INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO-MAIOR CONJUNTO

2021/2022

TII

AMEAÇAS HÍBRIDAS: A DOUTRINA RUSSA E A SUA APLICAÇÃO PRÁTICA

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Daniel Filipe de Carvalho Gomes

MAJOR, INFANTARIA

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

AMEAÇAS HÍBRIDAS: A DOUTRINA RUSSA E A SUA APLICAÇÃO PRÁTICA

MAJOR, INFANTARIA Daniel Filipe de Carvalho Gomes

Trabalho de Investigação Individual do CEMC 2021/22

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

AMEAÇAS HÍBRIDAS: A DOUTRINA RUSSA E A SUA APLICAÇÃO PRÁTICA

MAJOR, INFANTARIA Daniel Filipe de Carvalho Gomes

Trabalho de Investigação Individual do CEMC 2021/22

Orientador: TENENTE-CORONEL, ARTILHARIA Lourenço Serrão

Co-Orientador: CAPITÃO-DE-FRAGATA, MARINHA Rodrigues Vicente

Pedrouços 2022

Declaração de compromisso Antiplágio

Eu, **Daniel Filipe de Carvalho Gomes**, declaro por minha honra que o documento intitulado "**Ameaças Híbridas: a Doutrina Russa e a sua aplicação prática",** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Estado-Maior Conjunto 2021/22** no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 04** de **maio** de **2022**

Daniel Filipe de Carvalho Gomes

Agradecimentos

Uma primeira palavra de reconhecimento para o meu orientador, Tenente-Coronel Diogo Lourenço Serrão, que apesar da distância física, não se constituiu como fator limitador para o desenvolvimento deste trabalho, através de uma permanente disponibilidade e intrínseco aconselhamento. O seu conhecimento na temática abordada, a par de um rigor académico e elevado comprometimento e espírito crítico, permitiu que me sentisse seguro e confiante ao longo de toda a investigação.

Ao Capitão-de-Fragata Paulo Rodrigues Vicente, que na qualidade de coorientador se constituiu desde o primeiro momento como uma peça fundamental na correta abordagem da investigação, constituindo-se como facilitador na ligação profícua com as entidades estruturantes e elementos fulcrais na temática abordada.

Aos entrevistados, Contra-Almirante António Gameiro Marques, Dr. Josef Schröefl, Coronel Tirocinado António José Ruivo Grilo, Professor Miguel Pupo Correia, Coronel Óscar Manuel do Nascimento Rocha, Tenente-Coronel Hugo Miguel Moutinho Fernandes, Tenente-Coronel David Lopes Antunes, Tenente-Coronel José Carlos Reimão Teixeira, Tenente-Coronel Jorge Miguel Vinagreiro, Capitão-de-Fragata Sérgio Caldeira de Carvalho, pela atenção e disponibilidade apresentada ao acederem à partilha dos seus sustentados conhecimentos nesta área, e sem os quais não teria sido possível concluir a presente investigação.

Ao senhor Embaixador Luís Barreira de Sousa e ao Capitão-de-Mar-e-Guerra Hélder Fialho de Jesus, pelo cuidado sentido de aconselhamento e partilha de experiência, materializadas nas entrevistas exploratórias, proporcionando documentação estruturante e contactos essenciais para a investigação.

Ao Senhor Diretor de Curso, Capitão-de-Mar-e-Guerra Luís Daniel Carona Jimenez, pelo acompanhamento e estreita colaboração, constituindo-se como elemento facilitador no estabelecimento de contactos e obtenção de documentação estruturante.

A todos os Docentes e Auditores do Curso de Estado-Maior Conjunto 2021/2022, pela transmissão de conhecimento académico e pela sã camaradagem vivenciada, marcando de forma inolvidável a passagem por este momento da minha carreira profissional.

À minha família, por tudo!

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

As Ameaças Híbridas atuam através da combinação e sincronização dos seus instrumentos de poder, numa afetação multidimensional de um determinado alvo. Fruto da conectividade global, o ciberespaço materializa-se como o espaço de batalha onde as Ameaças Híbridas proliferam e catalisam a sua atividade, num racional difuso e de difícil detetabilidade. A Rússia é um ator que atua neste quadro de ação e potencia-se pelo estado de conflito permanente.

Assim, o presente trabalho estuda a aplicação russa de Ameaça Híbrida, propondo um possível modelo de utilização do ciberespaço.

Assente num raciocínio indutivo e numa estratégia qualitativa, baseado num estudo de caso, efetuou-se uma análise documental, permitindo consolidar os indicadores, através da realização de entrevistas a especialistas.

Como principais resultados obtidos, constata-se a atuação russa no ciberespaço, mormente nos conflitos Russo-Georgiano e Russo-Ucraniano, através do uso sincronizado de ferramentas, numa matriz conducente com o seu conceito doutrinário.

Através de um modelo conceptual cientificamente validado, conclui-se que a Rússia atua no ciberespaço, através do uso predominante de dez ferramentas, afetando transversalmente todos os domínios do seu adversário, num espectro de atuação abrangente, sendo sentido com maior preponderância as fases não cinéticas do seu quadro doutrinário, num racional de preparação e desestabilização.

Palavras-chave: Ameaças Híbridas, Rússia, Doutrina Russa, Ciberespaço, Conflito Russo-Georgiano, Conflito Russo-Ucraniano.

Abstract

Hybrid Threats act through the combination and synchronization of their instruments of power, in a multidimensional affectation of a given target. As a result of global connectivity, cyberspace is the battle space where Hybrid Threats proliferate and catalyse their activity, in a diffuse and undetectable environment. Russia is an actor that operates in this framework and is empowered by the state of permanent conflict.

Thus, this paper studies the Russian application of Hybrid Threat, proposing a possible model for the use of cyberspace.

Based on an inductive approach and a qualitative strategy, based on a case study, the reference documents analysis was carried out, allowing the consolidation of indicators, through interviews with experts.

The main results obtained show Russian action in cyberspace, especially in the Russo-Georgian and Russo-Ukrainian conflicts, through the synchronized use of tools, in a matrix consistent with its doctrinal concept.

Based on a scientifically validated conceptual model, it is concluded that Russia acts in cyberspace through the predominant use of ten tools, transversely affecting all domains of its adversary, in a wide-ranging spectrum of action, being felt with greater preponderance the non-kinetic phases of its doctrinal framework, in a priming and destabilization logic.

Keywords: *Hybrid Threats, Russia, Russian Doctrine, Cyberspace, Russian-Georgian Conflict, Russian-Ukrainian Conflict.*

Lista de abreviaturas, siglas e acrónimos

A	
AH	Ameaças Híbridas
C	
CCDCOE	NATO *Cooperative Cyber Defence Centre of Excellence*
CNCS	Centro Nacional de Ciber Segurança
E	
EMGFA	Estado-Maior General das Forças Armadas
EUA	Estados Unidos da América
F	
FFAA	Forças Armadas
G	
GH	Guerra Híbrida
H	
Hybrid CoE	*European Centre of Excellence for Countering Hybrid Threats*
I	
IUM	Instituto Universitário Militar
M	
MCDC	*Multinational Capability Development Campaign*
MPECI	Militar, Político, Económico, Civil, Informacional
N	
NATO	*North Atlantic Treaty Organization*
O	
OE	Objetivo Específico
OG	Objetivo Geral
P	
PMESII	Político, Militar, Económico, Social, Infraestruturas e Informacional
Q	
QC	Questão Central
QD	Questão Derivada
T	
TII	Trabalho de Investigação Individual
U	
UE	União Europeia

1. Introdução

Em 2005, através de um artigo elaborado por Mattis[1] e Hoffman[2] (2005), a comunidade académica e político-militar confrontou-se com a verbalização e conceptualização de Guerra Híbrida (GH), que redimensionou os domínios da guerra, esbatendo as diferenças nos distintos patamares do conflito.

Segundo Wither (2016, p. 75), durante a primeira década de 2000, em que se assistia a um sistema internacional unipolar dominado pelos Estados Unidos da América (EUA), o conceito "híbrido" aludia à capacidade de atores não-estatais[3] usarem meios letais cada vez mais sofisticados, e simultaneamente, os integrarem com uma intensa exploração do domínio ciber. Contudo, na visão de Hoffman (2007, p. 3), a "hibridização" dos conflitos podia também ser prática entre atores estatais, pelo uso de forma sincronizada dos métodos convencionais, não convencionais, ações terroristas e ações criminosas.

Em 2008, no conflito russo-georgiano, verificou-se a combinação de atividades cinéticas com o instrumento informacional numa "[…] *Blitzkrieg* propagandística e diplomática […]" (Guedes, 2009, p. 28), que permitiu inicialmente a moldagem do espaço de batalha e posteriormente a consolidação política russa no espaço internacional. Apesar da comunidade internacional anunciar diferentes abordagens à conceptualização de GH, é consensual que este conflito se constituiu como "área de testes" no que às "táticas híbridas" diz respeito (Nilsson, 2018, p. 15).

A retórica do General Gerasimov[4] em 2013, afirmou a complexidade e multidimensionalidade dos conflitos, fluindo nos diferentes domínios de poder "simultaneamente na terra, no ar, no mar e no espaço informacional" (Bērziņš, 2014, p. 4) e, teve aplicação prática em 2014, com a anexação da Crimeia, dando-se o início da crise russo-ucraniana.

A par do problema securitário na Ucrânia, em 2014, intensificou-se o interesse pelo conceito de GH pelos teorizadores ocidentais, porquanto na aplicação prática e sincronizada das várias ferramentas e métodos pela Rússia (Wither, 2016, p. 4), mas principalmente pela reflexão generalizada que a campanha russa se constituiu, pelas palavras do General

[1] Tenente-General James Norman Mattis, Corpo de *Marines* dos EUA.
[2] Tenente-Coronel Frank G. Hoffman, Corpo de *Marines* dos EUA.
[3] Ver Apêndice A – Corpo de Conceitos.
[4] General Valery Gerasimov- Chefe do Estado-Maior das Forças Armadas da Federação Russa, desde 2012 até ao presente (Shamiev, 2021).

Breedlove[5] como "[…] a mais surpreendente *Blitzkrieg* informacional alguma vez vista […]" (Breedlove, 2014, cit. por Vandiver, 2014, 3.º parágrafo).

Apesar de anteriormente aludido por Hoffman (2007), com o advento da crise russo-ucraniana, o conceito de Ameaça Híbrida (AH) ganha uma nova dimensão, trazido à luz pela União Europeia (UE), através de uma Comunicação Conjunta ao Parlamento Europeu e ao Conselho Europeu (UE, 2016). Com a tónica nas AH e no reforço da resiliência dos seus Estados-membros, fruto da instabilidade "a Leste", são elencadas propostas que permitam uma mobilização *whole-of-goverment*[6] (UE, 2016, p.2), constituindo-se este documento como percursor da criação do *European Centre of Excellence for Countering Hybrid Threats* (*Hybrid CoE*)[7] (Hybrid CoE, 2022a).

É neste contexto que importa relacionar a capacidade russa com a evolução tecnológica da atualidade, concretamente com a emersão do domínio do ciberespaço como o novo espaço de batalha, que facilita o anonimato aos atores que o usam.

Segundo Nunes et al. (2018, p. 19), este domínio caracteriza-se por ter "[…] duas camadas distintas, uma física […] e outra lógica […] onde se estabelecem as trocas de informação entre indivíduos e organizações […]", não sendo possível delimitar fronteiras e, por conseguinte, criar uma obtusidade legal no direito internacional. Esta visão é partilhada por Leonard (2021), que advoga que o conceito de conectividade pode criar oportunidades para conflitos *low-cost* e de carácter permanente, constituindo-se a Internet como um espaço de batalha para instrumentalizar os objetivos políticos através de ações legalmente duvidosas.

Seguindo esta linha de pensamento, a utilização do ciberespaço pela Rússia configura-se numa aplicação sincronizada de ações, que, segundo Pomerantsev (2014, 9.º parágrafo) se chegam a transfigurar numa alteração da própria realidade, alterando o foco das atenções, quer doméstica, quer internacionalmente, nas narrativas políticas do Ocidente sem preocupação de criar a sua própria narrativa.

Neste âmbito, as AH, as suas ferramentas e o uso do ciberespaço pela Rússia, como principal catalisador, tornam-se fulcrais no entendimento do futuro "arco do conflito" e no entendimento holístico que a expansão do espaço de batalha vai para além das operações

[5] General Philip Mark Breedlove – Comandante Supremo Aliado na Europa de maio de 2013 a maio de 2016 (Harvard Kennedy School, 2016).
[6] Ver Apêndice A – Corpo de Conceitos.
[7] O *Hybrid CoE*, é uma organização internacional independente, que serve de plataforma de diálogo entre a UE e a NATO, com o objetivo de combater as AH, seguindo uma abordagem *whole-of-government* e *whole-of-society* (Hybrid CoE, 2022b).

cinéticas (Danyk et al., 2017, p. 13), enfatizando que, segundo Thornton (2015, p. 42), "Moscovo perceciona que está em permanente conflito" com o Ocidente.

Assim, considera-se como objeto de investigação do presente Trabalho de Investigação Individual (TII), a aplicação russa de AH, materializando-se como Objetivo Geral (OG) propor um modelo da utilização do ciberespaço por parte da Rússia como AH.

Por forma a evitar derivações no estudo, importa proceder a uma delimitação espacial, temporal e conceptual (Santos & Lima, 2019).

A investigação incidiu espacialmente na Geórgia e Ucrânia, dada a materialização de "táticas híbridas" por parte da Rússia (Nilsson, 2018, p. 15).

Temporalmente, considera-se o período de 2008, no qual se desenvolveu o conflito Russo-Georgiano, motivado pelo confronto entre os movimentos separatistas pró-russos da Ossétia do Sul e Abecásia e o governo georgiano (Saberwal, 2018, p. 68), e o período compreendido entre 2013, onde se deu início aos protestos "Euromaiden", e 2014, com a anexação da Crimeia (Bērziņš, 2014).

Quanto ao conteúdo, a investigação será delimitada ao uso das ferramentas da AH, segundo modelos conceptuais de referência, no domínio do ciberespaço, integrando os conceitos doutrinários russos. Assim, dando primazia do uso do ciberespaço, serão analisados os acontecimentos históricos praticados pela Rússia, concretamente nas respetivas ações e efeitos provocados, nos conflitos da Geórgia em 2008, e da Ucrânia em 2013 e 2014.

Por forma a cumprir com o OG da investigação, torna-se necessário atingir os seguintes Objetivos Específicos (OE):

- OE1 – Investigar as ferramentas das AH possíveis de serem aplicadas no ciberespaço;
- OE2 – Analisar o uso das ferramentas das AH no ciberespaço, por parte da Rússia, em situações de conflito;
- OE3 – Analisar a integração da doutrina russa no modelo conceptual das AH;

Concorrendo diretamente para se atingir o cumprimento do OG, apresenta-se como Questão Central (QC): Qual o possível modelo de utilização do ciberespaço por parte da Rússia como AH?

A resposta a esta questão, permitirá, de forma conceptual, apresentar um modelo de atuação russa, centrado no uso do ciberespaço, possibilitando futuramente, a integração de outras análises de conflitos materializados pela Rússia.

Com o propósito de atingir a resposta à QC, foram identificadas três Questões Derivadas (QD):

- QD1 – Quais as ferramentas das AH que se adequam à utilização no ciberespaço?
- QD2 – De que forma foram aplicadas as ferramentas das AH, no ciberespaço, nos conflitos perpetrados pela Rússia?
- QD3 – Como se integra a doutrina russa no modelo conceptual das AH?

O presente trabalho encontra-se estruturado em cinco capítulos. Na introdução, foi enquadrado o tema e justificada a investigação, definido e delimitado o objeto de estudo, e apresentados os objetivos e questões da investigação.

No segundo capítulo é efetuado o enquadramento teórico e conceptual, onde se descreve o estado da arte e a revisão da literatura, apresentando as principais referências e conceitos estruturantes, culminado com a apresentação do modelo de análise.

No terceiro capítulo expõe-se a metodologia e o método, a estratégia de investigação, desenho de pesquisa, participantes e procedimento, a par do instrumento e técnicas de recolha de dados.

No quarto capítulo são apresentados os dados obtidos, sobre os quais serão discutidos os resultados, permitindo atingir os OE através das respostas às QD, por forma a responder à QC, atingindo consequentemente o OG.

No quinto e último capítulo apresentam-se as conclusões, contributos para o conhecimento, propõe-se recomendações para estudos futuros, e as limitações da investigação.

2. Enquadramento teórico e conceptual

De modo a contribuir para uma melhor compreensão do trabalho, detalham-se de seguida os principais estudos de acordo com os conceitos estruturantes, concretamente as AH, o ciberespaço e a doutrina russa. O capítulo culmina com a apresentação do modelo de análise.

2.1 Estado da arte/revisão da literatura

2.1.1 As Ameaças Híbridas

Analisando a temática "híbrida" nos vários estudos e obras literárias, e aludindo a Torossian et al. (2020, p. 4), assiste-se a um conjunto de abordagens conceptuais, tais como, "campanha híbrida", "conflito híbrido", "guerra híbrida" e "ameaças híbridas", estando as mesmas associadas às "diversas visões nacionais".

Para o presente trabalho, importa destacar os estudos realizados pelo *Multinational Capability Development Campaign* (MCDC)[8] e pelo *Hybrid CoE*, pela alusão ao conceito de GH e AH, respetivamente, e na medida em que os pressupostos concetuais se complementam, alcançando assim, um entendimento coerente e racional. Com enfoque no *Hybrid CoE* e aliado ao objetivo deste trabalho, realça-se o estudo de Giannopoulos, Smith e Theocharidou (2021) - *The Landscape of Hybrid Threats: a Conceptual Model*, cujo modelo conceptual servirá de base para a investigação, e sobre o qual se irá incidir a correlação entre as ferramentas das AH e os domínios afetados[9], e em que fase do espectro do conflito se desenvolvem.

Observando os quadros teóricos de referência acima apresentados, define-se os conceitos de GH e AH, e em que medida se relacionam.

