 BRÍZIDO, A. P. 2021. A estranha alquimia da Cláusula Martens: de 1864 até à I Conferência de Paz da Haia de 1899. *In:* SILVA, C. N. D. & SEIXAS, M. (eds.) *Estudos Luso-Hispanos de História do Direito.* Madrid: Editorial Dykinson.

64 SCHMITT, M. N. & VIHUL, L. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations : Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Camdridge, Cambridge University Press.

operações em que a recuperação da respetiva funcionalidade exija a substituição de componentes físicas ou, mais restritamente, a reinstalação do *software* operacional por só, nessa situação, entender-se ocorrer a expressão de um dano físico no próprio objeto[65].

A exclusão da noção de ataques de operações, com as mesmas consequências para as pessoas e objetos protegidos pelo DIH, assente na ideia da ausência de fisicalidade, parece-nos, por isso, questionável. Trata-se de um argumento, em nosso entendimento, inconsistente, pois não é aceitável um resultado em que a população civil, civis e objetos civis, em iguais circunstâncias, numas situações seja protegida e noutras não, com o argumento do dano não ter sido acompanhado de uma expressão física no objeto.

Com efeito, a maioria das ciberoperações, praticadas naquelas situações e no caso de destruição dados, é concebida para causar danos, devendo, por isso, os civis, população civil e objetos civis serem protegidos, evitando-se, ainda, os danos colaterais como vertido no artigo 57.º do I PA[66], considerando-se, para esse efeito, os princípios da prevenção e proporcionalidade.

Para além do exposto, seria, ainda, um convite para a conceção de técnicas informáticas que conduzissem à disfuncionalidade nos moldes descritos por fugirem ao perímetro de aplicabilidade do DIH. Com a minoria de peritos, entendemos, por isso, que todas as ciberoperações conducentes à disfuncionalidade do objeto deverem enquadrar a noção de ataque.

3.4. A doutrina assente no conceito da hostilidade

Importa, por isso, questionar pela alternativa que coloca o acento tónico no conceito da hostilidade posta por Melzer e, mais tarde, aprofundada por Dinniss. Longe de ser uma equação perfeita, ela tem, no entanto, o mérito de alargar o conceito de ataque e tentar adequá-la à prática estadual.

Pensamos, por isso, que o artigo 48.º/1 do I PA, ao referir operações militares, não está a reportar-se apenas a ataques. Apesar de constituírem, como referido por Bothe e Partsch, uma importante componente, não esgotam, contudo, o universo das operações militares. A alusão a operações destina-se principalmente para as distinguir de outro tipo de operações, concretamente, as campanhas ideológicas, políticas ou religiosas não abrangidas pelo DIH[67]. Por o preceito se enquadrar no Título IV, e na Secção referente à proteção geral contra os efeitos das hostilidades, parece-nos consentâneo, por isso, ser interpretado e enquadrado na secção a que respeita e com referência, ainda, ao conceito de hostilidades[68].

---

65 *Ibid.*

66 FLECK, D. 2013. Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict & Security Law,* 18º, 331-351.

67 BOTHE, M., PARTSCH, K. J. & SOLF, W. A. 2013. *New Rules for victims of armed conflicts: commentary on the two 1977 protocols additional to the Geneva Conventions of 1949 – Vol I.,* Leiden, Martinus Nijfhoff Publishers.

68 SANDOZ, Y., SWINARSKI, C. & ZIMMERMANN, B. 1987. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949,* Martinus Nijhoff, International Committee of the Red Cross. – parágrafo 1875.

Importa, todavia, conhecer melhor o pensamento estruturante de Melzer para podermos opinar, ainda que muito comedidamente. A abordagem proposta pelo autor afastou-se de Dörmann por a centralidade do raciocínio não assentar na qualificação das operações na noção de ataque, reconduzindo-a antes na noção, mais ampla, de hostilidades posta pelo DIH[69].

Segundo a Diretriz para a interpretação da participação direta nas hostilidades, ela é sinónima de um recurso coletivo, pelas partes do conflito, aos meios e métodos com o objetivo de ferir, condicionar o inimigo. Em sentido figurado, é descrita como sendo constituída pelo somatório de todos os atos hostis praticados pelos indivíduos que participam diretamente nas hostilidades[70].

Quanto à imputação do ato ao seu autor, esta ocorreria à luz dos critérios estabelecidos para a participação direta nas hostilidades, em que é consabido, também, o nexo da causalidade ser, justamente, o mais polémico por também ele deixar de fora grande parte, dos efeitos indiretos[71].

Para Melzer, todas as ciberoperações imputáveis a uma parte no conflito e concebidas para condicionar o adversário por causarem danos, destruição ou ferimentos ou por direta e adversamente, afetarem, ainda, as suas operações ou capacidades militares, são havidos como atos hostis e, por isso, são abrangidas pelas proibições e restrições impostas pelo DIH aquando da escolha dos meios e métodos de guerra[72].

Pelo que "ciberoperações praticadas com a intenção de disromper ou incapacitar um radar ou sistema de armas controlados com recurso a computadores, fornecimento de logística ou redes comunicacionais", que não causem danos diretos e, ainda, a própria eliminação, manipulação de dados praticados no sistema militar adversário condicionando, adversamente, a sua capacidade para a condução das hostilidades" são havidos pelo autor como sendo atos hostis, pelo que se enquadram no perímetro da aplicabilidade do DIH[73].

Conclusões

Como se compreende, a questão que nos propusemos abordar está longe de ser pacífica. Ambos os pensamentos expressam uma realidade incontornável: nem todas as ciberoperações militares praticadas são objeto do DIH ou, a serem-no, não convocam aplicabilidade de todo o acervo legal inerente ao DIH, concretamente, o princípio da distinção. O problema reside, por isso, na delimitação deste perímetro e o respetivo critério a utilizar para a concretização da noção de ataque do artigo 49.º do I PA.

Longe de ser perfeito, parece-nos que o conceito da hostilidade apresenta argumen-

69 MELZER, N. 2011. *Cyberwarfare and International Law,* United Nations, UNIDIR Resources.

70 MELZER, N. 2009. *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law,* Geneva, International Comission of the Red Cross.

71 *Idem.*

72 *Ibidem.*

73 *Idem.*

tos mais robustos por comparação com os argumentos apresentados pelo mundo cinético (peritos do Manual de Tallinn) e, ainda, o assente na dissecação das tipologias das operações militares subsumíveis no conceito de ataque (Dörmann), cujas críticas já foram por nós endereçadas no ponto 4.3. e para o qual remetemos.

Por se tratar de uma noção mais ampla e elástica, parece-nos, por isso, mais apta para abranger ciberoperações que não devem ser excluídas. Esta exclusão deixaria as pessoas e objetos protegidos pelo DIH em intolerável vulnerabilidade e, por isso, atentatória contra a própria essência do princípio da humanidade.

Contudo o DIH, ramo do Direito que rege a conflitualidade, não pode, também, alhear-se ao princípio da necessidade militar. Nesse contexto, entendemos que o conceito da hostilidade é aquele que permite ir ao melhor encontro das novos necessidades e desafios colocados pela conflitualidade no ciberespaço.

Se a guerra é um fenómeno cultural dotado de planeamento e de estratégia, a sua arte necessita de um conceito ajustado que permita o acompanhamento destas novas realidades, respeitando, naturalmente, as limitações decorrentes da razão de ser inerente ao princípio da humanidade. Sendo o ataque uma componente, ou seja, uma parte relacionada com um todo, parece-nos, por isso, desejável atender, para aquela integração, a uma realidade maior, como o colocado pelo conceito da hostilidade.

No entanto, não temos dúvidas, a equação não é perfeita e está longe de ser resolvida. Os desafios colocados pelo quotidiano, acopladas ainda à prática estadual seguida para a resolução dos problemas terão, decerto, uma importante palavra a dizer.

Bibliografia

AAVV 2013. *Commentary to the HPCR Manual on International Law Applicable to Air and Missile Warfare: Elaborated by the Drafting Committee of the Group of Experts under the supervision of Professor Yoram Dinstein,* Cambridge, Cambridge University Press.

AKANDE, D. 2012. Classification of Armed Conflicts: Relevant Legal Concepts. *In:* WILMSHURST, E. (ed.) *International Law and the Classification of Conflicts.* Oxford: Oxford University Press.

APPLEGATE, S. D. 2013. The Dawn of Kinetic Cyber. *In:* PODINS, K., STINISSEN, J. F. & MAYBAUM, M. (eds.) *5th International Conference on Cyber Conflict.* Tallin: NATO CCD COE Publications.

BANNELIER-CHRISTAKIS, K. 2018. Is the principle of distinction still relevant in cyberwarfare? *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

BARLOW, J. P. 1996. A Declaration on the Independence of Cyberspace. *How to fix the Internet* [Online]. Available from: https://www.eff.org/cyberspace-independence [Accessed 08.02.1996.

BOTHE, M., PARTSCH, K. J. & SOLF, W. A. 2013. *New Rules for victims of armed conflicts: commentary on the two 1977 protocols additional to the Geneva Conventions of 1949 – Vol I.,* Leiden, Martinus Nijfhoff Publishers.

BRÍZIDO, A. P. 2021. A estranha alquimia da Cláusula Martens: de 1864 até à I Conferência de Paz da Haia de 1899. *In:* SILVA, C. N. D. & SEIXAS, M. (eds.) *Estudos Luso-Hispanos de História do Direito.* Madrid: Editorial Dykinson.

CICV 2020. International humanitarian law and cyber operations during armed conflicts, November 2019. *International Review of the Red Cross,* 102, 482-492.

CLAPHAM, A. 2021. *War,* Oxford, Oxford University Press.

CORERA, G. 2022. Ukraine War: Don´t underestimate Russia cyber-threat, warns US. *BBC News*.

DINNISS, H. A. H. 2018. Attacks and Operations – The debate over network "attacks". *Paper for the Minerva Centre Conference, Jerusalem, Israel*, 1-9.

DINNISS, H. H. 2012. *Cyberwarfare and the Laws of War,* Cambridge, Cambridge University Press.