De acordo com o MCDC (2017, p. 3), GH é o uso sincronizado de instrumentos de poder[10] adequados às vulnerabilidades nacionais específicas (PMESII[11]) de um ator, a fim de alcançar efeitos sinérgicos, sendo, "polimórfica por natureza" (Coker, 2005, p. 149). Importa realçar que a sobreposição e fusão dos modos de conflito é característico da GH (Thornton, 2015, p. 41), na tentativa de um ator atingir os seus objetivos políticos sem fazer uso de uma operação militar de larga-escala (Najzer, 2020, p. 29). Genericamente, um ataque híbrido está explicado pelo MCDC, através de um modelo conceptual. Neste, conforme a

[8] O MCDC, liderado pelos EUA, é uma plataforma colaborativa de âmbito conjunto e multinacional, com o objetivo de desenvolver capacidades e de partilhar recursos e conhecimento (United Kingdom Government, 2017).
[9] Ver Apêndice B – Ferramentas das AH e Domínios afetados.
[10] Ver Apêndice A – Corpo de Conceitos.
[11] PMESII- Político, Militar, Económico, Social, Infraestruturas e Informacional (MCDC, 2017, p. 4).

Figura 1, estão presentes três fatores fundamentais: a aplicação dos instrumentos de poder do "agressor" (MPECI[12]) contra as vulnerabilidades críticas (PMESII) do alvo; a sincronização dos meios militares e não-militares no tempo, espaço e finalidade, e os efeitos não-lineares[13], que pela natureza imprevisível, apenas são evidentes quando se manifestam (MCDC, 2017, pp. 11-13). Após a ação por um instrumento de poder, esta manifestação pode ser detetada numa afetação de "primeira ordem ou de segunda e terceira ordem" nos domínios correspondentes, conforme Figura 1, onde se verifica a sinergia do efeitos provocados por uma ação política (i.e. M2) (MCDC, 2017, p. 14).

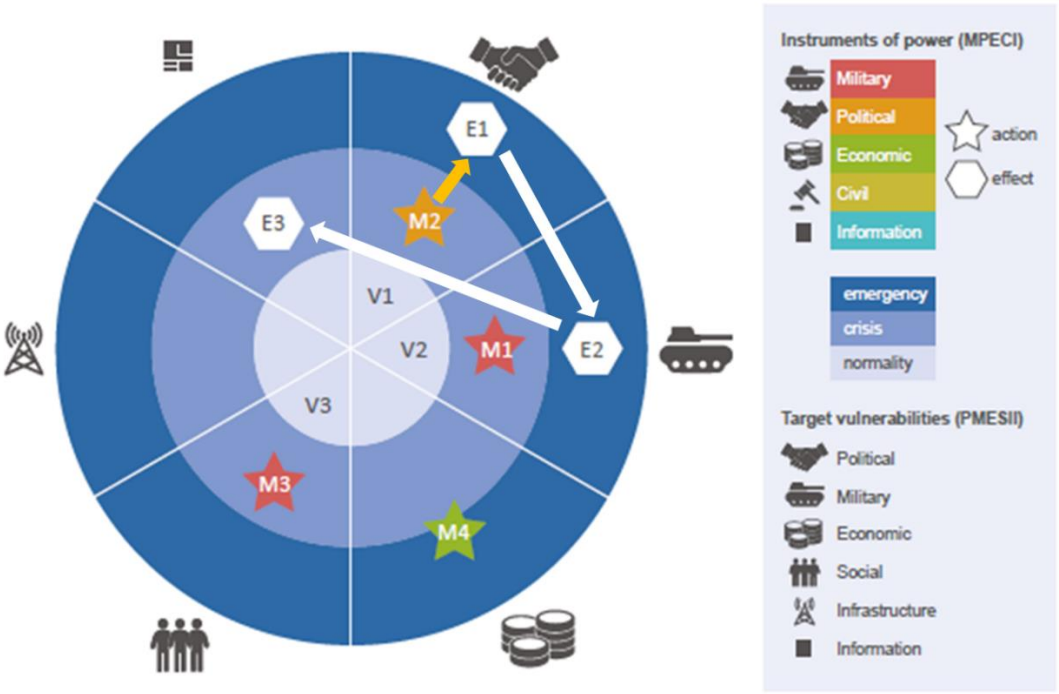

Figura 1 - Modelo conceptual do MCDC
Fonte: Adaptado de MCDC (2019, p. 15).

O conceito de AH é debatido atualmente pela sociedade académica e demais organizações político-militares, coexistindo diversas e diferentes abordagens. O conceito AH é tão antigo como a própria guerra, mas reveste-se e potencia-se atualmente pelas dinâmicas securitárias e pelas novas ferramentas, sendo estas exponenciadas pelo crescimento da tecnologia e aparecimentos de novos domínios, que são atacados sem precedentes históricos (Giannopoulos et al., 2021, p. 6).

De acordo com a *North Atlantic Treaty Organization* (NATO), AH é a combinação de meios militares e não-militares, de forma encoberta ou visível, incluindo a desinformação, ciberataques, pressão económica, e emprego de forças irregulares e regulares (NATO, 2021).

[12] MPECI- Militar, Político, Económico, Civil, Informacional.
[13] Ver Apêndice A – Corpo de Conceitos.

Segundo o mesmo conceito, a aplicação destes meios localiza-se numa zona pouco clara nos limites entre guerra e paz, com o objetivo principal de destabilizar a sociedade (NATO, 2021).

Para a UE, consiste numa ação perpetrada por um ator estado ou não-estado, na exploração das vulnerabilidades da UE para sua própria vantagem, através do uso coordenado de várias medidas, sejam elas diplomáticas, militares, económicas ou tecnológicas, mantendo-se abaixo dos limites formais de estado de guerra (UE, 2021).

Apesar de evidentes convergências nos conceitos apresentados, notam-se, porém, algumas dissonâncias, sobretudo no que respeita às ferramentas, quem as origina e com que objetivo são aplicadas.

Assim, considera-se para o presente trabalho, a definição do *Hybrid CoE*, como as ações conduzidas por atores estado e não-estado, cujo objetivo é afetar ou prejudicar um alvo, quer seja este local, regional ou estatal, no seu processo de decisão (Hybrid CoE, 2021). Segundo a mesma organização, estas ações são coordenadas e sincronizadas, visando deliberadamente as vulnerabilidades dos estados democráticos e suas instituições, ao serem aplicadas nos seus vários domínios (Figura 2), mantendo-se, no que respeita ao espetro do conflito, abaixo dos limites da deteção (Hybrid CoE, 2021).

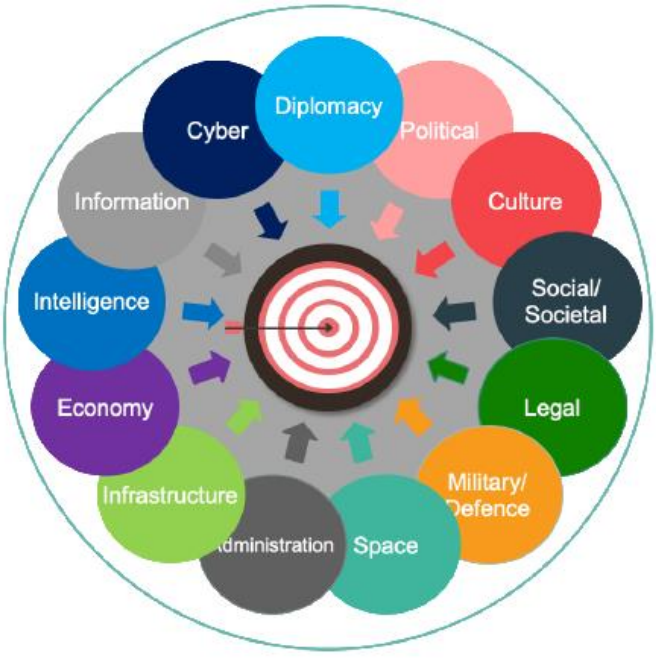

Figura 2 - Domínios afetados pelas AH
Fonte: Disponível em Giannopoulos et al. (2021, p. 27).

Por forma a perceber como atuam as AH, no seu quadro conceptual, realça-se o modelo apresentado por Giannopoulos et al. (2021), no qual estão presentes, de forma transversal, a dinâmica das ferramentas das AH com os domínios afetados, tendo como origem os atores

(estatais e não-estatais), a fim de atingir os objetivos estratégicos de um determinado alvo, nas diferentes fases de um conflito (Figura 3).

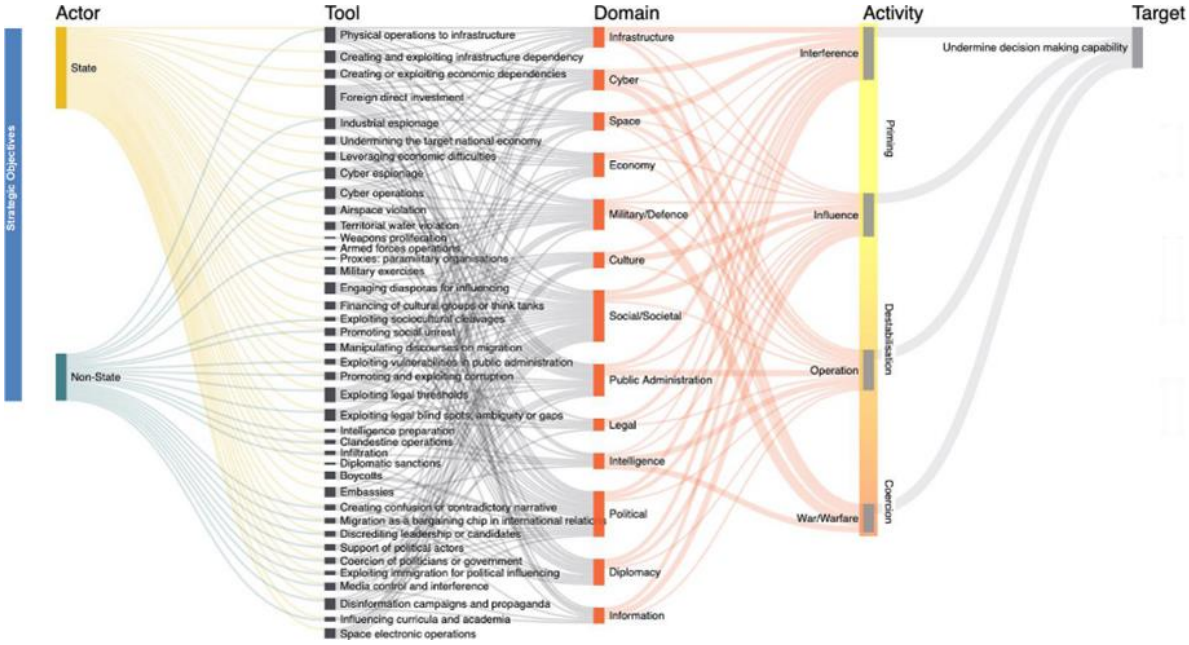

Figura 3 - Modelo conceptual das AH
Fonte: Disponível em Giannopoulos et al. (2021, p. 13).

Como premissa fundamental para o funcionamento de todo o sistema como AH, identifica-se a necessidade de as ferramentas serem aplicadas de forma combinada e sincronizada na afetação dos múltiplos domínios, que, pela suas características interdependentes, permitirão à AH, explorar ou criar vulnerabilidades (Giannopoulos et al., 2021, p. 12). O principal objetivo deste modelo é o sistema social do alvo, em detrimento das suas forças militares (Treverton, 2021, p. 37).

Similarmente, também o modelo conceptual das AH defende que os objetivos podem ser alcançados pelo efeito direto de uma ferramenta num determinado domínio, assim como pela atividade em "cascata", no qual são afetados outros domínios (Giannopoulos et al., 2021, p. 12).

Garantindo a opacidade do fenómeno e a necessidade de controlar o escalonamento da atividade híbrida (Najzer, 2020, p. 30), o seu modelo de atuação consubstancia-se, primordialmente, numa área de sombra, ou *gray zone*[14], que permite à AH atuar no balanceamento entre o legal e o ilegal, num quadro de impercetibilidade (Giannopoulos et al., 2021, p. 36).

Ilustrando o espectro de conflito, Giannopoulos et al. (2021, p. 36) enunciam que, numa lógica temporal, as AH podem atuar em três fases principais: a fase de Preparação

[14] Ver Apêndice A – Corpo de Conceitos.

(*Priming*[15]), a fase de Desestabilização (*Desestabilization*[16]) e a fase de Coação (*Coercion*[17]) (Figura 4). Neste espectro de atuação verifica-se a *gray zone* como área indetetável para a AH, a sobreposição das várias fases, e a possibilidade de a atividade sofrer flutuações multidirecionais na escalada do conflito, permitindo o mascaramento e a confusão situacional no adversário (Giannopoulos et al., 2021).

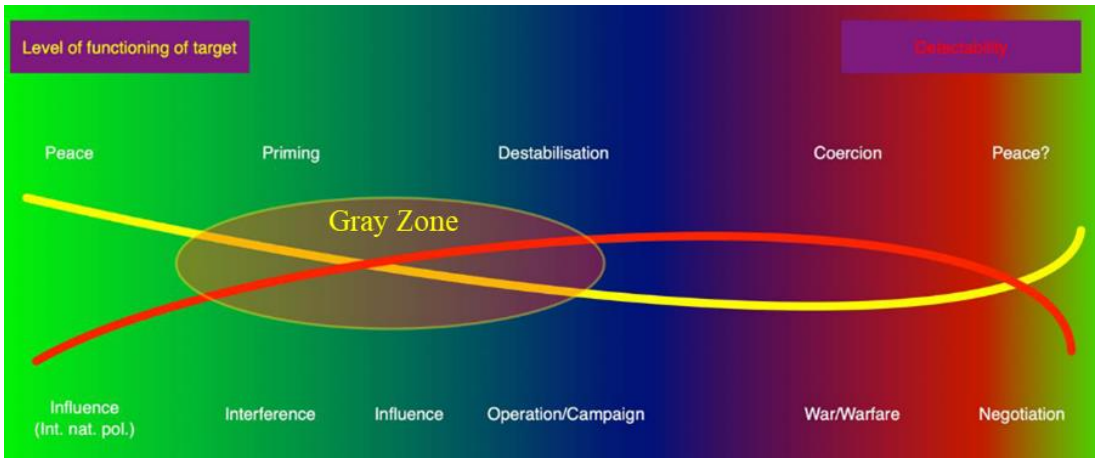

Figura 4 - Fases e Atividades principais das AH
Fonte: Adaptado de Giannopoulos et al. (2021, p. 37).

Analisando todas as características elencadas anteriormente, comprova-se a integração de conceitos entre as AH e a GH, porquanto se assiste ao uso sincronizado e combinado de meios inerentes ao poder de um ator, afetando de forma multidirecional os domínios de um estado alvo, explorando a opacidade do conflito, sob o qual, a "GH representa o último patamar do espetro da atividade das AH" (Giannopoulos et al., 2021, p. 41).

2.1.2 O Ciberespaço

Com a evolução exponencial da conectividade global, o ciberespaço constitui-se como um conceito dinamizador de estudos, organizações e plataformas multinacionais de conhecimento. Fruto dos vários relatórios e manuais emanados do NATO *Cooperative Cyber Defence Centre of Excellence*[18] (CCDCOE), intitulados de *Tallinn Papers e Tallinn Manuals*, nos quais se identificavam as ameaças emergentes e dinâmicas de conflito, a NATO em 2016, na Cimeira de Varsóvia, reconhece o ciberespaço como o quarto domínio operacional, a par dos domínios aéreo, terrestre e marítimo (NATO, 2022). Se anteriormente a este marco histórico, o ciberespaço já era alvo de estudo pelo seu uso, através das dinâmicas político-sociais (Hollis, 2011; Geers, 2015), posteriormente, assistiu-se ao desenvolvimento

[15] Ver Apêndice A – Corpo de Conceitos.
[16] *Ibidem.*
[17] *Ibidem.*
[18] Organização criada pela Estónia, em maio de 2008, que serve de plataforma de ligação e coordenação entre os Estados-Membros da NATO no âmbito da Ciberdefesa (CCDCOE, 2022).

de várias publicações internacionais e nacionais (Schröefl, 2020; Abaimov & Martellini, 2017; NATO, 2020; Nunes et al., 2018), almejando a análise conceptual e a articulação com os outros domínios operacionais.

Segundo Abaimov & Martellini (2017, p. 81), a assunção do ciberespaço como domínio operacional alavancou vantagens e evidentes benefícios para os Estados e demais organizações internacionais, porque, tal como aludido por Hollis (2011, p. 8), possibilitou a integração dos meios e conceitos doutrinários neste novo domínio, permitindo que os objetivos que outrora eram atingidos noutros domínios, fossem, agora, alcançáveis pelo ciberespaço.

Assim, no que respeita ao conceito de ciberespaço, este advoga várias abordagens por várias instituições nacionais e internacionais, fruto da evolução tecnológica recente e da conectividade em rede num mundo globalizado.

Em Portugal, de acordo com o Centro Nacional de Cibersegurança (CNCS), ciberespaço é uma "[…]metáfora usada para descrever o espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar de diferentes maneiras […]"(CNCS, 2021). Na continuidade nacional, segundo Nunes et al. (2018, p. 19), este é o "único domínio criado pelo homem", que genericamente é dividido em duas camadas distintas, uma camada física que se substancia às infraestruturas e equipamentos, e uma segunda camada, que integra as aplicações e conteúdos, permitindo o fluxo informacional, num espaço que não reconhece fronteiras nem distâncias.

De uma forma mais resumida, no âmbito da NATO, o ciberespaço consiste num ambiente computorizado, artificialmente construído e em constante desenvolvimento, numa conetividade globalizada e que cria dificuldades na responsabilização dos Estados (NATO, 2020, p. 2).

Dando conformidade ao alinhamento do conceito de AH, para este trabalho assume-se a definição que o *Hybrid CoE* integra no seu modelo conceptual, no qual define o ciberespaço como o único domínio criado pelo homem e que compreende a sua atuação entre a componente física dos equipamentos e a componente imaterial dos conteúdos, numa simbiose alavancada pela conectividade global (Schröefl, 2021, 7.º parágrafo).

No mesmo alinhamento, importa evidenciar que o ciberespaço se posiciona como um domínio transversal em relação aos demais, numa lógica de "*cross-domain"*, podendo extrapolar que possa ser considerado como um "superdomínio" (Hybrid CoE, 2019).