DINSTEIN, Y. 2002. Computer Network Attacks and Self-Defense. *In:* MICHAEL N. SCHMITT & O´DONNELL, B. T. (eds.) *International Law Studies.* United States: U.S Naval War College.

DÖRMANN, K. 2004. Applicabiltiy of the Additional Protocols to Computer Network Attacks. *In:* BYSTRÖM, K. (ed.) *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law: Proceeding of the Conference* Stockholm: Swedish National Defence College.

DORNBUSCH, J. 2018. *Das Kampfführungsrecht im internationalen Cyberkrieg,* Baden Baden, Nomos Verlagsgesellschaft.

DOSWALD BECK, L. 2002. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *Computer Network Attack and International Law.* Newport: Naval War Collete.

DROEGE, C. 2012. Get off my cloud: cyber warfare, international humanitaria law, and the protections of civilians. *International Review of the Red Cross,* 94, 533-578.

DUCHEINE, P. 2018. The notion of cyber operations. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

DUCHEINE, P. A. L. 2015. Miltary Cybe Operations. *In:* GILL, T. D. & FLECK, D. (eds.) *The Handbook of the International Law of Military Operations.* 2ª ed. ed. Oxford: Oxford.

DUNANT, H. 1939. *A Memory of Solferino,* Geneva, International Committee of the Red Cross.

FLECK, D. 2013. Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New *Tallinn Manual. Journal of Conflict & Security Law,* 18º, 331-351.

FORUM, W. E. 2022. *The Global Risks Report 2022,* Suiça, World Economic Forum.

GILL, T. D. 2018. International Humanitarian Law applied to cyber-warfare: Precautions, proportionality and the notion of "attack" under humanitarian law. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

GILL, T. D. & FLECK, D. 2015. The Handbook of the International Law of Military Operations. *In:* GILL, T. D. & FLECK, D. (eds.) *Private Contractors and Security Companies.* 2ª ed. ed. Oxford Oxford.

HOLLIS, D. 2011. Cyberware Case Study: Georgia 2008. *Small Wars Journal*, 1-10.

JASPER, S. 2022. The Risk of Russian Cyber Retaliation for the United States Sending Rockets to Ukraine. *Europe and Eurasia – Ukraine* [Online]. Available from: https://www.cfr.org/blog/risk-russian-cyber-retaliation-united-states-sending-rockets-ukraine [Accessed 15.06.2022].

KOH, H. H. 2012. International Law in Cyberspace. *Harvard International Law Journal,* 54, 1-12.

KOLB, R. & HYDE, R. 2008. *An Introduction to the International Law of Armed Conflicts,* Oxford, Hart

LEWIS, J. A. 2022. Cyber War and Ukraine. *Center for Strategic and International Studies*, 1-14.

MARTINS, M. 2012. Ciberespaço: uma Nova Realidade para a Segurança Internacional. *idn nação e defesa*, 32-49.

MELZER, N. 2009. *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law,* Geneva, International Comission of the Red Cross.

MELZER, N. 2011. *Cyberwarfare and International Law,* United Nations, UNIDIR Resources.

MICROSOFT 2021. Microsoft Digital Defense Report. s/local: Microsoft.

NUNES, P. F. V. 2006. Operações de Informação: Enquadramento e Impacto Nacional. *Revista Militar*, s/pag.

OTTIS, R. 2008. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective,* Tallin, Cooperative Cyber Defence Centre of Excellence.

PEREIRA, M. D. A. D. V. 2014. *Noções fundamentais de direito humanitário,* Coimbra, Coimbra.

POST, D. G. 2008. Governing Cyberspace: Law. *Santa Clara High Technology Law Journal,* 24, 883-913.

ROSCINI, M. 2014. *Cyber Operations and the Use of Force in International Law,* Oxford, Oxford University Press.

SANDOZ, Y., SWINARSKI, C. & ZIMMERMANN, B. 1987. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949,* Martinus Nijhoff, International Committee of the Red Cross.

SASSÒLI, M. 2007. Ius ad Bellum and Ius in Bello – The Separation between the Legality of the Use of Force and Humanitarian Rules to be respected in Warfare : Crucial or Outdated? *In:* SCHMITT, M. N. & PEJIC, J. (eds.) *International Law and Armed Conflict : Exploring the Faultlines : Essays in Honour of Yoram Dinstein*. Leiden, Boston: Martinus Nijhoff.

SASSÒLI, M. 2019. *International Humanitarian Law: Rules, Controversies and Solutions to Problems Arising in Warfare,* United Kingdom, Edward Elgar Publishing Limited.

SCHMITT, M. 2018. Introduction. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

SCHMITT, M. N. 2002. Wired warfare: Computer network attack and *jus in bello*. *International Review of the Red Cross,* 84º, 365-399.

SCHMITT, M. N. 2011. Cyber Operations and the *Jus in Bello*: Key Issues. *In:* PEDROZO, R. A. P. & WOLLSCHLAEGER, D. P. (eds.) *International Law and the Changing Character of War*. Newport, Rhode Island: Naval War College.

SCHMITT, M. N. 2012. "Attack" as a Term of Art in International Law: The Cyber Operations Context. *In:* C. CZOSSEC, R. OTTIS & ZIOLKOSKI, K. (eds.) *Social Science Research Network*. Tallin: NATO CCD COE Publications.

SCHMITT, M. N. 2013a. Classification of Cyber Conflict. *International Law Studies US Naval War College,* 89º, 233-251.

SCHMITT, M. N. 2013b. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Cambridge, Cambridge University Press.

SCHMITT, M. N. 2019. Wired warfare 3.0: Protecting the civilian population during cyber operations. *International Review of the Red Cross*, 1-13.

SCHMITT, M. N. & VIHUL, L. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Camdridge, Cambridge University Press.

SINGER, P. W. & FRIEDMANN, A. 2014. *Cybersecurity and Cyberwar: What Everyone needs to Know,* Oxford, Oxford University Press.

STAFF, U. D. O. D.-T. J. 2021. *DOD Dictionary of Military and Associated Terms,* Washington DC, US Department of Defense.

TOUGAS, M.-L. 2014. Commentary on Part I of the Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict. *International Review of the Red Cross,* 96º, 305-358.

TSAGOURIAS, N. 2018. The legal status of cyberspace. *In:* NICHOLAS TSAGOURIAS & BUCHAN, R. (eds.) *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar Publishing.

TURNS, D. 2012. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict & Security Law*, 17, 279-297.

WEBSTER, F. 2014. *Theories of the Information Society,* London, Routledge, Taylor & Francis Group.

WOLTAG, J.-C. 2014. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law,* Cambridge, Intersentia.

Um Olhar Sobre a Cibersegurança em Portugal

Vitória Sigareva

No mundo atual globalizado, a informação circula à velocidade da luz, não reconhecendo as fronteiras terrestres. Presenciamos uma sociedade mundial cada vez mais digital e dependente das novas tecnologias. O ciberespaço apresenta inúmeras vantagens e oportunidades, e facilita o diálogo, a cooperação e o progresso. No entanto, surge igualmente acompanhado de incertezas e ameaças, ao nível individual e estatal. A cibersegurança dos Estados, e das suas populações, pode encontrar-se em risco, caso não existam medidas concretas, formação pertinente ou recursos suficientes para assegurar a ciberdefesa e a cibersegurança nacionais.

O presente trabalho analisa de que maneira Portugal se encontra preparado para enfrentar as ameaças cibernéticas. Para isso, são apresentadas as principais tendências em cibercriminalidade em Portugal, nos últimos dois anos, e os mecanismos para lidar com os desafios, desenvolvidos desde o início do segundo milénio. Com este objetivo, e procurando enriquecer o estado da arte existente sobre este tema, o ensaio procura efetuar um mapeamento nacional e internacional da cibersegurança, apresentando a arquitetura global na qual Portugal se apoia para garantir a sua cibersegurança.

A cibersegurança consiste num conjunto de medidas de prevenção, monitorização, deteção, reação, análise e recuperação, que garantem a segurança individual e coletiva de uma sociedade. Pela sua importância, o tópico não passou despercebido aos olhos dos investigadores e académicos. Alguns autores debruçaram-se sobre as vulnerabilidades e os riscos constantes no mundo informático (Pereira, 2021); outros focaram-se nos problemas resultantes do período da pandemia COVID-19 (Barrinha, 2020). Outros investigadores efetuaram uma análise mais empírica, chegando à conclusão de que não existia uma cultura de cibersegurança consolidada em Portugal, que obrigasse todos os indivíduos e entidades a cumprirem com as ações de cibersegurança (Matos, 2018). De facto, Correia, Santos e Bilhim (2016) identificaram cinco *clusters* diferentes, na população portuguesa, em que num extremo se situavam pessoas desinformadas sobre, ou despreocupadas com, as práticas de cibersegurança, e no outro, pessoas a favor da vigilância e satisfeitas com as ações do Estado para garantir a cibersegurança no país.

Muitos trabalhos centraram-se na governança no domínio cibernético. Por governança cibernética, entendem as ações com vista à proteção dos respetivos interesses, em vários setores, que estejam direta ou indiretamente ligados ao domínio ciber (Greiman,

2018, p.149). As grandes questões são relativas à existência, ou não, de uma cibergovernança global, especialmente quando desafiada pelo setor privado (Liaropoulos, 2017); que tipos de cibergovernança se identificam (Greiman, 2018); será que não existe uma sobreposição das competências entre as entidades incumbentes (Santos, 2011); será que se deve apostar em regulações mais frequentes e abrangentes, ou deve-se dar liberdade para um maior desenvolvimento tecnológico?

Este trabalho não conseguirá dar resposta às grandes questões colocadas, mas vai procurar, introduzindo dados recentes, sumarizar a arquitetura nacional e internacional, que faz parte desta governança, de forma a identificar os principais atores, meios e práticas, que permitam, mais especificamente, a Portugal consolidar a sua cibersegurança.

Supõe-se que, tendo adotado a primeira estratégia nacional de cibersegurança apenas na segunda década do século XXI, Portugal não possui uma defesa no domínio cibernético muito desenvolvida ou consolidada. Considerando ainda que este tipo de ameaças não conhece fronteiras terrestres ou marítimas, os mecanismos de cooperação internacional encontram-se em constante evolução, beneficiando com isso a cibersegurança de Portugal.

Este trabalho estrutura-se em vários capítulos. Em primeiro lugar, é proposta uma contextualização conceptual e histórica da cibersegurança. Em segundo, é feito um enquadramento jurídico e institucional da mesma, a vários níveis. Considerando que o ciberespaço se afigura um fenómeno transfronteiriço, a cooperação interestatal e a complementaridade das convenções internacionais com as regulações nacionais são fundamentais para assegurar uma proteção eficaz e uma resposta coerente.

A secção seguinte evidencia as tendências em cibercriminalidade dos dois últimos anos, em Portugal, explicando a sua natureza, origem e alvo. O quarto capítulo é dedicado ao papel das Forças Armadas Portuguesas na prevenção e recuperação dos incidentes, assim como na formação e educação no domínio cibernético. De seguida, são apresentadas várias formas e mecanismos de cooperação internacional, e conclui-se com um breve olhar sobre a inteligência artificial.

1. Contextualização: a cibersegurança

A cibersegurança e a ciberdefesa são dois conceitos fundamentais quando se fala de proteção no espaço cibernético. A diferença entre os mesmos revela-se ténue, mas importante de esclarecer.

A ciberdefesa constitui uma responsabilidade alocada às Forças Armadas, com a missão de garantir a vigilância e, através de métodos preventivos, assegurar a defesa da soberania nacional. Implica uma navegação confiante no ciberespaço, de forma a conseguir proteger e deter os atos ilícitos neste domínio (Nunes, 2012, p.122).

Por sua vez, a cibersegurança também consiste na vigilância e na utilização de mecanismos que garantam a defesa da sociedade, dos indivíduos e das comunidades, dos seus direitos e liberdades, assim como dos bens e propriedade. Esta tarefa encontra-se sob a

responsabilidade complementar das Forças de Segurança e dos Serviços de Segurança (Ralo, 2013).

Segundo a conceptualização oficial do Centro Nacional de Cibersegurança, a cibersegurança define-se como um "conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem" (CNCS, 2020). Em linguagem corrente, cumprir uma regra de cibersegurança seria não guardar as palavras-passe nos computadores públicos ou não guardar os ficheiros confidenciais numa *drive* partilhada.

O conceito de cibersegurança surgiu na década de 70, quando o programador Ray Tomlinson criou o programa *Reaper*, que perseguia e eliminava o intruso *Creeper*, criado antes pelo investigador Bob Thomas. *Reaper* foi assim o primeiro *software* de antivírus (Devies, 2021). No final da década de 80, apareceram dois programas de antivírus comerciais. Nos anos 90, com o início da massificação do uso da internet, aumentou consideravelmente a produção de sistemas de proteção, sobretudo para os sistemas de governo, cuja informação afigurava-se como o alvo preferido dos *hackers*. Nos anos 2000, os ciberataques começaram a crescer em intensidade, frequência e gravidade (Devies, 2021).

Atualmente, existem vários tipos de ciberameaças, tais como, ciberterrorismo, cibercriminalidade, ciberespionagem e ciberguerra. Dentro de cibercriminalidade destacam-se: *ransomware* (bloqueio do acesso a um sistema ou a um computador até uma quantia de dinheiro ser paga), *malware* (software destinado a danificar um sistema ou ganhar acesso não-autorizado a um computador), *cryptojacking* (o uso secreto da energia de um computador para criar cripto-moeda), desinformação, negação de acesso, ameaças não-maliciosas e ataques contra cadeias de fornecimento (Interpol, 2022). Ainda no que toca à cibercriminalidade, pode-se distinguir dois tipos de ocorrências. Existem crimes que resultam das condições específicas da informática, como é o caso de *ransomware*. Outros crimes usufruem do espaço informático, porém, enquanto um meio para um fim; por exemplo, a burla *online* (Observatório de Cibersegurança, 2020, p.50).

Quanto aos dados, estes podem ser indevidamente divulgados, alterados ou destruídos. No âmbito da ciberguerra, podem ser cortadas as redes de eletricidade e Internet, e afetadas as redes logísticas de abastecimento.

Para a Agência Europeia para a Segurança das Redes e da Informação (ENISA), as principais tendências atuais em cibersegurança são a primazia de *ransomware* e das questões financeiras enquanto motivações, o crescente aparecimento de *criptojacking*, o aumento dos incidentes não-maliciosos e os crescentes ataques no setor da saúde. Ao mesmo tempo, constata-se uma maior agilidade dos governos na resposta às ciberameaças, e avanços tecnológicos por parte das empresas. São exemplos destas tecnologias a gestão da identidade, os processos de autenticação, e o recurso a técnicas de cifra e de *blockchain* para a proteção de dados (Carballo-Cruz, Cerejeira e Esteves, 2022, p.37).

2. Enquadramento jurídico e institucional: internacional, europeu e nacional

Considerando a complexidade e a gravidade de ataques e incidentes no espaço cibernético, surgiu a necessidade de regular, legalmente, estes atos, descrevendo a sua ação e a penalidade associada. Da mesma maneira, considerando as ciberameaças um fenómeno global, que pode afetar em igual medida todos os países, a comunidade internacional e as entidades políticas assinaram algumas convenções, com vista a uma uniformização das penalidades e reforço da cooperação contra as ameaças. Neste âmbito, e de grande relevância para o tema deste trabalho, destacam-se três níveis de enquadramento jurídico – internacional, europeu e nacional.

Contexto internacional

Ao nível internacional, poucos são os acordos que estipulam condições ou regras legais no domínio cibernético. A maior parte das regulações, ou a forma como a lei internacional poderá aplicar-se ao domínio da cibersegurança, delibera-se ao nível nacional ou regional, por instituições académicas ou organizações não estatais (e.g., Comité Internacional da Cruz Vermelha e grupos de especialistas independentes). Por exemplo, o fruto do trabalho de um destes grupos foi a elaboração dos dois Manuais de Tallinn, que apresentam uma análise da transposição das leis e princípios internacionais à segurança e defesa nacionais (Hollis, 2021).

De entre as entidades institucionais, destaca-se o papel da ONU, ainda que o seu trabalho seja modesto e recente. A primeira regulação vinculativa sobre cibersegurança das Nações Unidas (NU) foi aprovada apenas em 2021. Esta regulação, nº 155, pretende uniformizar as condições de aprovação dos veículos, para a sua colocação no mercado, consoante as regras de gestão dos sistemas informáticos e das técnicas de cibersegurança (UNECE, 2021).

No seio das Nações Unidas, identificam-se várias entidades que desenvolvem a sua atividade nesta esfera. O primeiro a ser destacado é o grupo de trabalho de objetivo aberto, para a segurança de e no uso de tecnologias de informação e comunicação (*open-ended working group on security of and in the use of information and communications technologies 2021-2025*). Estabelecido em 2020, pela Resolução 75/240 da AGNU, admite a participação de todos os membros das NU, Estados observadores, e organizações inter e não-governamentais, que tenham estatuto consultivo junto do ECOSOC. A missão consiste no estabelecimento de regras, normas e princípios sobre o comportamento dos Estados no ciberespaço; no desenvolvimento de iniciativas que promovam a segurança de informação e comunicação; na garantia do diálogo internacional, sob os auspícios das NU; assim como na promoção do conhecimento e entendimento sobre o espaço cibernético (UNODA, 2021). Por exemplo, em dezembro 2021, foi realizada uma sessão pelo Grupo de Trabalho, durante a qual foi feita uma introdução para o enquadramento internacional, relevante para moldar os comportamentos dos Estados no ciberespaço (UNIDIR, 2021).

A segunda entidade é o Comité de Cibercrime *ad hoc*, um comité intergovernamental, estabelecido com a Resolução 74/247 da AGNU, cujo objetivo consistia na redação da nova convenção do cibercrime até 2023 (Digwatch, 2023). A deliberação no contexto desta convenção, sobre o combate ao uso de tecnologias de informação e comunicação para fins criminosos, começou em março de 2022, sendo aprovada em maio pela Resolução da AGNU 75/282.

O Conselho da Europa adotou a Convenção sobre o Cibercrime na Cimeira em Budapeste, em novembro 2001. Este instrumento multilateral foi apresentado para a respetiva assinatura e ratificação dos 47 Estados-membros, tal como de outros meramente observadores. Todavia, apenas 27 Estados assinaram o tratado. Não obstante, salienta-se que este constitui o primeiro acordo internacional que regula o crime informático, através da uniformização das leis nacionais e da melhoria das técnicas de investigação.

Para além disso, o Conselho aprovou o Protocolo adicional à Convenção que criminalizava os atos de natureza racista ou xenófoba cometidos através de sistemas informáticos (2003), e o Protocolo adicional para o reforço da cooperação e partilha de provas eletrónicas (2022). Em 2007, foi assinado o acordo que proibia o uso de sistemas informáticos para a exploração e abuso sexual das crianças.

Ao nível internacional, destaca-se ainda a Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais, conhecida como Convenção de Malabo, adotada em 2014. O presente documento apresenta definições importantes para entender e regular o domínio cibernético (Digwatch, 2023). Importa referir ainda a existência de centros de operações, criados e geridos pelo setor privado. Um exemplo disto é Indra, uma empresa multinacional de tecnologia e consultoria, que, em 2013, criou o Centro de Operações de Cibersegurança, a fim de providenciar sistemas de segurança e proteção a empresas e organizações (Indra, 2013).

Contexto da União Europeia

A importância da cibersegurança ao nível europeu, deu origem, em 2004, à Agência Europeia para a Segurança das Redes e da Informação (ENISA), com o intuito de dar assistência e pareceres; promover a cultura e a prática de segurança nas redes de informação, nos serviços e nos produtos, aos Estados-membros, setor empresarial e instituições europeias; incentivar a cooperação e ciber-resiliência; e coordenar uma resposta em situações de ciberataque, ao abrigo do Regulamento (UE) 2019/881, também conhecido como *Cibersecurity Act* (Sen, 2022).

Importa sublinhar o direito fundamental à proteção de dados pessoais, ao abrigo do artigo 8º nº 1 da Carta de Direitos Fundamentais da União Europeia e do artigo 16º nº 1 do Tratado de Funcionamento da União Europeia.