Assim, verifica-se a concordância nas principais linhas conceptuais, pela "[…] natureza imaterial, volátil, subjetiva e humana […]" e pelo entendimento intrínseco que, o

ciberespaço se integra e transcende com os outros domínios (Honorato, Santos e Mateus, 2017, p.11), conforme Figura 5.

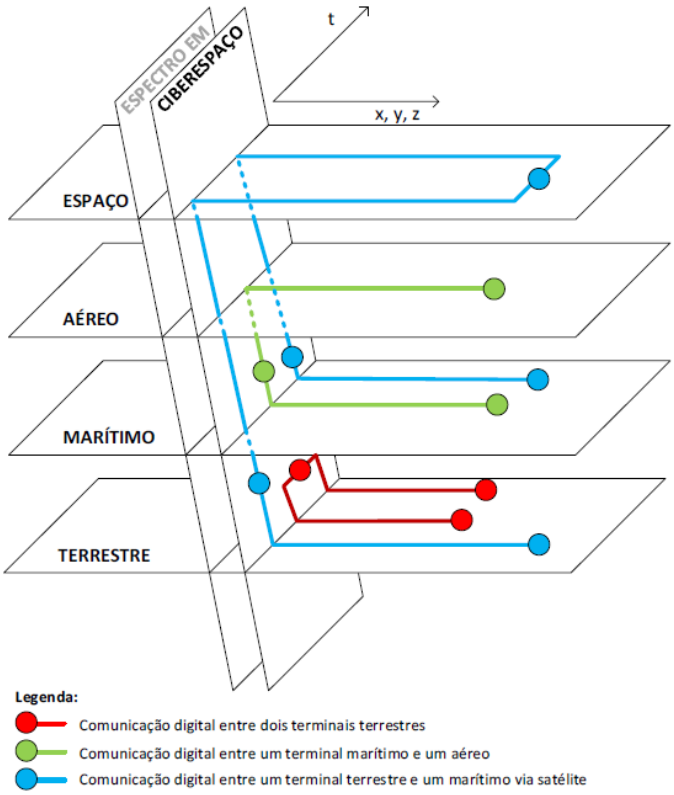

Figura 5 - Integração do Ciberespaço com os demais domínios
Fonte: Disponível em Honorato et al. (2017, p. 14).

Focando no ciberespaço, a publicação doutrinária da NATO (2020, pp. 2 e 3) define este domínio em três estratos principais: a camada física dos equipamentos e ligações, o nível lógico das aplicações e a camada das *cyber-persona*[19] (Figura 6). Segundo a mesma publicação, atendendo ao facto que o ciberespaço pode ser manipulado, importa referir que esta ação é desenvolvida pela última camada, através da dissociação real das pessoas ou organizações que nele atuam.

Figura 6 - Modelo tridimensional do Ciberespaço
Fonte: Disponível em NATO (2020, p. 3).

[19] Ver Apêndice A – Corpo de Conceitos.

Destarte, fruto da expansão do "campo de batalha" para além das ações cinéticas, através da convergência no uso das doutrinas tradicionais com a aplicação de novas tecnologias (Danyk et al., 2017, p. 23), o ciberespaço consubstancia-se num domínio que deve, doravante, ser considerado nos cenários da atual conflitualidade, sendo provido de mecanismos que permitam exponenciar as suas capacidades (Schröefl, 2020, p. 4).

Aliando esta premissa à temática das AH, segundo vários autores, comprova-se que o ciberespaço, apesar de se constituir como um domínio por si só, torna-se o principal catalisador de ações híbridas que afetam os outros domínios (Alves, 2020, p. 11; Schröefl, 2021). Quer pela abrangência e rapidez de atuação, assim como, pela dificuldade de identificação e atribuição dos atores que nele atuam (Abaimov & Martellini, 2017, p. 107), a atuação no ciberespaço, "[…] mesmo que com contornos agressivos, dificilmente se poderá considerar um ato de guerra à luz do Direito Internacional vigente[…]" (Nunes et al., 2018, p. 14).

2.1.3 A Doutrina Russa

Vários autores debruçam-se sobre a doutrina russa, atendendo à conflitualidade atual, e à forma como a Rússia se coloca nesse quadro (Chivvis, 2017; Nilsson, 2018; Clark, 2020; Weissmann, Nilsson, Palmertz & Thunholm, 2021), devendo-se contudo, referenciar as origens deste interesse, assim como as principais ideias dos autores que inicialmente o interpretaram (Chekinov & Bogdanov, 2013; Bērziņš, 2014; Kasapoglu, 2015). O fator que norteou o interesse académico adveio dos postulados veiculados pelo General Gerasimov, em 2013, na Academia das Ciências Militares Russa e posteriormente publicado numa revista militar[20], onde, o Chefe de Estado-Maior das Forças Armadas (FFAA) Russas, de forma retórica, apresentou um quadro conceptual da nova conflitualidade, no qual se esbatiam os níveis do espectro do conflito entre a paz e a guerra, e onde atuavam, cada vez mais integrados, os meios militares e não militares (Weissmann et al., 2021, p. 4).

A visão de Gerasimov, na qual acusava o Ocidente de conduzir uma GH contra a Rússia, através da ingerência nas "revoluções coloridas"[21] (Thornton, 2015, p. 42), permitiu a interpretação de muitos autores ocidentais face a esta retórica, na correlação de que, numa vertente puramente russa, se indicava como conflito não-linear (Kasapoglu, 2015).

[20] Em 26 de fevereiro de 2013, o General Valery Gerasimov publicou o artigo "*The Value of Science is in the Foresight: New Challenges demand rethinking the forms and methods of Carrying ou Combat Operations*" no jornal russo *Voyenno-Promyshlennyy Kurier* (Bartles, 2016).
[21] Ver Apêndice A - Corpo de Conceitos.

Destarte, Nilsson (2018, pp. 17-18) alude que o postulado de Gerasimov assentava no uso integrado de meios não-militares com os meios militares na condução dos conflitos, constituindo-se os primeiros como partes primordiais de uso em tempo de paz, por forma a estabelecer dependências e "pontos de pressão" no adversário, permitindo assim, a sua desestabilização sem recurso aos meios militares, evitando os custos que isso acarretaria.

O conflito da Geórgia em 2008, e posteriormente a anexação da Crimeia, em 2014, vieram demonstrar que a forma russa de fazer a guerra se tinha alterado, através de novas formas e meios de atuação, assim como pela centralização política das operações (Galeotti, 2014).

Com principal destaque neste trabalho, importa referenciar a teorização de Bērziņš (2014), que, através do trabalho realizado para a Academia Nacional de Defesa da Letónia, procurou identificar a nova forma de atuação russa, interpretando o artigo de Chekinov e Bogdanov (2013) e analisando os acontecimentos do conflitos contemporâneos, com enfoque no conflito da Ucrânia em 2014.

No artigo "*The Nature and Content of a New-Generation War*", Chekinov e Bogdanov (2013), analisaram as ideias conceptuais de vários especialistas russos, mormente no plano securitário e na evolução do pensamento estratégico russo no que concerne ao fenómeno da guerra. O principal testemunho destes autores materializou-se na conceção de um conjunto de ações e atividades político-militares, que, de forma faseada e integrada, permitiriam às FFAA russas combater as "guerras de nova-geração a médio e a longo prazo", usando formas de atuação maioritariamente indiretas (Chekinov & Bogdanov, 2013, p.23).

De forma sistematizada, Bērziņš (2014, p.4) analisou o "novo pensamento estratégico militar russo" e os seus novos métodos (Quadro 1), assente principalmente em quatro pilares: no confronto de forças militares enquadrados na ausência de "declaração de guerra"; no uso de civis armados para desenvolver ações militares; no uso de meios indiretos e assimétricos, e na aplicação sincronizada de ações nos vários domínios, incluído o informacional.

No mesmo alinhamento, Kasapoglu (2015, p. 4) reforçou a ideia de mudança do pensamento estratégico russo da sua matriz tradicional, que anteriormente preconizava o uso de operações militares de grande envergadura num quadro subsequente à declaração de guerra, para uma matriz difusa do uso do instrumento militar sincronizado com outros instrumentos de poder.

Quadro 1 - Alteração das características dos conflitos armados segundo Gerasimov

Métodos Militares Tradicionais	Novos Métodos Militares
Ação militar começa após projeção estratégica (Declaração de Guerra).	Ação militar começa por grupos de tropas durante tempo de paz (sem existência de Declaração de Guerra).
Confrontos entre grandes unidades, constituídas na sua maioria por componente terrestre.	Confrontos (evitando o empenhamento decisivo) de unidades específicas e altamente móveis.
Derrota do potencial humano, do poder de fogo, assumindo o controlo de zonas de fronteira para obter o controlo territorial.	Aniquilação do poder militar e económico do inimigo, através de ataques curtos e precisos contra infraestruturas militares e civis.
Destruição do poder económico e anexação territorial.	Utilização massiva de armas de alta precisão e Forças de Operações Especiais, robótica, e armas que utilizam novos princípios (armas lasers, radiação de ondas curtas).
Operações de combate em terra, ar e mar.	Utilização de civis armados (4 civis para 1 militar).
Direção de tropas através de hierarquia e governança rígidas.	Ataque simultâneo às Forças militares e instalações do inimigo em todo o território.
	Batalha simultânea em terra, ar, mar e no espaço informacional.
	Utilização de métodos assimétricos e indiretos.
	Direção de tropas através do espaço informacional comum.

Fonte: Adaptado de Bērziņš (2014, p. 4).

Aliado à mudança do pensamento russo, Bērziņš (2014, p. 5) incrementou que, a nova visão russa se consubstanciava na "mente humana" como o novo espaço de batalha, recorrendo primordialmente aos vetores informacionais e psicológicos, criando efeitos disruptivos nos elementos das forças militares e na sociedade em geral, na senda de alcançar a superioridade face a um adversário. Para Bērziņš (2014, p. 9), esta visão centrada na mente humana "representa uma guerra de sétima geração". Mas será este um conceito novo?

Segundo Kasapoglu (2015, p. 2), o pensamento estratégico russo, através da opção da não-linearidade e da influência da mente humana, é a revitalização do conceito soviético do "controlo-reflexivo"[22], permitindo um impacto no adversário de forma rápida e dissimulada.

Integrando os novos métodos russos e o racional de conflito não-linear, Bērziņš (2014) sistematiza o pensamento de Chekinov e Bogdanov (2013) num conjunto de atividades enquadradas em oito fases (Quadro 2), em conformidade com o aludido por Kasapoglu (2015) na medida em que se assiste à "compressão dos níveis estratégicos, operacionais e táticos", num espetro de conflito onde se presencia cada vez mais a "sincronização de meios convencionais e não-convencionais" (Kasapoglu, 2015, pp. 11 e 12).

[22] Ver Apêndice A – Corpo de Conceitos.

Quadro 2 - Fases e Atividades da Doutrina Russa

Fases	Atividades
I	Conflito assimétrico não militar (abrangendo informação, medidas morais, psicológicas, ideológicas, diplomáticas e económicas como parte de um plano para estabelecer uma favorável moldagem política, económica e militar).
II	Operações especiais para ludibriar os líderes políticos e militares através de medidas coordenadas, levadas a cabo por canais diplomáticos, *media*, e altas entidades governamentais e militares, através da fuga de dados falsos, ordens e diretivas.
III	Intimidação, engano e suborno de oficiais governamentais e militares, com o objetivo de os fazer abandonar os seus deveres
IV	Propaganda desestabilizadora para aumentar o descontentamento entre a população, impulsionada pela chegada de bandos de militantes russos, escalando a subversão.
V	Estabelecimento de zonas de exclusão aérea sobre o país a ser atacado, imposição de bloqueios, e utilização extensiva de empresas militares privadas em estreita cooperação com unidades convencionais.
VI	Início da Acão militar, imediatamente precedida de ações de reconhecimento e subversivas em larga escala. Todos os tipos, formas, métodos e forças, incluindo: forças de operações especiais, aplicação de meios espaciais, ação diplomática e de serviços secretos, e espionagem industrial.
VII	Combinação de operações de informação direcionadas, operações de guerra eletrónica, operações aeroespaciais; assédio contínuo da força aérea, combinado com o uso de armas de alta precisão lançadas a partir de várias plataformas (artilharia de longo alcance, e armas baseadas em novos princípios físicos, incluindo micro-ondas, radiação e armas biológicas não-letais).
VIII	Conquista dos restantes pontos de resistência e destruição de unidades inimigas sobreviventes através de operações conduzidas por unidades de reconhecimento para detetar quais as unidades inimigas sobreviventes e transmitir as suas coordenadas às unidades de mísseis e artilharia do atacante; barragens de fogo para aniquilar as unidades resistentes através de armas avançadas; operações aerotransportadas para cercar pontos de resistência; e operações de conquista de território por tropas terrestres.

Fonte: Adaptado de Bērziņš (2014, p. 6).

Aliado a este quadro conceptual, Clark (2020, p. 9) realçou que, a mudança fundamental no processo de planeamento russo consistia na "subordinação" das operações cinéticas às operações no domínio informacional, nas quais, segundo Chivvis (2017, p. 3), se verifica a operacionalização de mecanismos e capacidades, mormente as operações de informação e operações ciber[23]. Esta visão é reforçada por Jonsson (2019, p. 123), aludindo que a doutrina militar russa, emanada em 2010, estabelece que a "guerra informacional pode atingir objetivos políticos sem o uso da força", emancipando-se assim, da atividade cinética.

2.2 Modelo de análise

Concluída a explanação do estado da arte e da revisão de literatura, identificaram-se as bases conceptuais enquadrantes e o interesse da comunidade académica na temática da presente investigação, permitindo assim, o contributo para o conhecimento através do objeto de estudo e ao fenómeno associado (Quivy e Campenhoudt, 1998, p. 238 *cit*. por Santos & Lima, 2019). Em conformidade, elaborou-se o modelo de análise[24] onde são apresentados os conceitos estruturantes, as dimensões, respetivas variáveis e indicadores em estudo.

[23] Ver Apêndice A – Corpo de Conceitos.
[24] Ver Apêndice C – Modelo de Análise.

3. Metodologia e método

Verificando-se a importância que a metodologia assume na investigação científica (Sarmento, 2013; Santos & Lima, 2019), no presente capítulo são apresentadas a metodologia e método aplicado.

3.1 Metodologia

A metodologia aplicada na presente investigação e a estrutura utilizada, baseiam-se nas normas em vigor no Instituto Universitário Militar (IUM).

Para atingir o OG, a metodologia consubstancia-se na adoção do raciocínio indutivo, para que, através da "observação de factos particulares" e da sua interligação, nomeadamente as ações e efeitos relacionados com uso das ferramentas das AH, se possam estabelecer relações que, quando interpretadas, possibilitem projetar comportamentos genéricos consentindo responder à questão central e subsidiariamente às questões derivadas (Santos & Lima, 2019, p. 18).

Com vista a correlacionar os diferentes modelos e a compreender como a Rússia atua como AH, a estratégia de investigação a seguir será qualitativa, sendo um estudo essencialmente indutivo e analítico, no qual "a interpretação dos fenómenos sociais e a atribuição dos respetivos significados é feita a partir de padrões encontrados nos dados", procurando compreender a realidade social de um determinado grupo (Vilelas, 2009, cit. por Santos & Lima, 2019, p. 27).

O desenho de pesquisa a utilizar será um estudo de caso, na medida em que para alcançar o OG será analisada a "informação recolhida sobre um grupo específico" (Yin, 1993 e 2005, cit. por Santos & Lima, 2019, p. 36), concretamente a Rússia como AH, recorrendo ao uso do domínio do ciberespaço em dois contextos geográficos e temporais distintos.

3.2 Método

3.2.1 Participantes e procedimento

O percurso metodológico decorreu em duas fases.

Por forma a permitir uma correta abordagem à temática e a definição inicial do estado da arte, na primeira fase foi efetuada uma revisão bibliográfica, aliado à participação em Seminários e *Webinars*, dos quais se destaca "*A Crise Ucraniana e as Transformações no Espaço Pós-Soviético*"[25]. No mesmo período, e tendo como objetivo o enquadramento da

[25] *Webinar* realizado pelo Instituto de Defesa Nacional no dia 07 de fevereiro de 2022.

temática e a assimilação de conhecimento, foram realizadas entrevistas exploratórias[26]. O final desta fase culminou com a elaboração do projeto de investigação.

No que respeita à segunda fase da investigação, num primeiro momento, efetuou-se uma análise do modelo das AH vertido no estudo *The Landscape of Hybrid Threats* (Giannopoulos et al., 2021) que se constitui como base conceptual para o presente trabalho. Num segundo momento, analisaram-se os conflitos para induzir quais as ferramentas das AH usadas no ciberespaço, merecendo posterior validação através das entrevistas. Para estas, constituiu-se uma amostra não-probabilística intencional (Pardal & Correia, 1995, p. 34), convidando-se 17 especialistas nacionais e estrangeiros, dos quais dez[27] aceitaram ser entrevistados[28]. Das entrevistas resultou a validação das ferramentas e a afirmação de outras não tidas empiricamente.

3.2.2 Instrumentos de recolha de dados

Na presente investigação utilizaram-se como instrumentos de recolha de dados a entrevista e a análise documental:

- Foram efetuadas dez entrevistas semiestruturadas[29] (Santos & Lima, 2019, p. 85), constituídas por quatro questões. Foram escolhidas entrevistas semiestruturadas por forma a permitir aos entrevistados, mesmo seguindo o guião, exprimirem as suas opiniões, na mesma medida que permitiu ao entrevistador solicitar esclarecimentos adicionais (Sarmento, 2013, p. 34).

A análise documental, baseada em literatura científica e documentos oficiais do *Hybrid CoE*, MCDC, CCDCOE, serviu de base para a realização das entrevistas, mas também para efetuar a complementaridade de dados na análise dos resultados.

3.2.3 Técnicas de tratamento de dados

A análise das entrevistas semiestruturadas foi efetuada de acordo com a metodologia proposta por Sarmento (2013, pp. 48), através de análise temática ou categorial[30]. A análise categorial foi efetuada seguindo os seguintes passos para cada uma das questões:

- Constituição das unidades de contexto;

[26] Realizadas ao Capitão-de-Mar-e-Guerra Fialho de Jesus, na qualidade de ex-Chefe do Centro de CiberDefesa do Estado-Maior General das Forças Armadas (EMGFA), e ao Sr. Embaixador Luís Barreira de Sousa, Embaixador para a Ciberdiplomacia desde 2016.