Os centros de partilha de informação e análise (centros EE-ISA) são organizações não-lucrativas que procuram agilizar a ajuda perante as ciberameaças. Criada em 2016, a Organização Europeia de Cibersegurança (ECSO) providencia apoio à Comissão Europeia na parceria público-privada no domínio cibernético, e financia o projeto de ciber-

-resiliência da UE, no âmbito do Horizonte Europa (Sen, 2022). Ao nível de instituições, cabe ainda destacar o Centro de Investigação Conjunta (JRC) da Comissão Europeia. Um dos seus contributos prende-se com a elaboração da taxonomia da cibersegurança, que inclui um dicionário dos termos cibernéticos, história dos ataques e algumas perspetivas sobre possíveis medidas de proteção.

Existem as equipas de resposta aos incidentes de segurança de computador (CSIRT) e as equipas de resposta de emergência (CERT). Em 2018, entrou em vigor a Regulação Geral de Proteção de Dados.

Em 2020, foi adotada a nova Estratégia de Cibersegurança da UE, substituindo a primeira de 2013. A Estratégia sublinha a necessidade de atualizar as diretivas de cibersegurança e proteger as estruturas críticas. As diretivas dos sistemas e das redes informáticas estabelecem as capacidades nacionais que os Estados-membros devem ter para conseguirem implementar as medidas de proteção de dados, gestão de risco e prevenção dos cibercrimes. Prescrevem ainda a cooperação europeia e a monitorização nacional dos setores críticos, potenciais alvos dos ciberataques. A primeira diretiva (NIS) foi lançada em 2016, e a segunda (NIS2) em 2020.

A Europa Digital é o programa que procura investir em capacitação de talento em cibersegurança e em criação de infraestrutura e tecnologias de proteção. Por sua vez, *Connecting Europe Facility* é um investimento no reforço das capacidades dos Estados-membros e da cooperação entre eles, para a implementação da Estratégia de Cibersegurança. Há, assim, esforços no âmbito da ciberdiplomacia, quer com a cooperação na prevenção do ataque, quer na resposta ao mesmo, incluindo o regime de sanções desde 2019 (Sen, 2022).

Contexto português

À luz da Constituição da República Portuguesa (CRP), pode-se encontrar no artigo nº 35, "a proibição de uso da informática para tratamento de dados de cariz privado", tais como convicções políticas e religiosas; convicções filosóficas e filiação política ou sindical (adição de 1982); e origem étnica (adição de 1997). A lei constitucional surge, assim, como primeira garante da proteção de dados no espaço informático.

Em 1991, foi promulgada a Lei da Criminalidade Informática, o documento que tipificava a criminalidade ao nível das tecnologias de informação e comunicação. A Convenção de Budapeste de 2001 assume, no ordenamento jurídico português, a forma da Resolução da Assembleia de República nº 88/2009. A mesma foi reestruturada por via da nova Lei do Cibercrime, Lei nº 109/2009.

Atualmente, a defesa nacional encontra-se prevista no artigo nº 273 da CRP, sendo que é não só uma obrigação do Estado garantir a defesa nacional, como também assegurar a sua integridade territorial, liberdade e segurança a qualquer tipo de ameaça. Desta forma, infere-se que a segurança das ciberameaças está igualmente abrangida pelo artigo. O regime jurídico que regula a segurança do ciberespaço é o Decreto Lei nº 65/2021, de 20 de julho.

A primeira Estratégia Nacional de Segurança do Ciberespaço de Portugal foi criada em 2015. A mesma foi revista em 2019 e traça os objetivos do Estado até 2023. Neste documento são definidos os objetivos estratégicos de foro cibernético, nomeadamente a maximização da resiliência digital através da inclusão e colaboração em rede; a promoção da capacidade nacional de inovação, para um desenvolvimento socioeconómico e cultural; e a gestão dos recursos para garantir a sustentabilidade da segurança do ciberespaço (CNSC, 2019, p.11).

Os eixos de intervenção nos quais se apoia a nova estratégia delineiam uma linha de ação concreta. São eles: estrutura de segurança do ciberespaço; prevenção, educação e sensibilização; proteção do ciberespaço e das infraestruturas; resposta às ameaças e combate ao cibercrime; investigação, desenvolvimento e inovação; e cooperação nacional e internacional (CNSC, 2019, p.12-23).

A estratégia de 2015 encontrava-se alicerçada em cinco grandes pilares, a subsidiariedade, complementaridade, cooperação, proporcionalidade e sensibilização; enquanto a de 2019 privilegia subsidiariedade, complementaridade e proporcionalidade.

A Lei nº 58/2019, de 8 de agosto, assegurou a execução e implementação na ordem jurídica portuguesa do Regulamento Geral sobre a Proteção de Dados da UE. Foi criado o registo nacional de identificação com a finalidade de salvaguardar todo o núcleo confidencial relativo aos dados, bem como a sua responsabilização em caso de quebra de confiança, ao abrigo da Lei nº 2/73 de 10 de fevereiro.

Ao nível institucional, diversas entidades têm competência e domínio em cibersegurança, como a Polícia Judiciária, o Gabinete de Cibercrime do Ministério Público, a Comissão Nacional de Proteção de Dados e o Centro Nacional de Cibersegurança. Este foi fundado em 2014 e encontra-se incumbido da missão de ser a autoridade nacional de cibersegurança, na senda do Gabinete Nacional de Segurança.

3. As ciberameaças em Portugal: as tendências nos últimos anos

Portugal, como todos os países da comunidade internacional, vive num mundo onde o ciberespaço está a ganhar cada vez mais destaque e poder, e tem de se adaptar para responder de forma rápida e concreta a todo o tipo de ameaças que possam surgir. Costuma-se dizer que o conhecimento é a chave para o sucesso, pelo que a posse da informação no domínio cibernético ou o controlo das tecnologias de informação e comunicação poderão colocar o seu detentor numa posição privilegiada sobre os seus interlocutores.

Por este motivo, Portugal nos últimos anos tem verificado um aumento consistente das ações maliciosas no ciberespaço (entenda-se por ações maliciosas os ciberataques cirúrgicos, mas poderosos, a pessoas individuais, empresas privadas e a instituições públicas e estatais). Como exemplo recente de ataques a instituições do Estado português, nota-se a interceção dos documentos classificados da NATO enviados ao Estado-Maior-General das Forças Armadas (EMGFA), em setembro 2022 (Correia, Casanova e Lusa, 2022).

Na verdade, as informações que passam pelos altos níveis são alvos cobiçados. O facto de o Estado ser atacado nas suas sedes pode suscitar uma série de problemáticas, referentes à estabilidade do Estado junto da sua população e parceiros.

Por exemplo, a destruição de informação vital para a ação social do Estado deixa a população desamparada, em termos de apoios essenciais de equilíbrio social; um atentado às infraestruturas críticas[1] pode significar um ataque à própria soberania. Pode existir uma quebra de sigilo na troca de informação entre o Estado português e as organizações ou Estados com quem se relaciona. Consequentemente, o Estado pode transparecer alguma incapacidade de se proteger a si mesmo, o que transmitirá uma imagem de incompetência e fraqueza do poder governativo. As suas relações com organizações e parceiros poderão encontrar brechas ou fraquezas, pela perda de confiança, com resultados nefastos em todos os domínios.

No que toca às tipologias, as ações maliciosas podem ter origem em atores estatais, paraestatais e não estatais, e em atores internos ou externos a determinada entidade (empresa, instituição ou Estado). Os atores estatais são "entidades que atuam em nome de um órgão governamental, como, por exemplo, governos, representações oficiais, forças armadas ou serviços de informações" (Observatório de Cibersegurança, 2020, p.67). Os paraestatais são vinculados, dirigidos e/ou financiados pelo Estado, sem ligações formais. De entre estes, destacam-se os ciberterroristas e os *hackers* que vendem os seus serviços às estruturas oficiais. Os atores não estatais são os cibercriminosos, *hacktivistas*, *insiders*, empresas ou *freelancers* (p.67-8). Os atores predominantes no panorama de cibercrimes em Portugal são atores estatais, *hacktivistas* e cibercriminosos. Em 2021, a estes juntaram-se os *cyber-offenders,* cujo objetivo é perturbar as vítimas ou criar disrupções no funcionamento dos sistemas, através de assédios ou destruição de informação (Observatório de Cibersegurança, 2022, p.3-4).

As motivações variam entre o niilismo político (visando a destruição das instituições políticas existentes), o ganho financeiro, o vandalismo informático (em que, sem um objetivo concreto, se procura danificar os equipamentos ou informações digitais) e, eventualmente, o terrorismo. Em Portugal, os cibercriminosos regem-se maioritariamente pelos motivos económicos, extorquindo dinheiro a privados ou realizando fraudes para obter credenciais bancárias. Ao nível das instituições do Estado, podem ser contratados para ciberespionagem nos domínios político, estratégico, militar, económico e operacional, procurando obter informações, mas também sabotar ou comprometer os sistemas (Observatório de Cibersegurança, 2020, p.68).

Por sua vez, os *hacktivistas* em Portugal procuram desestabilizar os sistemas ou introduzir danos reputacionais em organizações, empresas ou indivíduos. Destacam-se as

1 Por infraestruturas críticas entendem-se setores ou equipamentos "cuja destruição total ou parcial, disfunção ou utilização indevida possa afetar, direta ou indiretamente, de forma permanente ou prolongada" o funcionamento de determinados setores (como energia, transporte, banca, saúde), dos órgãos de soberania ou da segurança nacional, ou os valores básicos da sociedade, como o bem-estar (Associação Portuguesa de Segurança, 2023).

práticas de ameaça do ataque, sem o ataque efetivo, expondo as fraquezas de uma entidade, e de divulgação das suas vulnerabilidades. Assim, os *hacktivistas* procuram o reconhecimento próprio ou a transmissão de uma determinada mensagem (Observatório de Cibersegurança, 2020, p.68). No início de 2022, houve ataques ao grupo de média, Impresa, e à Vodafone, com a destruição de dados, o que comprometeu a disponibilidade da informação e de serviços (Observatório de Cibersegurança, 2022, p.5).

Os relatórios do Observatório de Cibersegurança (2020 e 2022) evidenciam igualmente as tendências dos cibercrimes. Por exemplo, os incidentes mais frequentes em 2019 foram o *phishing* e a infeção com *malware* (incluindo *ransomware*), seguindo-se o compromisso de conta, indisponibilidade de serviço, destruição e corrupção de dados, burla *online* e furto de identidade (2020, pp.47 e 63).

Os setores mais afetados pelos incidentes de segurança tecnológica são os de informação e comunicação, TIC e telecomunicações. Seguem-se na lista as infraestruturas digitais; os prestadores de serviços de internet; a educação, ciência, tecnologia e ensino superior; e por fim, a banca. Os sistemas de controlo industrial foram igualmente apontados como alvos preferenciais, pelo seu carácter crítico (2020, pp.44 e 69).

Comparando com alguns valores europeus, em 2019, Portugal sofria menos incidentes de cibersegurança do que a média dos países na União Europeia (8% das empresas em Portugal, e 13% na UE; 27% dos indivíduos em Portugal, e 37% na UE).

Em 2021, destacam-se as práticas de roubo de informação, através de métodos como *phishing* (via *email*), *smishing* (SMS) e *vishing* (telefone). A burla e fraude *online* continuam a assumir relevância, enquanto o *ransomware* e o comprometimento de contas registaram um decréscimo (Observatório de Cibersegurança, 2022, p.3).

Destaca-se, igualmente, os ataques a cadeias de fornecimento. Em Portugal, o setor dos transportes e logística foi identificado como o segundo mais afetado por ataques de *phishing* e *smishing* em 2021, a seguir ao setor da banca (Observatório de Cibersegurança, 2022, p.9).

O relatório de 2022 conclui que a ocorrência de cibercrimes (e.g., negação de acesso) diminuiu, em comparação com o ano de 2021. Contudo, os crimes que usam os meios informáticos para os seus fins, como por exemplo, a burla ou fraude *online*, aumentaram. Aumentou igualmente a percentagem dos últimos em relação ao total dos crimes registados em Portugal (2022, p.10).

Pode-se supor que, muitas das vezes, em Portugal, a iliteracia informática do povo português assume-se como fator primordial para a possibilidade da existência de um incidente de segurança no ciberespaço. A suposição advém do facto de os ataques que têm maior expressão na estatística final poderem ter sido combatidos com um melhor conhecimento do ambiente informático, que permitiria ao utilizador reconhecer que estava perante um ciberataque (e.g., *phishing* ou *rasomware*), e, assim, tomar as medidas preventivas convenientes.

4. Forças Armadas (FA) portuguesas: o potencial e os desafios em cibersegurança

Perante as tendências e as vulnerabilidades acima apresentadas, Portugal tem investido na proteção cibernética de várias formas. Para aumentar a ciber-resiliência e a capacidade de resposta a um incidente, e melhorar a gestão das capacidades disponíveis, humanas e materiais, com o mínimo de prejuízo, procura-se seguir um modelo de atuação nos seguintes moldes, baseado no *NIST cybersecurity framework*:

– Identificar: o que deve ser protegido;
– Proteger: implementar os procedimentos tendentes à proteção da capacidade;
– Detetar: implementar mecanismos que detetem a ocorrência de um incidente;
– Responder: desencadear os mecanismos para finalizar o incidente;
– Recuperar: restaurar as capacidades afetadas pelo incidente.

Desta maneira, a formação, cuja falta foi apontada acima, assume um papel de destaque, assim como a modernização dos equipamentos e da tecnologia. Estes dois aspetos, devidamente geridos e em sinergia de esforços, poderão constituir um fator considerável para a dissuasão de uma eventual tentativa de um ato malicioso, ou seja, para a redução do risco e exposição a ciberataques. As Forças Armadas (FA) nacionais detêm a crucial responsabilidade da defesa militar do Estado, com esforços reconhecidos nesta direção.

Com o reconhecimento do ciberespaço como um domínio operacional, as FA acumularam a função da proteção, prevenção e combate às ciberameaças e cibercriminalidade. A sua atividade encontra-se regulada pelos mecanismos nacionais e alianças multinacionais, observando-se, igualmente, uma grande complementaridade entre os esforços nacionais e internacionais.

A título de exemplo, a Orientação Política para a Ciberdefesa (2013) prescrevia a incorporação da capacitação nacional, no âmbito do Planeamento de Defesa Militar, *NATO Defence Planning Process* e *EU Capability Defence Plan*. Segundo o antigo ministro da Defesa Nacional, Azeredo Lopes, as diretrizes da NATO e UE concederam um impulso às FA nacionais, para a sua modernização e qualificação. Por exemplo, a adesão portuguesa à PESC contribuiu para atenuar as falhas na ciberdefesa e favoreceu as indústrias e tecnologias para a ciberdefesa nacional (Lusa, 2018). O diretor do CNSC, Lino Santos, acrescenta que a proteção cibernética das infraestruturas críticas começou a intensificar-se apenas por influência europeia (2018, p.25).

Por influência ou com ajuda internacional, as FA portuguesas começaram a investir neste domínio. A título de exemplo, seguindo os desenvolvimentos da Aliança Atlântica, lançaram uma extensão nacional do projeto da NATO *Multinational Cyber Defence on Education and Training* (MNCDE&T), que procura um aumento da formação, treino e investigação nacionais, englobando as instituições públicas, como o Centro Nacional de Cibersegurança, universidades, empresas e bancos (Santos, 2018, p.42).

Referindo-se mais especificamente os ramos das Forças Armadas, a cibersegurança revela-se fulcral nos três. Um ciberataque aos sistemas de bordo ou de orientação pode-

rão provocar erros nos cálculos quanto ao posicionamento, distância ou recursos energéticos. Os sistemas conectados via satélite ou com ligação à internet podem ser alvo dos *hacktivistas*. A frequente complexidade dos materiais e equipamentos leva a que as preocupações com a diminuição dos custos prevaleçam sobre as de cibersegurança (Marques, 2019, p.16), podendo tornar os equipamentos mais vulneráveis aos ciberataques, também por este motivo. Os incidentes cibernéticos podem resultar, ainda, em problemas na identificação e perda de carga, devido ao roubo de informação. Adicionalmente, não existem regulamentos para a ação em situações de ciberataque, pelo menos, no espaço marítimo (Marques, 2019, p.16). Estes revelam-se apenas alguns dos incidentes que podem ocorrer durante um ciberataque.

Estas vulnerabilidades podem constituir alvos atrativos, por exemplo, para os cibercriminosos contratados pelas entidades estatais, no âmbito da ciberguerra; ou para os ciberterroristas, numa tentativa de provocar desorganização na ordem nacional.

A fim de prevenir estes incidentes, a estrutura da ciberdefesa nas FA foi dividida entre duas entidades. A primeira é a Comissão Coordenadora da Capacidade de Resposta a Incidentes de Segurança Informática (CC-CRISI), onde os representantes dos três ramos das FA definem as políticas de segurança da informação, decidem e coordenam as respostas aos ciberincidentes. A segunda é o Grupo de Resposta a Incidentes de Segurança Informática (GRISI), onde os especialistas técnicos dos três ramos procuram definir a reação e recuperação dos sistemas danificados (Silva, 2015, p.42-43).

Por sua vez, embora não de natureza estritamente militar, mas de papel fulcral, o Centro Nacional de Cibersegurança (CNCS) assumiu a coordenação operacional e de autoridade nacional em cibersegurança, a recolha de informação e o desenvolvimento de capacidade de reação através de equipas integradas na Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática. O seu mandato foi reforçado com o Regime Jurídico da Segurança do Ciberespaço, aprovado em 2018 (Carballo-Cruz, Cerejeira e Esteves, 2022, p.49). Em 2019, o CNCS publicou o Quadro Nacional de Referência para a Cibersegurança, que contém requisitos mínimos de segurança de informação recomendados para lidar com os desafios cibernéticos.

Cada ramo das FA também possui as suas políticas de ação e proteção para lidar com estes desafios. Os seguintes são apenas alguns exemplos. Em primeiro lugar, a política de segurança da Força Aérea portuguesa assenta em cinco aspetos: criação de diretivas de segurança, gestão e análise de risco, detenção de intrusões, equipas de reação e cultura de segurança (Silva, 2015, p.36-38).

Em segundo lugar, a cibersegurança da Marinha é dirigida através do Centro de Resposta que existe no Centro de Comunicações, de Dados e de Cifra da Marinha (CDCM), que pertence ao Comando Naval. "Os navios encontram-se equipados com ferramenta de análise em tempo real dos alertas de segurança dos equipamentos das redes, o *Security Information and Event Management* (SIEM)" (Antunes, 2013, p.38).

Por fim, o Exército tem vindo a consolidar uma visão doutrinária para uma capacitação em ciberdefesa, com o imprescindível contributo da Arma de Transmissões. Como resultado, foram elaborados o Estudo para a Superioridade de Informação das Forças

Terrestres (2010), o plano para a implementação deste estudo (2011), o Módulo Tático *Computer Incident Response Capability (*CIRC) e o Exercício *Ciber Perseu* (2012) (Nunes e Carvalho, 2021, p.10).

O *Ciber Perseu* consiste num exercício prático virtual que permite avaliar a capacidade de resposta aos ciberataques simulados, aferindo o conhecimento real em normas e procedimentos em vigor (CEMFA notícias, 2013 e 2019). Nestes exercícios participam atores de variados setores como comunicações, energia, transportes, entre outros, assim como entidades públicas e privadas, nacionais e estrangeiras.

Como foi possível aferir, a cibersegurança afeta quase todos os setores da atividade humana. Desta forma, revela-se imprescindível a cooperação nacional, não apenas entre os três ramos das FA, nem só entre as instituições públicas e o setor privado, mas também entre as forças e serviços de segurança. No que toca às responsabilidades dos últimos, e diferenciando pela tipologia do ciberincidente: a cibersegurança, no que toca a cibercrime e *hacktivismo,* é da responsabilidade das forças de segurança, tendo a Polícia Judiciária competência reservada nas investigações; a ciberespionagem e o ciberterrorismo, dos serviços de informação; enquanto que a ciberdefesa, durante a ciberguerra, é da responsabilidade das Forças Armadas (Antunes, 2013, p.33).