[27] Com responsabilidades profissionais e científicas no âmbito Ciber e na temática das AH, reúnem conhecimentos profundos, quer pelos cargos que ocupam ou ocuparam anteriormente, assim como pelos trabalhos de investigação desenvolvidos, aglutinando "características muito homogéneas que permitem o acesso a informação interessante e de forma concentrada" (Rego et al., 2018, p. 49).

[28] Ver Apêndice E – Lista de Entrevistados.

[29] Ver Apêndice F – Guião de Entrevistas Semiestruturadas.

[30] Ver Apêndice G – Análise de Conteúdo das Entrevistas Semiestruturadas.

- Determinação das unidades de registo;
- Elaboração do quadro matriz das unidades de contexto e de registo;
- Elaboração do quadro de análise de conteúdo, por categorias e subcategorias, com a quantificação das unidades de registo, de acordo com as unidades de enumeração;
- Produção de conclusões, "evidenciando os resultados superiores a 50% e enfatizando os resultados maiores ou iguais a 80%" (Sarmento, 2013, p. 66).

Foram utilizados os programas *Microsoft Excel*, *Microsoft Power Business Intelligence* e *Microsoft Word*, para apoio à organização e estruturação das unidades de contexto, determinação e quantificação das unidades de registo, e apresentação gráfica dos resultados.

4. Apresentação dos dados e discussão dos resultados

No presente capítulo apresentam-se os dados resultantes da investigação, discutindo-os, e dividindo-os em quatro subcapítulos. No primeiro são investigadas as ferramentas das AH que são passíveis de serem iniciadas ou potenciadas no ciberespaço, dando-se resposta à primeira QD. No segundo subcapítulo é efetuada uma análise ao uso das ferramentas das AH no ciberespaço por parte da Rússia, em dois conflitos recentes, permitindo responder à segunda QD. No terceiro, efetua-se uma análise à integração conceptual das AH na doutrina russa, permitindo responder à terceira QD. No quarto e último subcapítulo, é explanada uma síntese conclusiva, dando-se resposta à QC da investigação.

4.1 Ameaças Híbridas e o uso do Ciberespaço

Tendo como ponto de partida a lista conceptualizada por Giannopoulos et al. (2021) das 40 ferramentas das AH e respetivos domínios afetados[31], inferiu-se que dez das suas ferramentas usam o ciberespaço, pelo facto de afetarem o domínio ciber, sobre o qual, a sua ação pode causar "degradação, disrupção ou destruição dos sistemas em rede"(Giannopoulos et al., 2019, p. 35).

Contudo, atende-se ao facto que as AH são permeáveis às dinâmicas das alterações do ambiente onde atuam, podendo por isso, ser iniciadas ou estimuladas no ciberespaço (Danyk et al., 2017), não o afetando diretamente, mas apenas servindo-se deste, como meio para atuar.

Assim, foi efetuada uma consulta de bibliografia na procura de ações e efeitos nesse domínio espacial[32], permitindo analisar o uso de outras ferramentas das AH. Posteriormente, foram apresentadas aos dez entrevistados[33], por forma a validar as ferramentas passíveis de serem aplicadas no ciberespaço.

4.1.1 Adequação das ferramentas das Ameaças Híbridas no Ciberespaço

A partir das respostas dadas à primeira questão[34], efetuou-se uma análise categorial, concernente às ferramentas das AH apresentadas como passíveis de serem aplicadas no ciberespaço, sob as quais se enfatiza com mais de 80% de concordância:

[31] Ver Apêndice B – Ferramentas das AH e Domínios afetados.
[32] Ver Apêndice D – Lista de Indicadores.
[33] Ver Apêndice F – Guião de Entrevistas Semiestruturadas.
[34] Ver Apêndice G – Análise de Conteúdo das Entrevistas Semiestruturadas.

Quadro 3 - Unidades de Registo verificadas na primeira questão

Ferramentas das AH	Concordância (%)
1. Operações físicas contra infraestruturas	80
2. Criação e exploração da dependência de infraestruturas	100
4. Investimento estrangeiro direto	90
5. Espionagem industrial	100
6. Afetar a economia nacional do oponente	100
8. Ciber-espionagem	100
9. Operações Ciber	100
13. Operações Convencionais e não Convencionais das FFAA	100
14. Organizações Paramilitares (*Proxies*)	100
15. Exercícios militares	90
16. Influência através de diásporas	100
18. Exploração de clivagens socioculturais	100
19. Promoção da agitação social	100
21. Exploração de vulnerabilidades na Administração Pública (gestão de emergências)	100
23. Explorar limites, lacunas e incertezas na legislação	90
24. Aproveitamento das regras legais, de processos, Instituições e argumentos	100
25. Recolha de Informações	100
31. Criação de confusão e narrativas contraditórias	100
33. Desacreditar a liderança e/ou candidatos	100
37. Controlo e interferência nos *media*	100
38. Campanhas de desinformação e propaganda	100
40. Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite)	100

Verificando estes resultados importa referir que todas as ferramentas apresentadas tiveram um elevado grau de concordância, estando em sintonia com o referido por J. Schröefl (entrevista por via telemática[35], 28 de março de 2022), que "o ciberespaço é principal facilitador das AH", não deixando de referir que, segundo H. Fernandes (entrevista por via telemática, 23 de março de 2022), as ferramentas das AH indicadas podem atuar no ciberespaço, podendo, "de forma síncrona, atuar ou influenciar outros domínios espaciais".

Das respostas à mesma questão, foram indicadas, por mais de 50% dos entrevistados, as seguintes ferramentas:

- Apoio a atores Políticos;
- Coação de Políticos e/ou Governos.

Importa referenciar que estas ferramentas foram consideradas pela associação crescente das plataformas multimédia e pelo alcance das ações provocadas no ciberespaço, tal como referido por J. Schröefl (*op. cit.*), "tendo em consideração o domínio informacional, assiste-se a uma interferência nos atores políticos". Concretamente no que se refere à ferramenta "Apoio a atores Políticos", J. Teixeira (entrevista por via telemática, 29 de março de 2022) refere como indicador as "operações de influência com uso primordial nas redes

[35] Através da plataforma "Teams".

sociais", e no caso antagónico da "Coação de Políticos e/ou Governos", D. Antunes (entrevista por via telemática, 23 de março de 2022) evidencia o "racional de *cyber stalking*[36], que através da exposição mediática de informação pessoal influencia a ação do alvo", assim como, segundo A. Grilo (entrevista presencial, 04 de abril de 2022) "no caso americano, a exposição de informação de familiares de um ator político afetou diretamente a sua ação e credibilidade".

Ainda na senda das ferramentas indicadas pelos especialistas, obtiveram-se com baixo nível de concordância, abaixo dos 30%, as seguintes:

- Fomento das dificuldades económicas;
- Violação do Espaço Aéreo;
- Financiamento de grupos culturais e *think tanks*;
- Manipulação de discursos sobre migração para polarizar sociedades e minar democracias liberais;
- Promoção e exploração da corrupção;
- Operações Clandestinas;
- Aproveitamento da imigração para obter influência Política;
- Influência em currículos e estabelecimento de ensino.

Apesar do baixo grau de concordância, pela falta de dados que os confirmem, e através das respostas dos entrevistados, importa evidenciar as ferramentas "Financiamento de grupos culturais e *think tanks*" e "Promoção e exploração da corrupção". Quanto à primeira ferramenta, J. Teixeira (*op. cit.*) refere que esta "pode ser aplicada através de transações no ciberespaço (i.e. *bitcoins*), através das relações entre *Cyber-Personas*". Na mesma medida, tendo em conta a ferramenta "Promoção e exploração da corrupção", A. Marques (entrevista presencial, 21 de março de 2022) aponta para "existência de um subproduto digital (i.e. cripto-moedas), que pode promover os pagamentos de forma indetetável para ações criminosas".

4.1.2 Resposta à primeira questão derivada

Em resposta à QD "Quais as ferramentas das AH que se adequam à utilização no ciberespaço?", e após a analise efetuada, identificam-se as seguintes:

[36] Ver Apêndice A – Corpo de Conceitos.

Quadro 4 - Ferramentas das AH que se adequam ao uso do Ciberespaço

Ferramentas das AH que se adequam no uso do Ciberespaço
1. Operações físicas contra infraestruturas
2. Criação e exploração da dependência de infraestruturas
4. Investimento estrangeiro direto
5. Espionagem industrial
6. Afetar a economia nacional do oponente
8. Ciber-espionagem
9. Operações Ciber
13. Operações Convencionais e não Convencionais das FFAA
14. Organizações Paramilitares (*Proxies*)
15. Exercícios militares
16. Influência através de diásporas
18. Exploração de clivagens socioculturais
19. Promoção da agitação social
21. Exploração de vulnerabilidades na Administração Pública (gestão de emergências)
23. Explorar limites, lacunas e incertezas na legislação
24. Aproveitamento das regras legais, de processos, Instituições e argumentos
25. Recolha de Informações
31. Criação de confusão e narrativas contraditórias
33. Desacreditar a liderança e/ou candidatos
34. Apoio a Atores Políticos
35. Coação de Políticos e/ou Governos
37. Controlo e interferência nos *media*
38. Campanhas de desinformação e propaganda
40. Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite)

4.2 A Rússia como Ameaça Híbrida no Ciberespaço

Verificando-se, por parte da Rússia, a "propensão do desenvolvimento de capacidades e operações no ciberespaço"(Lilly & Cheravitch, 2020, p. 129), e atendendo que, segundo Freire (2022), as ações efetuadas no ciberespaço permitem à Rússia "obter influência no espaço pós-soviético", mormente na Geórgia e na Ucrânia, onde assenta a sua "afirmação no plano internacional", importa de seguida analisar os conflitos desenvolvidos pela Rússia nestes dois espaços, focando a lente no uso das ferramentas das AH no ciberespaço.

4.2.1 A utilização do Ciberespaço no conflito da Geórgia

Observando o conflito Russo-Georgiano, e após a investigação de ações e efeitos na bibliografia consultada[37], foram apresentadas aos dez entrevistados, as possíveis ferramentas das AH utilizadas no ciberespaço pela Rússia[38].

A partir das respostas dadas à segunda questão[39], efetuou-se uma análise categorial, que dos resultados obtidos se enfatiza com mais de 80% de concordância as ferramentas:

[37] Ver Apêndice D – Lista de Indicadores.
[38] Ver Apêndice F – Guião das Entrevistas Semiestruturadas.
[39] Ver Apêndice G – Análise de Conteúdo das Entrevistas Semiestruturadas.

Quadro 5 - Unidades de Registo verificadas na segunda questão

Ferramentas das AH	Concordância (%)
6. Afetar a economia nacional do oponente	90
8. Ciber-espionagem	100
9. Operações Ciber	100
13. Operações Convencionais e não Convencionais das FFAA	100
14. Organizações Paramilitares (*Proxies*)	100
15. Exercícios militares	100
21. Exploração de vulnerabilidades na Administração Pública (gestão de emergências)	100
23. Explorar limites, lacunas e incertezas na legislação	90
25. Recolha de Informações	100
31. Criação de confusão e narrativas contraditórias	100
33. Desacreditar a liderança e/ou candidatos	100
37. Controlo e interferência nos *media*	90
38. Campanhas de desinformação e propaganda	100

Verificando os resultados, tal como referiu J. Vinagreiro (entrevista por email, 05 de abril de 2022), "foi a primeira vez que as operações no ciberespaço foram utilizadas em sincronismo com as operações militares cinéticas", estando em alinhamento com o explanado por Nilsson (2018, p. 15) quando infere que na "Geórgia em 2008, foi a primeira vez que os ciberataques foram combinados com as operações militares convencionais".

Importa também evidenciar que, tal como aludido por H. Fernandes (*op. cit.*), "as ferramentas foram sentidas de forma direta ou indiretamente", estando em sintonia com o racional de "efeitos de segunda e terceira ordem nos domínios do adversário" (MCDC, 2017, p. 14).

Das respostas dadas pelos entrevistados, foram indicadas um conjunto de ferramentas, que reuniram um nível de concordância abaixo dos 30%, concretamente:

- Operações físicas contra infraestruturas;
- Influência através de diásporas;
- Operações Clandestinas;
- Infiltração;
- Apoio a atores Políticos;
- Coação de Políticos e/ou Governos.
- Operações eletrónicas.

Apesar do baixo nível de concordância, segundo J. Teixeira (*op. cit.*), importa realçar que a ferramenta "Operações eletrónicas" foi "utilizada de forma indireta, resultante do uso primário da ferramenta Operações ciber, através da afetação de uma aplicação georgiana de cálculo de tiro de artilharia, provocando a disrupção na sua eficácia". Este racional está em linha com o preconizado por Giannopoulos et al. (2019, p. 81), na medida em que as

"operações ciber podem manipular informação ou bases de dados", materializando-se como catalisador de outras ferramentas.

Assim, de forma gráfica e em concordância com o modelo conceptual de Giannopoulos et al. (2021), importa integrar a aplicação das ferramentas das AH, sentidas no ciberespaço no conflito da Geórgia, com os domínios conceptualmente afetados, assim como as fases de atuação preconizadas, conforme Figura 7.

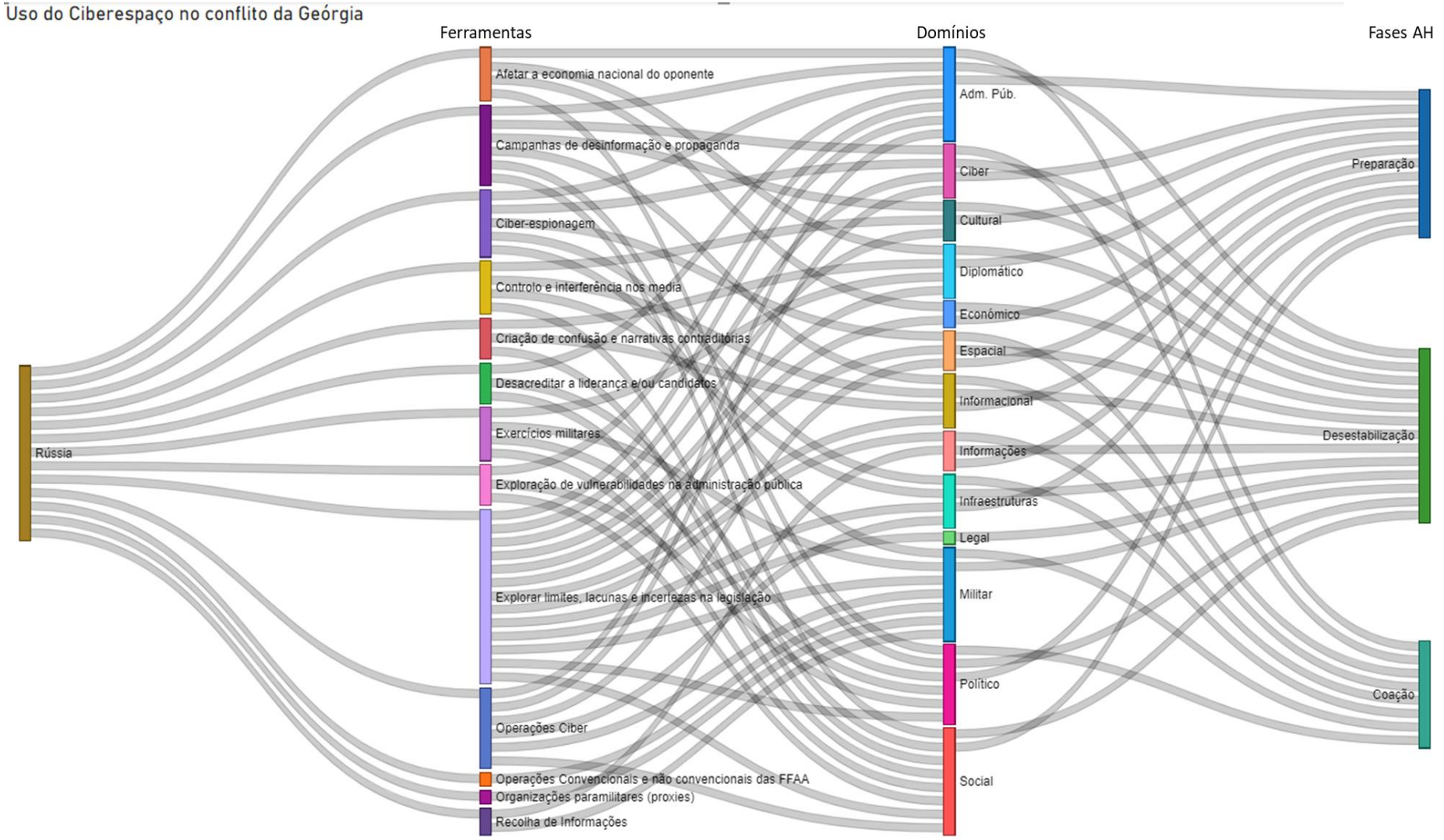

Figura 7 - Uso do Ciberespaço no conflito da Geórgia

4.2.2 A utilização do Ciberespaço no conflito da Ucrânia

No contexto do conflito Russo-Ucraniano, e da mesma forma que no subcapítulo anterior, foram apresentadas aos dez entrevistados, as possíveis ferramentas das AH utilizadas no ciberespaço pela Rússia[40].

A partir das respostas dadas à terceira questão[41], efetuou-se uma análise categorial, e enfatiza-se com mais de 80% de concordância as ferramentas:

Quadro 6 - Unidades de Registo verificadas na terceira questão

Ferramentas das AH	Concordância (%)
4. Investimento estrangeiro direto	90
6. Afetar a economia nacional do oponente	90
8. Ciber-espionagem	100
9. Operações Ciber	100
16. Influência através de diásporas	100
18. Exploração de clivagens socioculturais	100
19. Promoção da agitação social	100
21. Exploração de vulnerabilidades na Administração Pública (gestão de emergências)	100
23. Explorar limites, lacunas e incertezas na legislação	90
25. Recolha de Informações	100
31. Criação de confusão e narrativas contraditórias	100
33. Desacreditar a liderança e/ou candidatos	100
37. Controlo e interferência nos *media*	100
38. Campanhas de desinformação e propaganda	100
40. Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite)	100

Apurando-se a concordância das ferramentas assinaladas, releva-se a premissa de O. Rocha (entrevista por email, 14 de março de 2022) que "todas foram materializadas ou potenciadas através do ciberespaço", assim como, conforme J. Vinagreiro (*op. cit.*) evidencia, que "é notório que na comparação dos dois conflitos, no caso ucraniano, as ferramentas das AH foram mais potenciadas pelo ciberespaço".