Supõe-se que, por causa desta variedade, um único Centro de Cibersegurança não é suficiente, devendo existir outros para cibercrime, ciberdefesa e serviços de informações (Antunes, 2013, p.33). Importa ainda referir que o investimento em ciberdefesa foi reforçado, passando para 51 milhões de euros entre 2019-2030. Mas serão estes recursos suficientes para que as Forças Armadas Portuguesas enfrentem uma ciberguerra e ameaças híbridas?

5. Cooperação internacional: parceiros e mecanismos

O contexto europeu atual surge pautado pela guerra na Ucrânia. A guerra veio substituir a situação pandémica, que moldava as relações internacionais e as preocupações de segurança (inclusive, cibersegurança) nos anos anteriores. Com esta mudança na geopolítica, notaram-se algumas alterações no que toca aos principais atores e métodos de cibercriminalidade. Antes, os cibercriminosos procuravam obter dados sensíveis, sobretudo nos setores da banca ou da saúde, com vista a ganhos financeiros. Numa situação de guerra, salientam-se os atores estatais e paraestatais que usam ciberespionagem e sabotagem, dirigidas aos setores de administração pública, instituições do Estado e infraestruturas críticas. A disrupção em cadeias de fornecimento e a desinformação são outras técnicas frequentemente usadas agora. Os *hacktivistas* poderão estar mais motivados ainda, por razões políticas ou ideológicas (Observatório de Cibersegurança, 2022, p.6-7).

Relembra-se uma das tendências em Portugal – o aumento do número de cibercrimes, em relação ao total de crimes no país. O mesmo acontece por todo o mundo. Por isso, todas as declarações ou regulamentações, sejam europeias ou nacionais, atribuem um grande destaque à cooperação internacional, dada a natureza da ameaça cibernética, que não conhece fronteiras. Esta interação abrange as instituições estatais e os setores

industrial, comercial e tecnológico, do domínio cibernético (Monteiro e Pinto, 2016, p.4). Portugal tem cooperado e beneficiado de várias parcerias internacionais, que serão expostas abaixo.

NATO

A ciberdefesa passou a integrar a agenda permanente da NATO, desde 2002, e o conceito estratégico, desde 2010. Após o ciberataque massivo à Estónia (2007), a NATO emitiu a primeira Política de Defesa Cibernética (2008). Desta forma, Portugal tinha de proteger as suas próprias instalações, mas podia pedir auxílio à Aliança, em caso de um ciberataque. A garantia de ajuda coletiva ficou consagrada pela introdução da possibilidade de invocar o artigo n.º 5 do Tratado em situações de ciberataque massivo (desde 2014). Em 2018, foi criado o Cyber Operation Centre, que permite a coordenação de operações.

As estruturas portuguesas têm também beneficiado da liderança de vários projetos da NATO, permitindo adquirir conhecimentos e experiências cibernéticas. Exemplos são os *Smart Defence Projects*, a NATO Communications and Information Systems School (NCISS) e a sua fusão em NCI Academy. Por fim, as forças nacionais ganham treino relevante em exercícios como *Cyber Coalition* e *Locked Shields*.

União Europeia

Na UE, diversas entidades estão encarregadas de delinear as orientações estratégicas e operacionais, apoiar as investigações e qualificações, providenciar material técnico e forense, e disponibilizar tecnologias proativas e reativas, aos Estados-membros, nos domínios de cibersegurança e ciberdefesa. Para nomear apenas algumas: a Agência da União Europeia para a Cibersegurança e o Centro Europeu Especializado em Cibercriminalidade.

Portugal tem acumulado prática, experiência e conhecimento através da participação em exercícios de treino, como o ciberataque ao Estado imaginário *Blueland* e o projeto *Cyber Ranges* da UE; e através da *Cyber Defence Training and Exercicse Coordination Platform*. Adicionalmente, usufrui da partilha de informações, fazendo parte do *Pooling & Sharing* e da EU PESCO *Cyber Threat and Incident Repsonse Information Sharing Platform*, desde 2018.

Por outro lado, contribui para o reforço da formação e treino, coliderando a Disciplina de Ciberdefesa do Grupo de Treino Militar da União Europeia (com França), a Plataforma de Treino e Exercício para a Ciberdefesa, e o PESCO *Cyber Academy and Innovation Hub* (EU CAIH), que constitui uma extensão do projeto homólogo nacional português.

Por fim, como acima mencionado, a UE tem publicado regulações e diretrizes[2] para o combate das diferentes formas de cibercriminalidade, permitindo a Portugal construir um quadro jurídico nacional cibernético mais sólido.

2 De entre as publicações e trabalhos europeus identificam-se: EU Cybersecurity Act (2019), EU-Wide Cybersecurity Certification Scheme, Stakeholder Cybersecurity Certification Group, Blueprint for Coordinated Response to Major Cyber-Attacks (2013), Joint Cyber Unit (2021), entre outros (Sen, 2023).

Organização para a Cooperação e Desenvolvimento Económico

A OCDE desenvolve políticas estandardizadas para o reforço da confiança nas tecnologias de informação e comunicação. Portugal poderá reforçar a sua capacidade de gestão de riscos e investigações em segurança digital a partir das suas recomendações, usufruindo do debate no Fórum Global sobre Segurança Digital para a Prosperidade.

Organização de Segurança e Cooperação na Europa

A OSCE aposta nas medidas de criação de confiança entre os Estados, a fim de reduzir os riscos de ciberconflito, causados por erros de cálculo ou perceções erradas. Para isso, a OSCE providencia consultas sobre potenciais ciberincidentes, regula a escalada de tensões, abre espaço para a exposição das abordagens nacionais, e promove a cooperação em matérias de informação e equipamentos tecnológicos, sobretudo relativos às estruturas críticas, de forma a fortalecer a sua ciberdefesa.

Conselho da Europa

O Conselho da Europa procura sensibilizar para o risco de ciberataques e cibercrimes. Como foi mencionado na segunda secção, a Convenção de Budapeste (2001) estabeleceu uma política comum, de tipificação dos crimes informáticos com vista a facilitar a partilha de conhecimento e informações (Carballo-Cruz, Cerejeira e Esteves, 2022, p.51).

Nações Unidas (NU)

As Nações Unidas providenciam recomendações para a articulação dos pressupostos jurídicos e legislativos com a implementação de políticas públicas.

A cooperação no âmbito das NU permite gerir e minimizar o impacto da cibercriminalidade de forma mais eficaz. Para apresentar apenas um exemplo, Portugal deve aproveitar o programa de Cibersegurança e Novas Tecnologias, ajudando o seu setor privado a prever e atenuar os efeitos da utilização das tecnologias por terroristas ou outros grupos violentos (Carballo-Cruz, Cerejeira e Esteves, 2022, p.51). Foi, também, possível providenciar um ambiente cibernético mais seguro para os cidadãos portugueses com a criação do Relator Especial sobre o Direito à Privacidade.

Por fim, parece interessante considerar a possibilidade da aplicação do artigo n.º 51 da Carta das Nações Unidas, e a legítima defesa numa situação de ciberataque.

6. O futuro presente: as ameaças híbridas e a inteligência artificial

Olhando para a geração atual, cada vez mais digital, assistimos à evolução constante de novas formas de ameaça e influência através do ciberespaço. Apesar de não existir uma definição que gere concordância, pode-se dizer que este tipo de ameaças englobam uma nova realidade, abrindo portas à denominada guerra híbrida. De acordo com o

European Centre of Excellence for Countering Hybrid Threats, "uma característica inerente das ameaças híbridas envolve confundir dicotomias tradicionais e criar ambiguidade e incerteza. O objetivo é atingir os interesses e objetivos nacionais por meio de estratégias como minar a confiança do público nas instituições democráticas, aprofundar a polarização doentia, desafiar os valores centrais das sociedades democráticas, interferir nas eleições democráticas e afetar a capacidade de tomada de decisão dos líderes políticos, mesmo pelo uso de meios militares" (Hybrid CoE, 2022).

As ciberameaças revelam-se híbridas por natureza. Por exemplo, a capacidade de interferir nos assuntos internos dos outros Estados, alterando ou manipulando os dados, muitas vezes sem provas físicas e claras, constitui um ato naquela zona cinzenta que existe entre guerra e paz. Um ciberataque pode não ser um motivo de guerra entre dois países, mas contribui para um clima de tensão, comprometendo a coexistência pacífica.

Desta forma, as medidas que possam e venham a ser implementadas para segurança do ciberespaço devem contemplar, com uma avaliação cuidada e prudente, a utilização das tecnologias emergentes, nomeadamente, a inteligência artificial (IA). As ideias futuristas da IA dominar o mundo estão a tornar-se uma realidade bem presente.

A IA, não sendo um novo fator no panorama do ciberespaço, começa hoje a ser objeto de regulamentação mais apertada, considerando a disponibilização, os avanços tecnológicos e o conhecimento da utilização deste tipo de capacidades, por indivíduos e/ou instituições que poderão causar a disrupção de sistemas públicos e privados. Neste campo, a União Europeia iniciou um processo de regulamentação europeu, de forma a estabelecer regras para a utilização, segurança jurídica, segurança da utilização e facilitação do desenvolvimento de tecnologias de inteligência artificial (Comissão Europeia, 2021). Contudo, o processo revela-se recente e ainda não são claros os efeitos da mesma sobre a esfera de atuação do Estado português.

Considerações finais

No mundo atual, digital e globalizado, o ciberespaço ocupa, cada vez mais, um espaço prioritário na vida das pessoas, sendo, inclusive, reconhecido como o domínio operacional das Forças Armadas. A ciberdefesa abrange as ameaças à soberania do Estado, enquanto a cibersegurança engloba todo o espaço coletivo nacional. Existe uma panóplia de tipos de ciberameaças e possíveis formas de cibercrime, tais como ciberterrorismo, cibercriminalidade, ciberespionagem e ciberguerra.

Infelizmente, estes incidentes continuam a crescer e a ocupar cada vez maior destaque nos registos policiais. No contexto atual português, prevalecem os atores estatais, *hacktivistas*, cibercriminosos e *cyber-offenders*, enquanto principais atores. De entre as motivações, prevalecem as causas financeiras (no contexto pandémico), políticas e ideológicas (perante a guerra na Ucrânia). Os setores mais afetados são os de transmissão de informação, infraestruturas digitais, educação e ciência, e a banca. As cadeias logísticas também constituem alvos destacados.

No foro jurídico, poucas são as convenções internacionais que regulam o domínio cibernético. O principal organismo internacional é a Organização das Nações Unidas, embora os seus avanços sejam modestos. Sublinham-se, no entanto, os esforços das organizações regionais, como a União Africana, a União Europeia ou o Conselho da Europa. De facto, a UE fornece um abrangente quadro jurídico, transposto para a lei portuguesa. Portugal beneficia igualmente de diversos mecanismos, projetos e corpos direcionados para a análise, investigação e criação de diretrizes para os Estados-membros.

A Estratégia Nacional de Segurança do Ciberespaço portuguesa delineou as linhas orientadoras nacionais neste domínio, prescrevendo a incorporação dos compromissos assumidos com a União Europeia e a NATO. Estas duas entidades afiguram-se como as principais parceiras de Portugal que apresentam, de facto, mecanismos de atuação efetiva em caso de necessidade. No âmbito das outras parcerias, a cooperação centra-se na criação de uma cultura de cibersegurança, baseada na interação entre os atores estatais e não estatais. Esta cultura prende-se com a partilha de informação e conhecimento, formação e treino conjuntos, disponibilização de tecnologias e materiais, e emissão de recomendações e orientações (não pressupondo nenhuma aliança ou resposta assistida em caso de ataque). Esta realidade torna difícil a garantia da cibersegurança para um país que tenha limitados recursos financeiros, materiais e humanos.

Do acima exposto, infere-se que o Estado português é o único responsável por desenvolver as suas capacidades materiais, modernizadas e adequadas, a fim de garantir a sua defesa. Os dados evidenciam que os atores estatais, não estatais e privados, e as próprias Forças Armadas de Portugal, não são imunes aos ciberataques. A natureza híbrida dos acontecimentos cibernéticos, que integram a parte cinzenta das relações globais, implica uma grande flexibilidade de adaptação, necessidade de modernização e, inclusive, incorporação de práticas e equipamentos de inteligência artificial na garantia da ciberdefesa e cibersegurança nacionais.

Apesar da liderança ativa portuguesa em projetos de formação e treino, interroga-se se os esforços efetuados são suficientes para garantir uma literacia digital da população. Pode-se questionar se o Estado faz o suficiente para promover as sinergias internas, com as empresas ou autarquias locais, para a implementação das medidas de ciberdefesa junto da população. Pouco é feito para criar uma maior literacia digital e cibernética da população portuguesa.

Serão os recursos financeiros disponibilizados para o próximo quinquénio suficientes para garantir uma modernização nos equipamentos e tecnologias das forças de segurança, e acompanhar os progressos em IA?

Estas e outras questões levantadas com o presente ensaio evidenciam um certo grau de incerteza nas capacidades autónomas de Portugal em garantir a sua própria cibersegurança, de forma a prevenir e atenuar os ciberincidentes. Existem investimentos cada vez maiores e reforçam-se as capacidades nacionais, contudo Portugal continua a precisar de ajuda externa. Ainda assim, serão as alianças, das quais Portugal faz parte, capazes e disponíveis para dar um apoio maior?

Referências Bibliográficas

5th NATO CYBER DEFENCE. (2019). Academia Militar. https://academiamilitar.pt/5th-nato-cyber-defence.html

(6th meeting) Open-ended working group on security of and in the use of information and communications technologies 2021–2025, Third substantive session. (2022, July). UN Web TV. https://media.un.org/en/asset/k1a/k1aexi8av1

A Convenção de Crimes Cibernéticos da ONU e a guerra entre Rússia e Ucrânia. (2022, March). Data Privacy Brasil Research. https://www.dataprivacybr.org/a-convencao-de-crimes-ciberneticos-da-onu-e-a-guerra-entre-russia-e-ucrania/

A História dos Ciberataques. (2021). Crispus from Pelican Bay. https://cyber-security.pt/blog/a-historia-dos-ciberataques/

About ECSO. (2022). European Cyber Security Organisation. https://ecs-org.eu/

About the NCI Academy. (2022). NCI Agency (NATO). https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html

Academia Militar. (2018, April). *4 th NATO Cyber Defence Smart Defence Projects' (CD SDP) Conference*. NATO Smart Defence. https://ensino.academiamilitar.pt/SI

Ad Hoc Committee on Cybercrime. (2023). Digital Watch Observatory. https://dig.watch/processes/cybercrime-ad-hoc-committee

Almeida, C. (2018). A Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço. *III Seminário IDN Jovem*, 271–288.

Antunes, M. T. D. (2013). *O Hacktivismo e as Forças Armadas*. Instituto de Estudos Superiores Militares.

Baadsgaard, J. (2021). Cybersecurity Laws & Regulations. *IPOhub*.

Barbas, J., & Sancho, C. (2018). *Cibersegurança e Políticas Públicas: Análise comparada dos casos chileno e português*. Lisboa: Instituto da Defesa Nacional.

Barrinha, A. (2020). Cibersegurança em Tempos de Pandemia. *National Defense Institute of Portugal*, 3. https://www.jstor.org/stable/pdf/resrep25591.pdf

Carballo-Cruz, F., Cerejeira, J., & Esteves, R.-B. (2022). *Cibersegurança em Portugal*.

Cibersegurança: como combate a UE as ciberameaças. (2022, September). Consilium. https://www.consilium.europa.eu/pt/policies/cybersecurity/

CNCS. (2021). Sobre nós. https://www.cncs.gov.pt/pt/sobre-nos/

COI Strategy and Defence. (2022). Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats). https://www.hybridcoe.fi/coi-strategy-and-defence/

Compêndio de auditoria: A cibersegurança na UE e nos seus Estados Membros PT. (2020).

Coriolano, T. G., Garcia, A. P., Costa, M. R. S. P., & Faria, N. C. F. de. (2021). *Entidades paraestatais: o que são?* Politize. https://www.politize.com.br/entidades-paraestatais-o-que-sao/

Correia, P. M. R. A., Santos, S. I. da S., & Bilhim, J. A. de F. (2016). Clusters de Percepções sobre cibersegurança e cibercriminalidade em Portugal e as suas implicações para a implementação de políticas públicas nesse domínio. *Revista Da FAE*, 19(2), 22–37. https://revistafae.fae.edu/revistafae/article/view/98

Correia, G., Casanova, R., & Agência Lusa. (2022). Documentos da NATO enviados a Portugal foram intercetados por hackers e colocados à venda na "dark web". *Observador*, *Crime informático*.

Council of Europe. (2001). Convention on Cybercrime. *European Treaty Series*, 185.

Cryptojacking. (2022). Interpol. https://www.interpol.int/Crimes/Cybercrime/Cryptojacking

Cyber defence. (2022). NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm

Cyber/ICT Security. (2022). OSCE. https://www.osce.org/secretariat/cyber-ict-security

Davies, V. (2021, October 4). The history of cybersecurity. *Cyber Magazine*.

EDA-developed cyber training platform handed over to Portugal. (2022). European Defence Agency. https://eda.europa.eu/news-and-events/news/2022/05/25/eda-developed-cyber-training-platform-handed-over-to-portugal#

Enquadramento da Ciberdefesa. (2022). SGMDN. https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/enquadramento

Está a Europa preparada para ciberataques? (2022). *Euronews*, *Mundo*.

Estratégia Nacional de Segurança do Ciberespaço. (2022, June). Portugal Digital. https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/conhecer-as-estrategias-para-a-transicao-digital/estrategia-nacional-de-seguranca-do-ciberespaco/

Estratégia Nacional de Segurança do Ciberespaço 2019-2023. (2019). CNCS. https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

EU digital investment programs budget 2027. (2022). Statista. https://www.statista.com/statistics/1115327/eu-digital-investment-programmes-budget/

EU-NATO cooperation – Factsheets. (2020, June). EEAS Website. https://www.eeas.europa.eu/eeas/eu-nato-cooperation-factsheets_en

European Cybercrime Centre – EC3. (2022, March). Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

European Interactive Map. (2022). Digital Skills and Jobs Platform. https://digital-skills-jobs.europa.eu/en/european-interactive-map

European Security & Defence College. (2019). *Handbook on Cyber Security* (2nd ed.). Austrian Ministry of Defence.

Exército Português realiza Exercício CIBER PERSEU 21. (2021). Exército Portugal. https://www.exercito.pt/pt/informacao-publica/noticias/3320?fbclid=IwAR09hXuQqSUoNFQdRCDQHiCabeNgDUsUzX4FBzRcgQkjcOD5bGf7Q1PkQsg

Força Aérea Portuguesa. (2022). CEMFA. https://www.emfa.pt/noticias-tag-ciberdefesa

Greiman, V. (2018). Reflecting on cyber governance for a new world order: an ontological approach. In P. Demartini & M. Marchiori (Eds.), *Proceedings of the 17th European Conference on Research methodology for business and management studies* (pp. 148–155). ACPI. https://books.google.pt/books?hl=en&lr=&id=gU9mDwAAQBAJ&oi=fnd&pg=PA148&dq=cyber+governance+in+the+world%3F&ots=Eui5a_h1NW&sig=re3Orx4QzUohi41yfPFOaMGaUto&redir_esc=y#v=onepage&q=cyber%20governance%20in%20the%20world%3F&f=false

Hollis, D. (2021). A Brief Primer on International Law and Cyberspace. *Carnegie Endowment for International Peace*.

Indra. (2013). Indra Creates An Advanced Cybersecurity Operations Center . *DefenceTalk*, *Technological News*.

Jesus, H. F. de. (2021). Ciberdefesa – Uma componente de Segurança. *Revista Militar*, 2631.

Joint Cybercrime Action Taskforce (J-CAT). (2022, August). Europol. https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce

Lederer, E. (2019). UN gives green light to draft treaty to combat cybercrime. *AP News*.