Da lista apresentada, foi indicada por 60% dos entrevistados a ferramenta "Apoio a atores políticos. Nesta senda, M. Correia (entrevista via telemática, 24 de março de 2022) refere que "no caso da Ucrânia, o apoio a atores políticos pró-russos foi evidente como efeito reverso da desacreditação das lideranças na altura vigentes". Na mesma medida, A. Marques (*op. cit.*) reforça que "na desacreditação dos oponentes políticos russos, deu-se inerentemente, força e apoio aos candidatos pró-russos".

Apesar de ter sido indicada por 40% dos entrevistados, importa salientar a ferramenta "Coação de Políticos e/ou Governos". De acordo com A. Marques (*op. cit.*) foi evidente a aplicação desta ferramenta no ciberespaço, na medida em que "o Governo de Kiev ficou

[40] Ver Apêndice F – Guião das Entrevistas Semiestruturadas.
[41] Ver Apêndice G – Análise de Conteúdo das Entrevistas Semiestruturadas.

coagido na sua ação política, através das narrativas Russas", e que temporalmente, segundo H. Fernandes (op. cit.) a sua exponenciação pelo ciberespaço ocorreu "na fase que antecedeu o conflito, por forma a coagir os políticos pró-ocidentais".

Assim, de forma gráfica e em concordância com o modelo conceptual de Giannopoulos et al. (2021), importa integrar a aplicação das ferramentas das AH, sentidas no ciberespaço no conflito da Ucrânia, com os domínios conceptualmente afetados, assim como as fases de atuação preconizadas, conforme Figura 8.

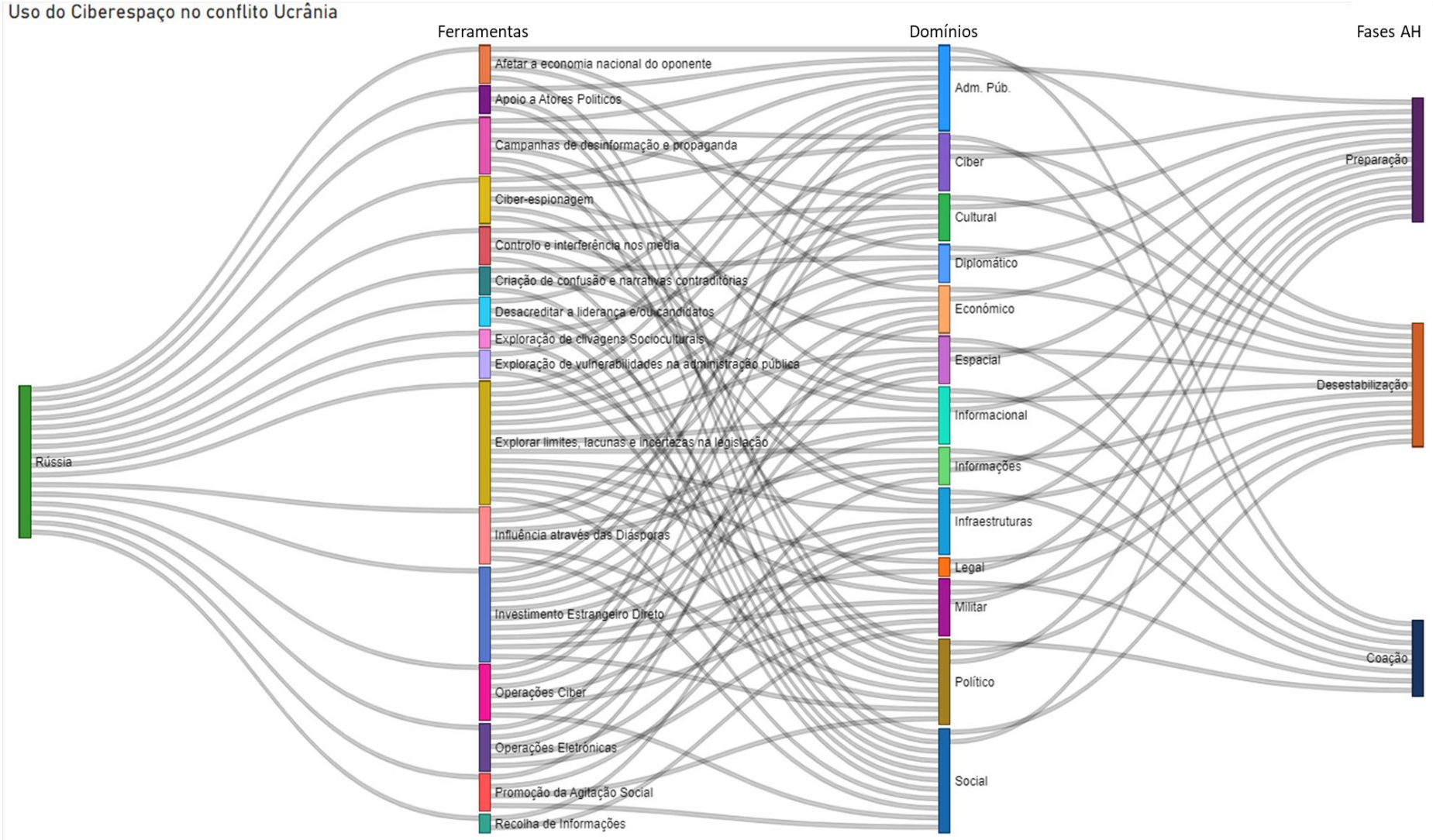

Figura 8 - Uso do Ciberespaço no conflito da Ucrânia

4.2.3 Resposta à segunda questão derivada

No seguimento da análise efetuada aos conflitos da Geórgia e da Ucrânia, aclaram-se os dados que permitem dar resposta à QD "De que forma foram aplicadas as ferramentas das AH no ciberespaço, nos conflitos perpetrados pela Rússia?". Assim, procedeu-se à integração das ferramentas aplicadas no ciberespaço por parte da Rússia, através do modelo conceptual Giannopoulos et al. (2021), no qual se verifica a aplicação total de 19 ferramentas, dando-se enfoque à padronização de dez ferramentas observadas nos dois momentos de conflito, integrando a afetação conceptual dos domínios do ator-alvo, num espectro abrangente das fases preconizadas nas AH, conforme refletido na Figura 9.

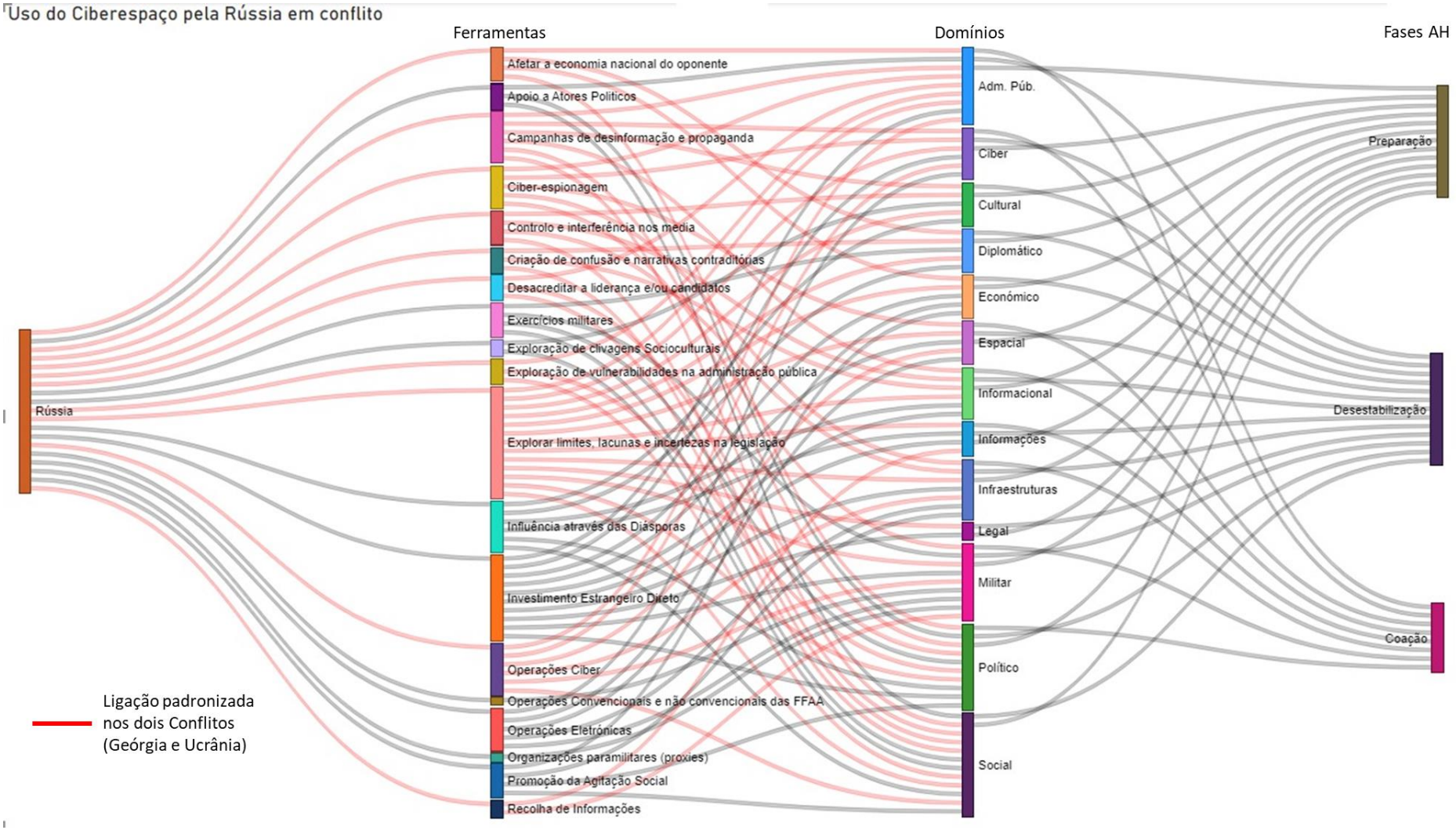

Figura 9 - Uso do Ciberespaço pela Rússia em conflito

4.3 As Ameaças Híbridas na Doutrina Russa

Conforme aludido por Berzin (2014, p. 7), o novo conceito estratégico russo não deve ser entendido como uma campanha clássica, mas compreendido como a operacionalização de um novo pensamento estratégico.

Relacionando as fases[42] do espectro de atuação das AH com as características das AH que englobam diferentes tipos de atividades, nos vários níveis de intensidade e através de diferentes alcances (Giannopoulos et al., 2021, p. 36), analisa-se de seguida a integração da atuação russa nesta equação.

4.3.1 A Doutrina Russa no espectro de atuação das Ameaças Híbridas

A partir das respostas dadas à quarta questão[43], efetuou-se uma análise categorial, referente à integração das fases da doutrina russa nas fases de atuação das AH.

No que respeita à fase de "Preparação" no espectro de atuação das AH, enfatiza-se com 100% de concordância a Fase I da doutrina russa, sendo aludido por D. Antunes (*op. cit.*) "que as atividades da Fase I são decisivas na Preparação", tornando claro a "abrangência de medidas numa lógica de moldagem do adversário"(Bērziņš, 2014, p. 6). Ainda na fase de "Preparação", realça-se a Fase II russa com 78% de concordância, dando nota que, segundo J. Schröefl (*op. cit.*) "as atividades da Fase II atuam maioritariamente na *gray zone*".

Passando para a subcategoria "Desestabilização", enfatiza-se com 100% de concordância dos entrevistados a Fase III e a Fase IV da doutrina russa, tornando-se claro que "parte das atividades destas fases retiram-se da opacidade da *gray zone*", conforme evidenciado por A. Grilo (*op. cit.*). No que respeita à integração da Fase III, A. Gameiro (*op. cit.*) refere que esta se encontra numa "linha de fronteira entre a *gray zone* e a área detetável", e que a suas atividades ao "afetarem elementos estruturais de um alvo estão já na fase de desestabilização". No que respeita à Fase IV, alinhado com a premissa de que as "atividades de propaganda dão a perspetivação da escalada de subversão" (Bērziņš, 2014, p. 6), D. Antunes (*op. cit.*) identifica que a "utilização de Operações Psicológicas nesta fase permitem a redução temporal de um futuro conflito".

Ainda nesta subcategoria, apesar de ter obtido 44% de concordância dos entrevistados, importa salientar a presença da Fase II, que conforme vincado por J. Schröefl (*op. cit.*), "está presente na *gray zone* mas com atividades a integrar a fase de desestabilização". Nesta senda, salienta-se na mesma medida a Fase V com 44% de concordância, aludindo à perceção dos entrevistados que pode ser iniciada na fase final da desestabilização, e tal como referido por

[42] Preparação, Desestabilização e Coação.
[43] Ver Apêndice G – Análise de Conteúdo das Entrevistas Semiestruturadas.

A. Marques (*op. cit*.) "com a implementação de zonas de exclusão aérea por parte de um possível agressor, pode ser considerada numa fase de transição para a Coação".

No que respeita à subcategoria da Coação, enfatizam-se os resultados com mais de 80% de concordância, mormente: a Fase V, a Fase VI, a Fase VII e a Fase VIII. Observando as atividades apresentadas por Bērziņš (2014, p. 6) nas fases anteriormente referenciadas, verifica-se a presença de uma matriz maioritariamente cinética da aplicação russa, estando alinhada com a assunção veiculada por S. Carvalho (*op. cit*.) na medida em que " a partir da Fase V as atividades enquadram-se num plano de conflito, impondo impactos cinéticos".

4.3.2 Resposta à terceira questão derivada

No seguimento do referido e respondendo à QD3 "Como se integra a doutrina russa no modelo conceptual das AH?", apresenta-se na figura 10 a disposição das Fases da doutrina russa no espectro de atuação das AH.

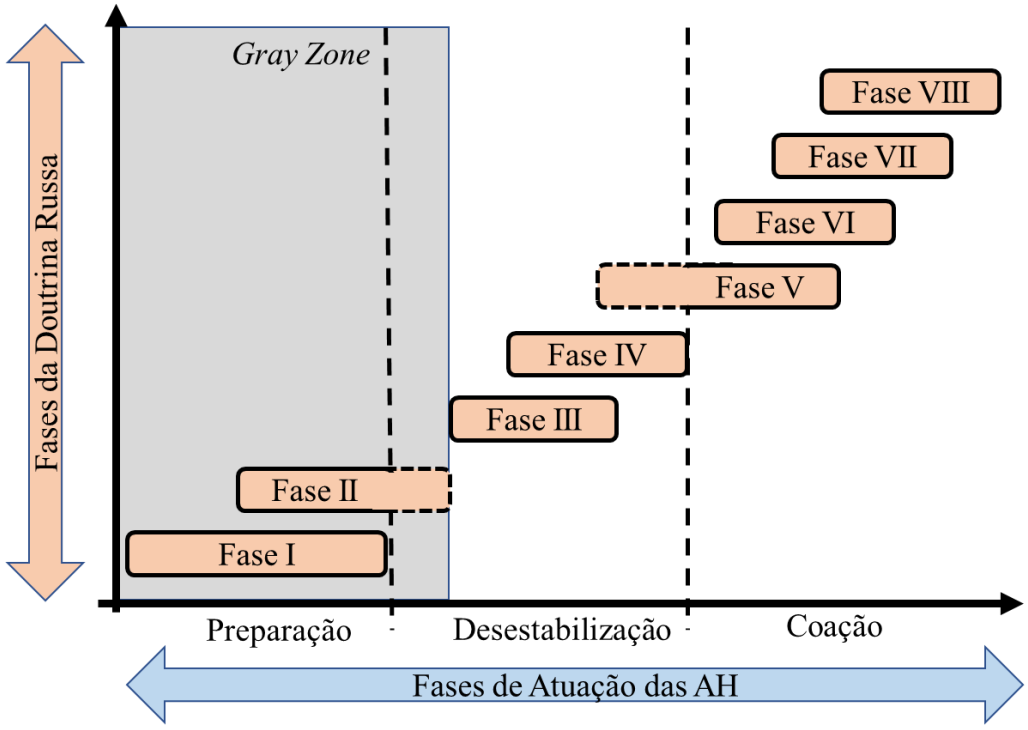

Figura 10 - Integração da Doutrina Russa no espetro de atuação das AH

4.4 Síntese conclusiva

Na sequência das respostas às QD, cumpre responder à QC "Qual o possível modelo de utilização do ciberespaço por parte Rússia como AH?". Assim, apresenta-se um possível modelo conceptual, conforme Figura 11, que integra as ferramentas das AH utilizadas no ciberespaço por parte da Rússia com os domínios conceptualmente afetados, assentes nas fases conceptuais do seu pensamento doutrinário, verificando neste, uma predominância nas fases compreendidas entre a Fase I e Fase IV, numa lógica de moldagem e desestabilização.

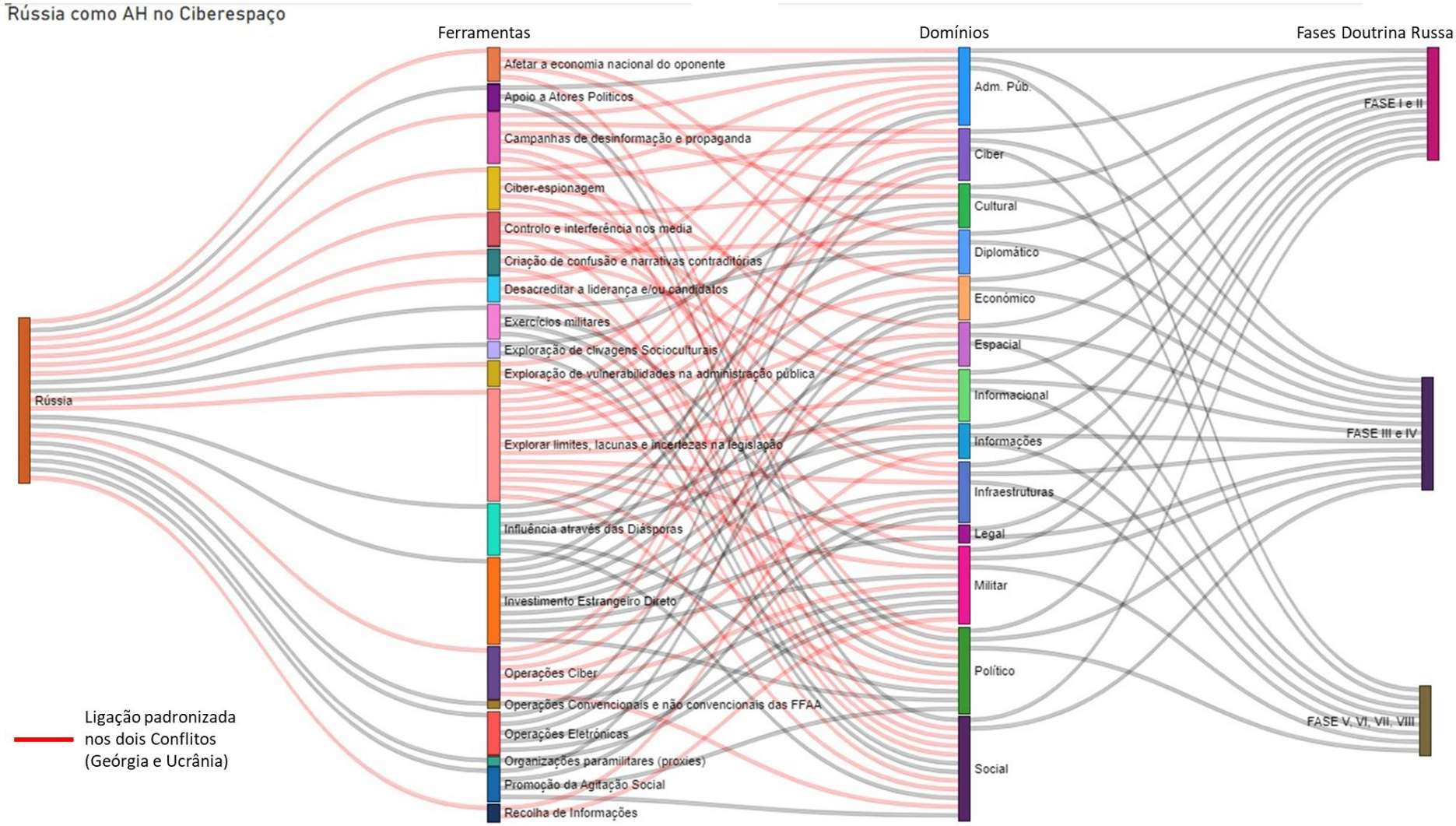

Figura 11 - Possível modelo de utilização do Ciberespaço pela Rússia como AH

5. Conclusões

Na conflitualidade atual, assiste-se cada vez mais ao esbatimento do espectro dos conflitos, através de ações síncronas perpetradas por uma abrangência de atores, num quadro de evidente disrupção com a sistematização clássica dos eventos, provocando desafios securitários no sistema internacional. Foi nesta moldura securitária que emergiu o conceito de "conflito híbrido", almejando teorizar de forma racional, as dinâmicas de atuação entre os vários atores, sejam eles estatais ou não-estatais, através da aplicação de métodos convencionais e não-convencionais, por forma a atingir os seus objetivos.

Nesta senda surgiu o conceito de GH, que acentua a combinação sincronizada dos vários instrumentos de poder disponíveis por um determinado ator contra as vulnerabilidades críticas do seu alvo, dando especial acento tónico ao instrumento militar como ponto focal de todas as formas de afetação.

Com o conflito Russo-Georgiano em 2008, e posteriormente com as ações desenvolvidas pela Rússia na Ucrânia, culminando com a anexação da Crimeia em 2014, intensificou-se a conexão da teorização "híbrida" com o desafio securitário provocado por esse ator, assistindo-se ao estabelecimento de plataformas colaborativas multinacionais, na busca de conhecimento transversal e de formas de resiliência face à nova tipologia de ameaça.

É neste enquadramento que surge o *Hybrid CoE* e o foco no fenómeno "híbrido" através do conceito das AH, que assente num modelo dinâmico, alumia a sincronização dos meios militares e não militares com o objetivo de afetar o processo de decisão do alvo, num espectro de atuação transversal, flutuando entre a opacidade da "*gray zone"* até à detetabilidade das atividades manifestamente coercivas. Desta forma, e integrando a taxonomia "híbrida", o conceito de GH é um estado de maturidade da ação da AH quando esta recorre aos meios predominantemente militares através de ações cinéticas.

Fruto da evolução tecnológica recente e da conectividade em rede num mundo globalizado, o ciberespaço constitui-se como um espaço de batalha catalisador das AH, presenciando-se por parte da Rússia, a adoção decisiva deste domínio operacional. É este o palco da guerra psicológica e de informação, que não é mais uma componente de apoio ao belicismo patente nas primeiras gerações da guerra, para passar a ser o meio de combate primordial face às democracias ocidentais.

Neste seguimento, considerando a Rússia como um ator que usa AH e almejando propor um modelo de sua utilização do ciberespaço, efetuou-se um estudo de caso, limitado

a dois conflitos recentes, utilizando para isso um raciocínio indutivo, assente numa estratégia qualitativa.

Tendo como objetivo o enquadramento da temática e a assimilação de conhecimento, foram realizadas entrevistas exploratórias, a par de uma leitura de bibliografia de referência e à participação em Seminários e *Webinars*. Posteriormente, e envolvido no raciocínio indutivo, foi feita uma revisão bibliográfica, permitindo firmar os indicadores essenciais para a investigação, concorrendo para a elaboração do guião de entrevista. A realização deste momento assentou numa amostra não-probabilística intencional, através de entrevistas semiestruturadas a dez especialistas com responsabilidades profissionais e científicas no âmbito Ciber e na temática das AH. A análise documental, apoiou-se na literatura científica e em documentos oficiais do *Hybrid CoE*, MCDC, CCDCOE, que, além de servir de base para a realização das entrevistas, permitiu também efetuar a complementaridade de dados na análise dos resultados.

Como principais conclusões, e após a analise efetuada, identificaram-se como possíveis de serem aplicadas no ciberespaço, as seguintes ferramentas das AH:

- Operações físicas contra infraestruturas;
- Criação e exploração da dependência de infraestruturas;
- Investimento estrangeiro direto;
- Espionagem industrial;
- Afetar a economia nacional do oponente;
- Ciber-espionagem;
- Operações Ciber;
- Operações Convencionais e não Convencionais das FFAA;
- Organizações Paramilitares (*Proxies*);
- Exercícios militares;
- Influência através de diásporas;
- Exploração de clivagens socioculturais;
- Promoção da agitação social;
- Exploração de vulnerabilidades na Administração Pública (incluindo gestão de emergências);
- Explorar limites, lacunas e incertezas na legislação;
- Aproveitamento das regras legais, de processos, Instituições e argumentos;
- Recolha de Informações;

- Criação de confusão e narrativas contraditórias;
- Desacreditar a liderança e/ou candidatos;
- Apoio a atores Políticos;
- Coação de Políticos e/ou Governos.
- Controlo e interferência nos *media*;
- Campanhas de desinformação e propaganda;
- Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite).

No que respeita às ferramentas das AH aplicadas pela Rússia no conflito da Geórgia, das 24 anteriormente elencadas, foram sentidas 13 ferramentas no ciberespaço, com a afetação conceptual de todos os domínios preconizados, num espectro de atuação transversal nas três fases. Concomitantemente, no conflito da Ucrânia, foram aplicadas 16 ferramentas no ciberespaço por parte da Rússia, afetando igualmente todos os domínios conceptualmente preconizados e integrando as três fases do espectro de atuação. Agregando os dois momentos analisados, verificou-se a aplicação cumulativa de 19 ferramentas no ciberespaço por parte da Rússia, verificando-se que dez das quais foram consistentes em ambos os conflitos, afetando transversalmente os domínios do ator-alvo, num espectro alargado das fases das AH.

Relativamente à integração da doutrina russa e da matriz não-linear das suas fases conceptuais com o modelo de atuação das AH, verificou-se que: a Fase I e a Fase II engloba atividades no âmbito da Preparação das AH; as Fases III e IV norteiam a sua atuação na fase de Desestabilização; e, da Fase V até à Fase VIII, pela sua matriz cinética, enquadram-se na fase de Coação das AH.

Como contributo para o conhecimento, a investigação permitiu propor um possível modelo de utilização do ciberespaço por parte da Rússia como AH.

No que respeita às ferramentas das AH aplicadas pela Rússia e sentidas no ciberespaço, consideraram-se 19 ferramentas, das quais se evidenciam dez pelo seu uso consistente:

- Afetar a economia nacional do oponente;
- Ciber-espionagem;
- Operações Ciber;
- Exploração de vulnerabilidades na Administração Pública (incluindo gestão de emergências);
- Explorar limites, lacunas e incertezas na legislação;

- Recolha de Informações;
- Criação de confusão e narrativas contraditórias;
- Desacreditar a liderança e/ou candidatos;
- Controlo e interferência nos *media*;
- Campanhas de desinformação e propaganda.

No que respeita aos domínios afetados, interligando conceptualmente as ferramentas acima elencadas, assiste-se à transversalidade de afetação nos 13 domínios identificados pelo modelo conceptual que serviu de base a este trabalho. Referente à atuação das ferramentas nos domínios afetados, apresenta-se da mesma forma, uma transversalidade no espectro de atuação das Fases doutrinárias russas, assistindo-se a uma maior representatividade no intervalo entre as Fases I e IV, em detrimento do intervalo compreendido entre as Fases V e VIII, sob os quais as atividades tendem a ser maioritariamente cinéticas.

Assumindo a coerência dos resultados obtidos no presente trabalho, importa identificar duas limitações à investigação. A primeira limitação prende-se com a abordagem académica de efetuar um estudo recorrendo a fontes abertas, que apesar de concorrer para a divulgação do presente conteúdo, limitou ainda assim, a análise aprofundada da aplicabilidade russa das ferramentas investigadas e dos efeitos provocados nos domínios afetados. Quanto à segunda limitação, alude-se ao facto de muita da bibliografia disponível sobre a temática do ciberespaço, associar exclusivamente este domínio espacial às operações ciber, podendo criar enviesamentos conceptuais, concretamente no estudo de outras atividades que usam a conectividade em rede, sobretudo no âmbito das AH.

Concernente a estudos futuros, percebendo a importância desta temática e da correlação do ator em estudo, torna-se pertinente aprofundar a atuação no ciberespaço por parte da Rússia, numa fase posterior da anexação da Crimeia até ao conflito bélico vivido na atualidade, concretamente nas ferramentas sentidas pela Ucrânia e em que medida foram afetados os seus domínios, concorrendo assim para um conhecimento mais consolidado e que, paralelamente, permita o melhoramento da prevenção e do combate às AH.

Referências bibliográficas

Abaimov, S., & Martellini, M. (2017). *Cyber Arms: Security in Cyberspace*. Boca Raton: CRC Press.

Alves, A. J. F. M. (2020). *A prevenção e o combate às Ameaças Híbridas: Impacto para as Forças Armadas Portuguesas*. (Trabalho de Investigação Individual, Curso de Promoção a Oficial General 2019-2020). Instituto Universitário Militar, Lisboa.

Australian Government. (2021). *The Whole of Government Challenge*. [Página *online*]. Retirado de https://legacy.apsc.gov.au/whole-government-challenge.

Awati, R. (2022). *Cyberstalking*. [Página *online*]. Retirado de https://www.techtarget.com/searchsecurity/definition/cyberstalking.

Bartles, C. K. (2016). Para Entender Gerasimov. *Military Review* (pp. 46–54). Retirado de https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/MilitaryReview_20160430_art010POR.pdf.

Bērziņš, J. (2014). *Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy*. *Paper* apresentado no Center for Security and Strategic Research, Riga.

CCDCOE. (2022). *About us*. [Página *online*]. Retirado de https://ccdcoe.org/about-us/.

Chekinov, S. G., & Bogdanov, S. A. (2013). The Nature and Content of a New-Generation War. *Military Thought* (pp. 12–23). Retirado de https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf.

Chivvis, C. (2017). *Understanding Russian "Hybrid Warfare": And What Can Be Done About It*. *Paper* apresentado no House Armed Services Committee, Washington D.C.

Clark, M. (2020). Russian "Hybrid Warfare." *Military Learning and the Future of War Series- Institute for the Study of War*. Retirado de https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf.

CNCS. (2021). *Glossário*. [Página *online*]. Retirado de https://www.cncs.gov.pt/pt/glossario/.

Coker, C. (2005). Cultural Ruthlessness and the War against Terror. *Australian Army Journal: Vol. III* (pp. 145–164). Retirado de https://search.informit.org/doi/pdf/10.3316/ielapa.200604653.

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber Conflicts. *Connections: The Quarterly Journal* (pp. 5–24). doi: 10.11610/connections.16.2.01.

European External Agency Service. (2018). *EUMC Glossary of Acronyms and Definitions - Revision 2017*. Bruxelas: European Union Military Committee.

Freire, M. R. (2022). *A Crise Ucraniana e as Transformações no Espaço Pós-soviético*. Em: Instituto da Defesa Nacional, A Crise Ucraniana e as Transformações no Espaço Pós-Soviético. *Webinar* organizado pelo Instituto de Defesa Nacional, Lisboa.

Galeotti, M. (2014). The ‘ Gerasimov Doctrine ’ and Russian Non - Linear War. *Moscows Shadows* (pp. 1–10). Retirado de https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

Geers, K. (2015). *Cyber War in Perspective: Russian aggression against Ukraine*. Tallinn: NATO CCD COE Publications.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2019). *The landscape of hybrid threats: A conceptual model*. *Working Paper* apresentado para a Comissão Europeia, Brussels.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The Landscape of Hybrid Threats: A conceptual model*. Luxembourg: Publications Office of the European Union.

Guedes, A. M. (2009). *A Guerra dos Cinco Dias: A invasão de Geórgia pela Federação Russa*. Lisboa: Instituto de Estudos Superiores Militares.

Harvard Kennedy School. (2016). . Former SACEUR, GEN Philip Breddlove [Página *online*]. Retirado de https://www.belfercenter.org/event/former-saceur-gen-philip-breedlove.

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hibrid Wars*. *Paper* apresentado no Potomac Institute for Policy Studies, Arlington.

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal* (Vol. 7, pp. 1–9). Retirado de https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Honorato, M. C., Santos, L. F. C. D., & Mateus, R. M. J. R. (2017). *O Ciberespaço como 5.º Domínio Operacional: Impacto Estratégico na Política de Defesa Nacional*. (Trabalho de Investigação de Grupo da Área de Ensino de Estratégia do Curso de Promoção a Oficial General 2016/2017). Instituto Universitário Militar, Lisboa.

Hybrid CoE. (2019). *Breaking the dominance of other domains?* Em: Cyber Power in Hybrid Warfare Symposium. Simpósio organizado pelo Hybrid CoE, Helsinquia.

Hybrid CoE. (2021). *Hybrid Threats*. [Página *online*]. Retirado de https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon.

Hybrid CoE. (2022a). *Establishment of Hybrid CoE*. [Página *online*]. Retirado de

https://www.hybridcoe.fi/establishment/.

Hybrid CoE. (2022b). *What is Hybrid CoE?* [Página *online*]. Retirado de https://www.hybridcoe.fi/who-what-and-how/.

Hybrid CoE, & CCDCOE. (2019). Nuclear energy and the current security environment in the era of hybrid threats. *Probation Journal* (Vol. 65, Issue 3). Retirado de https://stratcomcoe.org/publications/nuclear-energy-and-the-current-security-environment-in-the-era-of-hybrid-threats/74.

Jonsson, O. (2019). *The Russian Understanding of War: Blurring the lines between War and Peace*. Washington D.C.: Georgetown University Press.

Kasapoglu, C. (2015). Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control. *NATO Research Paper* (Vol. 121, pp. 1–8). Retirado de https://www.ndc.nato.int/news/news.php?icode=877.

Koval, N. (2015). Revolution Hacking. K. Geers (Ed.), *Cyber War in Perspective: Russian agression against Ukraine* (pp. 55–58). Tallinn: NATO CCD COE Publications.

Leonard, M. (2021). *Conflitos Híbridos e transformações na ordem internacional*. Em: Instituto de Defesa Nacional, III Seminário de Defesa Nacional. Seminário organizado pelo Instituto de Defesa Nacional, Lisboa.

Lewis, J. A. (2015). Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. K. Geers (Ed.), *Cyber War in Perspective: Russian agression against Ukraine* (pp. 39–47). Tallinn: NATO CCD COE Publications.

Libicki, M. (2015). The Cyber War That Wasn´t. K. Geers (Ed.), *Cyber War in Perspective: Russian agression against Ukraine* (pp. 49–54). Tallinn: NATO CCD COE Publications.

Lilly, B., & Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. *International Conference on Cyber Conflict, CYCON* (pp. 129–155). Retirado de https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf.

Mattis, J. N., & Hoffman, F. G. (2005). Future Warfare: The rise of Hybrid Wars. *Proceedings*. [Página *online*]. Retirado de https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.

Multinational Capability Development Campaign. (2017). *Understanding Hybrid Warfare*. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Multinational Capability Development Campaign. (2019). *MCDC Countering Hybrid Warfar Project : Countering Hybrid Warfare*. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

Najzer, B. (2020). *The Hybrid Age: International Security in the Era of Hybrid Warfare*. Londres: I.B. TAURIS.

NATO. (2020). *Allied Joint Publication - 3.20: Allied Joint Doctrine for Cyberspace Operations*. Bruxelas: NATO Standartization Office.

NATO. (2021). *NATO's response to hybrid threats*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_156338.htm.

NATO. (2022). *Cyber Defence*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en.