Lété, B., & Pernik, P. (2017). EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions (policy brief). *GMF of the United States*, 38 (Security and Defense Policy).

Liaropoulos, A. N. (2017). Cyberspace governance and state sovereignty. *Democracy and an Open-Economy World Order*, 25–35. https://doi.org/10.1007/978-3-319-52168-8_2/COVER

Liebowitzzx, D., Nepal, S., Moore, K., & et al. (2021). Deception for Cyber Defence: Challenges and Opportunities. *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications*, 173–183. https://doi.org/10.1109/TPSISA52974.2021.00020

Lumiste, L. (2018). *Chatham House report: Space – NATO cyber security's weak spot*. CCD COE. https://ccdcoe.org/incyder-articles/chatham-house-report-space-nato-cyber-securitys-weak-spot/

Lusa. (2018). Portugal tem papel central na área da cibersegurança da NATO e da UE. *Dinheiro Vivo*.

Madnick, S. (2022). New Cybersecurity Regulations Are Coming. Here's How to Prepare. *Harvard Business Review*.

Marques, A. G. M. (2019). A segurança do ciberespaço em Portugal e no setor marítimo. *Cadernos Navais*, 52.

Matos, A. (2018). *Cibersegurança: políticas públicas para uma cultura de cibersegurança nas empresas*. ISCTE. https://repositorio.iscte-iul.pt/handle/10071/17630

Meireles, L. (2018). NATO destaca papel da "ciberdefesa" em Portugal. *Expresso*.

Militão, O. P. (2014). *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional*. Faculdade de Ciências Sociais e Humanas, Universidade NOVA de Lisboa.

Militares portugueses participaram em exercício internacional de ciberdefesa. (2021). Security Magazine. https://www.securitymagazine.pt/2021/04/19/militares-portugueses-participaram-em-exercicio-internacional-de-ciberdefesa/

Ministério da Defesa Nacional. (2013). Orientação Política para a Ciberdefesa. *Diário Da República*, 2(208).

Monteiro, S., & Pinto, S. (2016). Cibersegurança e ciberdefesa – Portugal e NATO. *Revista Da Armada*, 507, 4–5.

NATO Exercise Cyber Coalition 2021. (2021). *INsig2*.

NATO realizou maior exercício anual de ciber defesa. (2020). *Security Magazine*.

Negreiro Achiaga, M. D. M. (2022). *The NIS2 Directive: A high common level of cybersecurity in the EU*. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

North Atlantic Treaty Organisation. (2022). CCD COE. https://ccdcoe.org/organisations/nato/

Nunes, P. F. V. (2020). *A Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Definição de uma Estratégia Militar para o Ciberespaço* (Instituto Universitário Militar, Ed.). Coleção 'ARES'.

Nunes, P. V., & Carvalho, L. S. (2021). A afirmação de Portugal na Educação e Treino em Ciberdefesa: do Projeto MNCDE&T à edificação do CAIH. *Mensagem*, *Por Engenho e Ciência*, 10–20.

Nunes, P. V., & Moniz, P. (2021). Cyberspace security and the protection of critical infrastructures: the European Digital Agenda and national resilience. *EuroDefence-Portugal*.

O Centro de Ciberdefesa. (2022). SGMDN. https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx

Observatório da Cibersegurança. (2022). *Cibersegurança em Portugal: riscos & conflitos*.

Observatório da Cibersegurança. (2020). Cibersegurança em Portugal: riscos & conflitos. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2020-observatoriociberseguranca-cncs.pdf

ONU cria cargo de relator para direito à privacidade na era digital. (2015). ONU News. https://news.un.org/pt/story/2015/03/1506521-onu-cria-cargo-de-relator-para-direito-privacidade-na-era-digital

Open-ended Working Group Cyber 201: Framework Recap. (2021, December 7). UNIDIR. https://www.unidir.org/events/open-ended-working-group-cyber-201-framework-recap

Open-ended working group on information and com0munication technologies. (2021). United Nations Office for Disarmament Affairs. https://meetings.unoda.org/meeting/57871

Pereira, A. M. (2021). *Ciber segurança na indústria 4.0: criação de website informativo*. http://ric.cps.sp.gov.br/handle/123456789/7505

Pinho, P. M. de C. (2020). O modelo de ciberdefesa nacional: solução centralizada ou distribuída? IUM.

Pinto, S. da S. (2016). *Política e Plano de Ação para a Ciberdefesa NATO: Perspetivas de Evolução*. 10º Simpósio Internacional 'Estratégia Da Informação Nacional'. https://academiamilitar.pt/images/10_SIMPOSIO_INTERNACIONAL/Apresentacoes/4.Sinergias-Nacionais-e-Coop-Internacional_DELNATO.pdf

Pós-Graduação em Cibersegurança e Ciberdefesa. (2017). PG CS e CD. https://academiamilitar.pt/images/site_images/Eventos/Folheto_-_PG_CS_e_CD.pdf

Projetos e Iniciativas. (2022). Defesa Nacional. https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/projetos/Paginas/default.aspx

Proposal for directive on measures for high common level of cybersecurity across the Union. (2020, December). European Commission. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União. (2021). Comissão Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=PT

Proteção e Gestão de Risco de Infraestruturas Críticas. (2023). APSEI – Associação Portuguesa de Segurança. https://www.apsei.org.pt/areas-de-atuacao/protecao-civil/protecao-e-gestao-de-risco-de-infraestruturas-criticas/

Prucková, M. (2022). *Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO*.

CCD COE. https://ccdcoe.org/incyder-articles/cyber-attacks-and-article-5-a-note-on-a--blurry-but-consistent-position-of-nato/

Ralo, J. (2013). CiberSegurança e CiberDefesa. *Direção-Geral de Política de Defesa Nacional*.

Relations with the European Union. (2022, June). NATO. https://www.nato.int/cps/en/natolive/topics_49217.htm

Relatório Cibersegurança em Portugal: riscos & conflitos. (2020, June). Centro Nacional de Cibersegurança Nacional. https://www.cncs.gov.pt/docs/relatorio-riscos-conflitos-2020.pdf

Relatório Cibersegurança em Portugal: riscos & conflitos. (2021). Centro Nacional de Sibersegurança Nacional.

Relatório Sociedade 2020 – Termos, Siglase e Abreviaturas. (2020). Centro Nacional de Sibersegurança Portugal. https://www.cncs.gov.pt/pt/relatorio-sociedade-2020-termos-siglase-e-abreviaturas/

Resolução do Conselho de Ministros n.º 91/2019. (2019). *Diário Da República*, 108(Série I).

Sandler, M. (2022). *UN Regulation No 155 & how to comply? What you need to know*. Cyres Consulting. https://www.cyres-consulting.com/un-regulation-no-155-requirements-what-you-need-to--know/

Santos, D. G. G. (2014). *A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança*. ISCTE – Instituto Universitário de Lisboa.

Santos, J. L. A. dos. (2011a). *Contributos para uma melhor governação da cibersegurança em Portugal*. Universidade NOVA de Lisboa. http://hdl.handle.net/10362/7341

Santos, L. C. dos, Nunes, P. V., Ralo, J., & Mendes, C. P. (2018). Defesa do Ciberespaço. In P. Viegas, N. Carlos, P. Mendes, & E. Al. (Eds.), *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 33–46). IDN Cadernos.

Santos, L. (2016). *Estratégias Nacionais de Cibersegurança*. Centro Nacional de Cibersegurança. https://academiamilitar.pt/images/10_SIMPOSIO_INTERNACIONAL/Apresentacoes1.Estrat-Seg-Ciberespao_CNCS.pdf

Santos, L. (2018). Segurança do Ciberespaço. In P. Viegas, N. Carlos, P. Mendes, & et al. (Eds.), *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 25–32). IDN Cadernos.

Schmitt, M. (Ed.). (2013). *Tallinn Manual on the International Law applicable to Cyber Warfare* (1st ed.). Cambridge University Press.

Sen, K. (2022, September 4). *List of Cybersecurity Regulations in the European Union*. UpGuard. https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-2

Silva, E. L. G. P. de O. (2015). *Cibersegurança das Infraestruturas Críticas Nacionais*. Academia da Força Aérea.

The Portuguese Armed Forces complete Cyber Perseu, the National Cyberdefense exercise, using Indra's Minsait Cyber Range platform. (2018, January). Indra. https://www.indracompany.com/en/noticia/portuguese-armed-forces-complete-cyber-perseu-national-cyberdefense-exercise-using-indras

Transnational Threats Department Cyber/ICT Security. (2016). OSCE Secretariat. https://www.osce.org/files/f/documents/c/c/256071.pdf

Treaties & International Agreements on Cyber Crime. (2022). Georgetown Law Library. https://guides.ll.georgetown.edu/c.php?g=363530&p=4821478

UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles (2022). UNECE. https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll

United Nations. (2021). *UN Regulation No. 155*, 3, 1–30.

Vass, S. (2019). *Cyber operations centre: a capability user perspective*. 5th NATO Cyber Defence Smart Defence Projects' Conference: Cyber NATO-EU Cooperation. https://academiamilitar.pt/images/site_images/5th_NATO_Cyber_Defence/8_Brigadier_General_HUN_Army_Sandor_VASS_Director_Cyberspace_Operations_Centre_ACO_-_CyOC.pdf

Viegas, P., Carlos, N., Mendes, P., Ralo, J., Santos Luís Camelo, L., Santos, D., Moniz, P., De, S., & Casimiro, V. (2018). Contributos para uma Estratégia Cacional de Ciberdefesa. *IDN Cadernos*, 28.

Vieira, S. de J. (2016). *Segurança da Informação no Ciberespaço – A Cibereducação no caminho da Cibersegurança*. Escola Naval.

Vitor Rodrigues Viana (Ed.). (2012). Cibersegurança. *IDN Cadernos*, 133(5).

Índice de IDN Cadernos Publicados

		III SÉRIE
2022	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

VII SEMINÁRIO IDN JOVEM

Covilhã, 6 e 7 de dezembro de 2022

idn Instituto da Defesa Nacional

ISSN 1647-9068

00049