Nikitina, Y. (2014). The "Color Revolutions" and "Arab Spring" in Russia Official Discourse. *Connections: The Quarterly Journal* (Vol. 14, pp. 87–104). Retirado de https://www.jstor.org/stable/pdf/26326387.pdf.

Nilsson, N. (2018). Russian Hybrid Tactics in Georgia. *Central Asia-Caucasus Institute - Silk Road Studies Program*. Retirado de http://isdp.eu/content/uploads/2018/01/Russian-Hybrid-Tactics-in-Georgia.pdf.

Nunes, P. V., Mendes, C. P., Ralo, J., Santos, L., Santos, L. C., Moniz, P., & Casimiro, S. V. (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: Instituto de Defesa Nacional.

Pakharenko, G. (2015). Cyber Operations at Maidan: A First-Hand Account. K. Geers (Ed.), *Cyber War in Perspective: Russian agression against Ukraine* (pp. 59–66). Tallinn: NATO CCD COE Publications.

Pardal, L. A., & Correia, E. (1995). *Métodos e técnicas de investigação social*. Porto:Areal.

Pomerantsev, P. (2014). How Russia Is Revolutionizing Information Warfare. *Defense One*. [Página *online*]. Retirado de https://www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635/.

Rego, A., Cunha, M. P., & Junior, V. M. (2018). Quantos participantes são necessários para um estudo qualitativo ? Linhas Práticas de Orientação. *Revista de Gestão dos Países de Língua Portuguesa* (pp. 44–57). Retirado de https://bibliotecadigital.fgv.br/ojs/index.php/rgplp/article/view/78224/74934.

Saberwal, A. (2018). Russia and Hybrid Warfare: Achieving Strategic Goals without Outright Military Force. V. Deshpande (Ed.), *Hybrid Warfare: The Changing*

Character of Conflict (pp. 62–73). Nova Deli: Institute for Defence Studies & Analysis.

Santos, L. A. B., & Lima, J. M. M. (Coord.) (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.ª ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora.

Schröefl, J. (2020). *Cyber power is changing the concept of war*. *Paper* apresentado no HYbrid CoE Analysis/ 21. Retirado de https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis_21_Cyber-Power.pdf. www.hybridcoe.fi

Schröefl, J. (2021). Cyber Power between Fiction and Reality. *The Defence Horizon*. Retirado de https://www.thedefencehorizon.org/post/cyber-power-between-fiction-and-reality.

Shamiev, K. (2021). Understanding Senior Leadership Dynamics within the Russian Military. *Center for Strategic & International Studies*. Retirado de https://www.csis.org/analysis/understanding-senior-leadership-dynamics-within-russian-military.

Stuckenberg, D. J. (2018). *Re-orienting NATO Deterrence: The Reality of Strategic Gray Zone Threats*. Retirado de https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-16.pdf.

Thornton, R. (2015). The Changing Nature of Modern Warfare: Responding to Russian Information Warfare. *RUSI Journal* (pp. 40–48). doi:10.1080/03071847.2015.1079047.

Torossian, B., Fagliano, L., & Görder, T. (2020). Hybrid Conflict: Neither war, nor peace. *Strategic Monitor 2019-2020- The Hague Center for Strategic Studies* (pp. 1–39). Retirado de https://hcss.nl/pub/2019/strategic-monitor-2019-2020/hybrid-conflict/.

Treverton, G. F. (2021). An American View: Hybrid Threats and intelligence. M. Weissmann, N. Nilsson, B. Palmertz, & P. Thunholm (Eds.), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 36–45). Londres: Bloomsbury Publishing Plc.

União Europeia. (2016). *Comunicação Conjunta ao Parlamento Europeu e ao Conselho: Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

União Europeia. (2021). *Defense Industry and Space*. [Página *online*]. Retirado de https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_pt.

United Kingdom Government. (2017). *Multinational Capability Development Campaign*. [Página *online*]. Retirado de https://www.gov.uk/government/collections/multinational-capability-development-campaign-mcdc.

Vandiver, J. (2014). Allies must prepare for Russia “hibrid war". *Star and Stripes*. [Página *online*]. Retirado de https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464.

Weissmann, M., Nilsson, N., Palmertz, B., & Thunholm, P. (2021). *Hybrid Warfare*. Londres: Bloomsbury Publishing Plc.

Wirtz, J. J. (2015). Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. K. Geers (Ed.), *Cyber War in Perspective: Russian agression against Ukraine* (pp. 29–37). Tallinn: NATO CCD COE Publications.

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal* (pp. 73–87). Retirado de https://www.jstor.org/stable/26326441. https://doi.org/10.11610/connections.15.2.06.

Apêndice A – Corpo de Conceitos

Ator não estatal – No contexto das AH, constitui-se como uma entidade que participa nas Relações Internacionais e que exerce poder suficiente para interferir, influenciar e provocar mudanças, sem qualquer afiliação a instituições oficiais ou a um Estado (Giannopoulos et al., 2021, p. 22).

Coercion phase – Fase onde a atividade pode ser denominada guerra híbrida ou guerra híbrida, porquanto a atividade se torna detetável e atribuível. A atividade nesta fase representa o "hard end" do espectro de escalada das ameaças híbridas, pois faz uso de todos os domínios estratégicos e fontes de poder (Hybrid CoE & CCDCOE, 2019, p. 12).

Controlo-Reflexivo – Consiste em métodos sistemáticos de afetação das perceções do adversário, assim como as suas decisões, forçando-o a agir voluntariamente de uma forma que seria favorável aos interesses estratégicos da Rússia (Kasapoglu, 2015, p. 2)

***Cyber-persona* –** Uma Cyber-persona não consiste em pessoas ou organizações reais, mas sim numa representação de sua identidade virtual. Uma identidade virtual pode ser um endereço de e-mail, identificação de usuário ou uma conta de rede social (NATO, 2020, p. 3).

Cyberstalking – É um crime em que alguém assedia ou persegue uma vítima usando meios eletrônicos ou digitais, como redes sociais, e-mail, mensagens instantâneas (IM) ou mensagens "postadas" num grupo de discussão ou fórum. Os *cyberstalkers* aproveitam o anonimato proporcionado pela internet para perseguir ou assediar as suas vítimas, sem serem punidos ou mesmo detetados (Awati, 2022).

Desestabilization phase – Fase onde o ator espera prolongar, na forma de uma campanha (múltiplas operações), ou usar para uma operação e depois de-escalar e retornar à fase de *priming*. Nesta fase a atividade torna-se mais agressiva e envolve mais violência, fruto da necessidade do ator ou pelo surgimento da oportunidade, ou, devido à frustração do ator com a situação do seu *status quo*. Nesta fase, é mais provável que a atividade ultrapasse os limites do aceitável e inaceitável, bem como da ação legal e ilegal (Giannopoulos et al., 2021, p.40).

Gray zone – Espaço que no espectro de conflito se situa entre a Paz e a Guerra, onde as atividades podem ser difíceis de atribuir, atuando abaixo do limite que pode levar ao início de hostilidades abertas deter (Stuckenberg, 2018, pp. 16–6).

Instrumentos de poder – São elementos do ambiente MPECI (Militar, Político, Económico, Civil e Informacional). Quando esses elementos são "*Weaponized*", os instrumentos de poder podem-se tornar ferramentas de ataque.(MCDC, 2017, p. 32).

Não-Linear – Refere-se a efeitos imprevistos de ataques de GH que não são causalmente lineares, sendo o resultado de interações sinérgicas de ataques, em que o todo é maior que a soma de suas partes. Efeitos não lineares nem sempre podem ser previstos pelo atacante ou defensor (MCDC, 2017, p. 32).

Operações Ciber – Operação destinada a manter a liberdade de manobra no Ciberespaço / no domínio cibernético para cumprir objetivos operacionais, negar liberdade de ação a adversários e possibilitar outras atividades operacionais (European External Agency Service, 2018, p. 60).

Priming phase – Fase que procura, através das suas atividades, um efeito de longo prazo na atitude ou comportamento de um indivíduo, grupo ou organização. Pode ser vista como completamente legal, apenas criando uma ameaça potencial, ao testar as fronteiras entre aceitável e inaceitável, bem como legal e ilegal.(Hybrid CoE & CCDCOE, 2019, p. 11).

Revoluções "coloridas" – No espaço pós-soviético são entendidas como a Revolução Rosa na Geórgia (2003), a Revolução Laranja na Ucrânia (2004) e a Revolução Tulipa no Quirguistão (2005). A única característica que esses eventos compartilham é considerada a natureza não violenta da mudança de regime, resultante de protestos em massa (Nikitina, 2014, p. 87).

Whole-of-Government – Abordagem no qual as agências de serviço público trabalham além das suas fronteiras por forma a alcançar um objetivo partilhado através de uma resposta integrada a questões específicas (Australian Government, 2021).

Apêndice B – Ferramentas das AH e Domínios afetados

Quadro 7 - Ferramentas das AH e Domínios afetados

Ferramentas das AH	Domínios afetados
1. Operações físicas contra infraestruturas	Militar, Económico, Social, Infraestruturas, Informacional, Ciber, Espacial, Administração Pública (Adm. Púb.)
2. Criação e exploração da dependência de infraestruturas (incluindo dependência civil-militar)	Militar, Económico, Infraestruturas, Ciber, Espacial, Adm.Púb.
3. Criação e exploração de dependências económicas	Político, Económico, Diplomático, Adm.Púb.
4. Investimento estrangeiro direto	Político, Militar, Económico, Infraestruturas, Informacional, Ciber, Espacial, Adm.Púb., Informação, Legal
5. Espionagem industrial	Económico, Infraestruturas, Informacional, Ciber, Informações
6. Afetar a economia nacional do oponente	Político, Económico, Diplomático, Adm. Pub.
7. Fomento das dificuldades económicas	Político, Económico, Diplomático, Adm. Púb.
8. Ciber espionagem	Militar, Infraestruturas, Ciber, Espacial, Adm.Púb.
9. Operações Ciber	Militar, Infraestruturas, Ciber, Adm. Púb., Espacial, Social
10. Violação do espaço aéreo	Político, Militar, Social, Diplomático
11. Violação do espaço marítimo	Político, Militar, Social, Diplomático
12. Proliferação de armamento	Militar
13. Operações convencionais e não convencionais das FFAA	Militar
14. Organizações paramilitares (*proxies*)	Militar
15. Exercícios militares	Político, Militar, Social, Diplomático
16. Influência através de diásporas	Político, Social, Informacional, Diplomático, Cultural, Informações
17. Financiamento de grupos culturais e *think tanks*	Político, Social, Cultural, Diplomático
18. Exploração de clivagens socioculturais	Social, cultural
19. Promoção da agitação social	Político, Económico, Social, Infraestruturas
20. Manipulação de discursos sobre migração para polarizar sociedades e minar democracias liberais	Político, Social, Cultural, Legal
21. Exploração de vulnerabilidades na Adm. Púb. (incluindo gestão de emergências)	Político, Social, Adm. Púb.
22. Promoção e exploração da corrupção	Económico, Social, Legal, Adm.Púb.
23. Explorar limites, lacunas e incertezas na legislação	Militar, Económico, Social, Infraestruturas, Informacional, Ciber, Cultural, Legal, Informações, Diplomático, Político, Espacial, Adm.Pub.
24. Aproveitamento das regras legais, de processos, instituições e argumentos	Militar, Económico, Social, Infraestruturas, Informacional, Ciber, Espacial, Cultural, Adm. Púb., Legal, Informações, Diplomático, Político
25. Recolha de informações	Militar, Informações
26. Operações clandestinas	Militar, Informações
27. Infiltração	Militar, Informações
28. Sanções diplomáticas	Político, Económico, Diplomático
29. Boicotes	Político, Económico, Diplomático
30. Embaixadas	Político, Social, Informações, Diplomático
31. Criação de confusão e narrativas contraditórias	Social, Informacional, Diplomático
32. Migrações como moeda de troca nas relações internacionais	Político, Social, Diplomático
33. Desacreditar a liderança e/ou candidatos	Político, Social, Adm. Púb.
34. Apoio a atores políticos	Político, Adm. Púb., Social
35. Coação de políticos e/ou governos	Político, Adm. Púb., Legal
36. Aproveitamento da imigração para obter influência política	Político, Social
37. Controlo e interferência nos *media*	Social, Infraestruturas, Informacional, Cultural
38. Campanhas de desinformação e propaganda	Político, Social, Informacional, Ciber, Cultural, Adm. Pub.
39. Influência em currículos e Unidades Ensino	Social, Cultural
40. Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite)	Militar, Económico, Infraestruturas, Ciber, Espacial

Fonte: Adaptado de Giannopoulos et al. (2021, pp. 33–35).

Apêndice C – Modelo de Análise

Quadro 8 - Modelo de análise

<table>
<tr><td>Objetivo Geral (OG)</td><td colspan="5">Propor um modelo da utilização do ciberespaço por parte da Rússia como AH.</td></tr>
<tr><td>Questão Central (QC)</td><td colspan="5">Qual o possível modelo de utilização do ciberespaço por parte Rússia como AH?</td></tr>
<tr><th>Objetivos Específicos</th><th>Questões Derivadas</th><th>Conceitos</th><th>Dimensões</th><th>Variáveis</th><th>Indicadores</th></tr>
<tr><td rowspan="2">OE 1: Investigar as ferramentas das Ameaças Híbridas possíveis de serem aplicadas no ciberespaço.</td><td rowspan="2">QD1: Quais as ferramentas das Ameaças Híbridas que se adequam à utilização no ciberespaço?</td><td>AH e Ciberespaço</td><td>Ferramentas das AH</td><td>Ferramentas iniciadas ou exponenciadas no ciberespaço</td><td>Ações-Efeitos</td></tr>
<tr><td colspan="4">Técnicas de recolha de dados:
Pesquisa documental
Entrevistas semiestruturadas</td></tr>
<tr><td rowspan="3">OE 2: Analisar o uso das ferramentas das AH no ciberespaço, por parte da Rússia, em situações de Conflito.</td><td rowspan="3">QD 2: De que forma foram aplicadas as ferramentas das AH no ciberespaço, nos conflitos perpetrados pela Rússia?</td><td rowspan="2">AH e Ciberespaço</td><td rowspan="2">Ferramentas das AH no ciberespaço</td><td>Conflito Rússia-Geórgia</td><td>Ações-Efeitos</td></tr>
<tr><td>Conflito Rússia-Ucrânia</td><td>Ações-Efeitos</td></tr>
<tr><td colspan="4">Técnicas de recolha de dados:
Pesquisa documental
Entrevistas semiestruturadas</td></tr>
<tr><td rowspan="3">OE 3: Analisar a integração da doutrina russa no modelo conceptual das AH.</td><td rowspan="3">QD 3: Como se integra a doutrina russa no modelo conceptual das AH?</td><td>AH</td><td>Espectro de Atuação</td><td>Fases:
- Preparação
- Desestabilização
- Coação</td><td rowspan="2">Atividades</td></tr>
<tr><td>Doutrina Russa</td><td>“Doutrina Gerasimov”
Guerra não-Linear</td><td>Fases (8 fases)</td></tr>
<tr><td colspan="4">Técnicas de recolha de dados:
Pesquisa documental
Entrevistas semiestruturadas</td></tr>
</table>

Apêndice D – Lista de Indicadores

Quadro 9 - Lista de Indicadores

Tool	Uso do ciberespaço (OE1)	Uso na Geórgia (Ciberespaço) (OE2)	Uso na Ucrânia 2013/2014 (Ciberespaço) (OE2)
1	"Cyber Ops target computers systems to disrupt, deny, degrade, destroy information…or the computers and network themselves (Abaimov & Martellini, 2017, p. 88)" ; "According to press reports, the United States was behind the Stuxnet malware attack on centrifuges at Iran's Natanz enrichment facility (Wirtz, 2015, p.29)		
2	"The use of cyber assets has been a form of force projection that helps initiate crises far ahead…that affect energy infrastructure, (Danyk et al., 2017, p.15)" ; "The most prominent example of this tool is energy dependency" (Giannopoulos et al., 2019, p.73).		
4	"In particular, energy infrastructure and EU energy supply related to Russia as well as the AS (Autonomous Systems) ownership scheme that constitutes the backbone of the internet need to be thoroughly addressed (Giannopoulos et al., 2019, p. 75)"		"The Crimean case and the way the unique internet exchange point was compromised demonstrates that controlling access to the internet for specific geographical areas is feasible (Giannopoulos et al., 2019, p. 75)"
5	"cyber operations may be a method of acquiring foreign intelligence unrelated to specific military objectives, such as understanding technological developments or gaining information about an adversary's military capabilities (Abaimov & Martellini, 2017, p. 88)"		
6	"a major cyber-attack on a cloud services provider such as Amazon could trigger economic losses" (Abaimov & Martellini, 2017, p. 127) ; "Cyber weapons…still cause physical destruction not directly but as a follow-up impact…if cities are without electricity for a prolonged period, that could result in a greater number of deaths (Schröefl, 2020, p. 5)"	"Russian action against Georgia's paramount strategic installation, the Baku-Ceyhan oil pipeline...Indeed the cyber-attack fit into an overall Russian strategy centered on Georgia's oil infrastructure (Hollis, 2011, p. 4)"	"There are also many attacks on Ukrainian businesses: examples include the Ukrainian Railway Company, Kievstar mobile operator, a SMART-TV retail shop, and a city billboard (Pakharenko, 2015, p. 63)"
8	"malware-based cyber espionage network GhostNet of over 1,295 infected computers collecting intelligence on 103 countries (Abaimov & Martellini, 2017, p. 122)" ; "Private sector reports that cyber espionage tools have been discovered in Ukraine and in NATO countries. Malware analysis suggests that the campaigns are based in Russia (Geers, 2015, p. 11).	"the (alleged) Russian attackers conducted a dress rehearsal for their synchronized cyberattack early in July 2008. These extensive preparatory actions imply a strategic planning process that began long before July 2008 (Hollis, 2011, p. 4)"	"About the War in Ukraine…There has been vigorous Cyber espionage (Libicki, 2015, p. 50)" ; "Beyond disabling the site and successfully displaying incorrect election results, CERT-UA discovered advanced cyber espionage malware on the CEC network (Sofacy/APT28/Sednit) (Koval, 2015, p. 57)"
9	"Israel forces against Syria reactor…Accompanied with the strike was a cyberattack on Syria's air defences, which left them unaware of the attack on the nuclear reactor […] In 2007, a large-scale denial of service attack was launched in Estonia against…banking services, and e-commerce (Abaimov & Martellini, 2017, p. 118)"	"In 2008 combined cyber and kinetic attacks against Georgia due to the "real-life" implications of having communications disrupted during Kinetic combats (Abaimov & Martellini, 2017, p. 84)"	"On 02 of December of 2013, pro-Ukrainian websites were targeted by DDoS attacks, the majority of which came from commercial botnets employing Black- Energy and Dirt Jumper malware (Pakharenko, 2015, p. 61)"
13	"US Air Force has had Information Warfare Squadrons since the 1980 ...It was aimed at weapons systems used by Iran's Islamic Revolutionary Guard Corps, (Abaimov & Martellini, 2017, p. 89)"	"Many of the most serious attacks began just as the tanks began to roll...Official sites in Gori, were shut down by DDoS attacks before the Russian planes got there (Hollis, 2011, p.5)" ; "In Georgia cyber attacks were closely coordinated with Russian military operations (Lewis, 2015, p.45)"	
14	"the way proxies are instrumental for the Hybrid Threats relating activity and especially when it comes to online…activity, blurs the picture even further	"to employ their people's patriotic 'hacker militia' to conduct a network attack against a nation-state,	

	and shows how the "battle" can be over before crosses a threshold for war (Giannopoulos et al., 2021, p.42)"; "reports describe a 'troll factory' in St. Petersburg, Russia, where hundreds of people are allegedly creating pro-Russian government content for both domestic and international social media (Geers, 2015, p. 11)"	they must…synchronize those cyberspace operations with combat activity in the physical realm […] It seems that web sites in Georgia were attacked by rogue elements within Russia (Hollis, 2011, pp. 2 e 5)"	
15	"The planned attacks need to be practiced at a low level to assess their effectiveness. In future cyber combat, nations will need to conduct these preparatory operations, reconnaissance activities, and probing attacks well in advance of any network attack conducted in support of traditional military operation […] Cyberspace warfare capabilities are represented by trained human capital…tested, and refined in strenuous cyberspace combat exercises (Hollis, 2011, pp. 6 e 8)"	"the (alleged) Russian attackers conducted a dress rehearsal for their synchronized cyberattack early in July 2008, preparatory actions imply a strategic planning process that began long before July 2008 (Hollis, 2011, p. 4): Small-scale DDoS attacks began in June, before the war between Russia and Georgia" (Abaimov & Martellini, 2017, p.120).	
16	"Diasporas may be considered hybrid threats when their actions are covertly manipulated by the government of the host country in order to influence the behavior of the homeland or, conversely, when a homeland government may exploit diaspora sentiments for its purposes" (Giannopoulos et al., 2019, p.83).		"the actions of national media outlets, organized by the Russian Federation, aggravated an already complex situation by appeals to encourage simple narratives" (Danyk et al., 2017, p.15) ; "Ukrainian media became inaccessible in Crimea, result of Kremlin propagating their version of facts" (Bērziņš, 2014, p.7)
18	"Sociocultural cleavages provide fertile ground for a hybrid adversary to exploit with a view to creating social tension, polarizing society, instilling fear in the population or undermining their trust in the government. Disinformation campaigns often target contentious issues. Those issues having the potential to create or sustain a crisis are particularly attractive" (Giannopoulos et al., 2019, p. 85).		"information campaign fostered sociopolitical destabilization in the country and continues to negatively affect[…]is expected to encourage the widening range of negative information streams in order to aggravate existing civil mistrust and anti-government behavior" (Danyk et al., 2017, pp. 10 e 14)
19	"the spread of false and malicious information encourages beliefs and behavior that would normally be kept in check by existing social mores and civic expectations[…] sock-puppeting (government agents playing the role of online commentators (Danyk et al., 2017, pp. 13-14)		"Ukrainian officials report a sophisticated attack against the Central Election Commission on May 2014…computer virus is launched to undermine the credibility of the elections and presents false election results" (Geers, 2015, p.11) ; "Information Warfare encouraging an increase in crime and separatism activities" (Danyk et al., 2017, p. 10).
21	"hybrid threats affect the entire society. Therefore, defending against them requires a whole-of- government approach…such capabilities include cyber security analysis" (Giannopoulos et al., 2019, p.87) ; "Russian movement into the Ukraine was accompanied by myriad cyber-attacks, against computers in Poland, the European Parliament, and the European Commission" (Wirtz, 2015, p. 35).	"Georgian citizens could not access web sites for information and instructions. Georgian authorities discovered their Internet access and communications networks to be exceptional vulnerable to (alleged) Russian interference." (Hollis, 2011, p. 2).	" annexation of Crimea began with a disinformation campaign to create ambiguity and delay Ukraine's response" (Wirtz, 2015, p.35) ; "…coincided with the lethal shooting of protestors in Maidan (Feb, 2014), the mobile phones of opposition parliament members were flooded…in an effort to prevent them from communicating and coordinating defences" (Pakharenko, 2015, p.61).
23	Cyber and telecommunications technologies may present challenges…uncertainty surrounds the question whether or not international law prohibits interference into the cyber domain and infrastructure of another nation where that interference does not amount to acts prohibited by the principle of non-intervention (Giannopoulos et al., 2019, p.91)	"(StopGeorgia.ru) this forum featured a updated list of target websites and encouraged visitors to download a free software program, allowed them to participate instantly in the attacks" (Abaimov & Martellini, 2017, p.121)	"Russia's activities in Ukraine have implications for cyber warfare and for cyber norms…have carved new contours for conflict that do not map perfectly to existing concepts and rules for warfare and defence." (Lewis, 2015,p.42)

24	"domestic regulations regarding intellectual property, the media, technology may be utilized in support of hybrid activity. Russia increased the source code reviews – overseen by the Russian Security Service to approve foreign technology being sold in the country" (Giannopoulos et al., 2019, p. 91)		
25	"The intensity of intelligence collection will likely vary and range from passive OSINT approaches to intensive CYBINT operations[…]in April 2017 the Danish Defence Minister said that ATP or Fancy Bear, a group that gained illegal access to email accounts of U.S Democratic Party campaign in 2016, had also hacked the emails of selected Danish defence staff for two years" (Giannopoulos et al., 2019, p.93)	"These attacks included various DDOS attacks to deny/disrupt communications and information exfiltration activities conducted to accumulate military and political intelligence from Georgian networks."(Hollis, 2011, p.3)	"based on our analysis of IP activity, the attackers began their reconnaissance in mid-March 2014 – more than two months prior to the election[…]Ukrainian mobile operators saw an increase in the volume of cyber crime emanating from Crimea, and it is likely that Russian security services acquired intelligence from information collected in this way" (Pakharenko, 2015, p. 57 e 62)
31	"hybrid adversary may employ conflicting narratives to create confusion and undermine decision-making processes in the target state" (Giannopoulos et al., 2019, p. 97) ; "Even if information does not create a conscious change in beliefs, it can impact the interpretation of future information by providing effective anchoring and priming media" (Danyk et al., 2017, p.13)	"Russian Hacker Foruns, effectively disrupted the dissemination of information by the Georgian government at a crucial stage in the conflict" (Abaimov & Martellini, 2017, p.122); "Cyberspace domain operations conducted by the Russian cyber militia supported that effort by denying and degrading the Georgian government's ability to communicate, both internally and with the outside world (Hollis, 2011, p. 5)	"On 21 May 2014, CyberBerkut compromised the Central Election Commission, the attackers posted on the CEC website a picture of Ukrainian Right Sector leader Dmitry Yarosh, incorrectly claiming that he had won the election (Pakharenko, 2015, p.56) ; "a bugged phone call between the Estonian Ministry and the EU, fuels conspiracy theories and appears to support the Russian narrative regarding sniper shootings at Euromaidan" (Geers, 2015, p.11)
33	"using controlled fake social media accounts to sow discord and oppose the Clinton campaign, and by leaking stolen emails from the Clinton campaign through WikiLeaks…one release was timed to immediately follow the release of a video considered damaging to candidate Trump" (Giannopoulos et al., 2019, p.98)	"Russian hacktivists shutting down and defacing the websites of the President, the Georgian Parliament, the Ministries of Defense and Foreign Affairs, the National Bank of Georgia" (Abaimov & Martellini, 2017, p.120)	"The goal was to establish a general loss of civic confidence in the government of Ukraine by launching an information warfare campaign aimed at discrediting government authorities" (Danyk et al., 2017, p.10) ; "the publication of allegedly leaked Ukrainian government documents detailing a secret, fascist government agenda"(Pakharenko, 2015, p.56)
37	"The hybrid adversary seeks to support their disinformation campaign and limit the access to information…they will attempt to gain control of media outlets in the target state and develop a considerable presence on social media" (Giannopoulos et al., 2019, p.100) ; "reports describe a 'troll factory' in St. Petersburg, Russia, where hundreds of people are allegedly creating pro-Russian government content for both domestic and international social media" (Geers, 2015, p.11)	"Russian hacktivists shutting down and defacing two online news agencies" (Abaimov & Martellini, 2017, p.120) ; "Russian-oriented hackers/militia took out news web sites specifically in the areas that the Russian military intended to attack in the ground and air domains" (Hollis, 2011, p.6)	"Russia started internet/media propaganda to undermine resistance, thus avoiding the use of firepower[…]Crimean parliament officially asked to join the Russian Federation, and the Ukrainian media became inaccessible in Crimea" (Bērziņš, 2014, pp. 4 e 7); "Today in Crimea, Russian authorities have implemented content filtering for internet access, including the censorship of Ukrainian news sites"(Pakharenko, 2015, p.62)
38	"disinformation campaigns can use a wide range of channels and technologies to disseminate their messages. Social networks, blogs, and other digital media can be used to extend the reach of the hybrid adversary's domestic media outlets and disseminate information via state-sponsored user accounts, bots or advertisements". (Giannopoulos et al., 2019, p.101)	"These attacks also included web site defacement for Russian propaganda purposes" (Hollis, 2011, p. 3)	"Pro-Russia media, discussion forums, and social network groups were active in propaganda dissemination. The Crimea campaign was even buttressed by mass changes in Wikipedia, where Russian propaganda teams altered articles related to the events taking place" (Pakharenko, 2015, p. 62)
40	"Electromagnetic pulse (EMP) and cyberattack..operating in tandem, can disable not just a significant portion of the the electrical grid and critical infrastructure, but also the network- centric military response to such an attack (Abaimov & Martellini, 2017, p. 93)		On November 30 (2013), mobile phone communications were systematically shut down through mobile operators, and armed police units physically attacked the protesters.(Pakharenko, 2015, p. 60)

Apêndice E – Lista de Entrevistados

Quadro 10 - Lista de entrevistados

Posto/Título e Nome	Cargo/Função/Experiência	Código
Contra-Almirante António Gameiro Marques	Diretor-Geral do Gabinete Nacional de Segurança	E2
Dr. Josef Shröefl	Subdiretor da Comunidade de Interesse Estratégico e de Defesa do Centro de Excelência Europeu para o Combate às Ameaças Híbridas (*Hybrid CoE*). Autor de vários livros e artigos sobre a temática das Ameaças Híbridas e Domínio Ciber.	E6
Coronel Tirocinado António José Ruivo Grilo	Coordenador da Área de Ensino do Estudo das Crises e dos Conflitos Armados (IUM): Autor do TII do Curso de Promoção a Oficial General 2020/2021 *A Defesa Nacional na prevenção e no combate de ameaças híbridas.*	E8
Professor Miguel Pupo Correia	Professor Catedrático no Instituto Superior Técnico de Lisboa, Investigador em Cibersegurança, Coordenador do Programa de Doutoramento em Segurança de Informação.	E5
Coronel Óscar Manuel do Nascimento Rocha	Ex-Assessor no Gabinete da Secretaria-Geral do Sistema de Segurança Interna	E1
Tenente-Coronel Hugo Miguel Moutinho Fernandes	2º Comandante do Regimento de Comandos, tendo desempenhado o cargo de Chefe da Repartição de Lições Aprendidas da Divisão de Doutrina, Normalização e Lições Aprendidas do Estado-Maior do Exército. Autor do artigo *As novas guerras: o desafio da guerra híbrida*.	E3
Tenente-Coronel David Lopes Antunes	*Cyber Defence Programe Manager na European Defence Agency* (EDA)	E4
Tenente-Coronel José Carlos Reimão Teixeira	Chefe do Centro de Ciberdefesa do Estado-Maior-General das Forças Armadas. Funções anteriores: Representante Nacional no NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) e Chefe da Repartição de Guerra de Informação da Direção de Comunicações e Sistemas de Informação (Exército Português)	E7
Tenente-Coronel Jorge Miguel da Encarnação Vinagreiro	Chefe do Centro de Operações do Ciberespaço no Centro de CiberDefesa do Estado-Maior-General das Forças Armadas	E9
Capitão-de-Fragata Sérgio Ricardo Caldeira de Carvalho	Oficial de Operações do Centro de Ciberdefesa do Estado-Maior-General das Forças Armadas	E10

Apêndice F – Guião das Entrevistas Semiestruturadas

Cabeçalho

Excelentíssimo(a) Senhor(a),

Chamo-me Daniel Carvalho Gomes, sou Major de Infantaria do Exército Português, e encontro-me a frequentar o Curso de Estado-Maior Conjunto 2021/2022, que decorre no Instituto Universitário Militar.

Durante este curso os auditores elaboram Trabalhos de Investigação Individual (TII), nos quais se abordam questões relevantes e importantes para a compreensão da conflitualidade atual, e consequentemente, para o futuro das Forças Armadas Portuguesas. Neste âmbito, encontro-me a realizar um TII, intitulado "Ameaças Híbridas: a doutrina Russa e a sua aplicação prática".

O objetivo geral deste TII consiste em propor um modelo da utilização do ciberespaço por parte da Rússia, como ameaça híbrida (AH), estando delimitado, temporalmente de 2008 a 2014, espacialmente à Geórgia e à Ucrânia, e ao nível do conteúdo, às ferramentas das AH e o seu uso no ciberespaço.

A investigação compreende três áreas principais: (i) Investigar as ferramentas das AH possíveis de serem aplicadas no ciberespaço, (ii) analisar o uso do ciberespaço por parte da Rússia em situações de conflito, estando esta área dividida nos conflitos da Geórgia e da Ucrânia, (iii) e analisar a integração da doutrina russa no modelo conceptual das AH.

Solicito a sua autorização para gravar a presente entrevista e para referir no trabalho o conteúdo da mesma associado ao seu nome. Caso seja a sua intenção, garanto a sua confidencialidade e tratarei a informação recolhida de forma anónima. Estimo que a entrevista dure um máximo de 30 minutos.

O seu conhecimento e experiência são essenciais para a qualidade e relevância deste trabalho, pelo que, agradeço a sua disponibilidade para a prossecução da presente investigação.

Caraterização do entrevistado

Nome do Entrevistado:
Posto:
Cargo/Função:
Data da entrevista:
Local:
Hora de início:
Hora de fim:

Questões

Síntese introdutória (pergunta 1)

Segundo o *Hybrid CoE* (2021), AH definem-se: como as ações conduzidas por atores estado e não-estado, cujo objetivo é afetar ou prejudicar um alvo, quer seja este local, regional ou estatal, no seu processo de decisão, e que, estas ações são coordenadas e sincronizadas, visando deliberadamente as vulnerabilidades dos estados democráticos e suas instituições, ao serem aplicadas nos domínios político, económico, militar, civil e informacional, mantendo-se, no que respeita ao espetro do conflito, abaixo dos limites da deteção.

Segundo *Schröefl* (2021), ciberespaço é um domínio que compreende a sua atuação entre a componente física dos equipamentos e a componente imaterial dos conteúdos, numa simbiose alavancada pela conectividade global, e que, no âmbito das AH, além de um domínio, pode constituir-se como um potenciador das ações híbridas. No quadro 1, apresenta-se o conjunto de ferramentas das AH e os domínios que estas afetam no adversário, segundo o modelo conceptual da publicação: *The Landscape of Hybrid Threats- A conceptual Model* (Giannopoulos et al., 2021), com as ferramentas que afetam o domínio Ciber (assinaladas a cinzento), correlacionando que são usadas no domínio do Ciberespaço.

Quadro 11 - Ferramentas das AH e Domínios afetados

Ferramentas das AH	Domínio afetados
1. Operações físicas contra infraestruturas	Militar, Económico, Social, Infraestruturas, Informacional, **Ciber**
2. Criação e exploração da dependência de infraestruturas (incluindo dependência civil-militar)	Militar, Económico, Infraestruturas, **Ciber**
3. Criação e exploração de dependências económicas	Político, Económico
4. Investimento estrangeiro direto	Político, Militar, Económico, Infraestruturas, Informacional, **Ciber**
5. Espionagem industrial	Económico, Infraestruturas, Informacional, **Ciber**
6. Afetar a economia nacional do oponente	Político, Económico
7. Fomento das dificuldades económicas	Político, Económico
8. Cyber espionagem	Militar, Infraestruturas, **Ciber**
9. Operações Cyber	Militar, Infraestruturas, **Ciber**

10. Violação do espaço aéreo	Político, Militar, Social
11. Violação do espaço marítimo	Político, Militar, Social
12. Proliferação de armamento	Militar
13. Operações convencionais e não convencionais das FFAA	Militar
14. Organizações paramilitares (proxies)	Militar
15. Exercícios militares	Político, Militar, Social
16. Influência através de diásporas	Político, Social, Informacional
17. Financiamento de grupos culturais e *think tanks*	Político, Social
18. Exploração de clivagens socioculturais (étnicas, religiosas e culturais)	Social
19. Promoção da agitação social	Político, Económico, Social, Infraestruturas
20. Manipulação de discursos sobre migração para polarizar sociedades e minar democracias liberais	Político, Social
21. Exploração de vulnerabilidades na administração pública (incluindo gestão de emergências)	Político, Social
22. Promoção e exploração da corrupção	Económico, Social
23. Explorar limites, lacunas e incertezas na legislação	Militar, Económico, Social, Infraestruturas, Informacional, **Ciber**
24. Aproveitamento das regras legais, de processos, instituições e argumentos	Militar, Económico, Social, Infraestruturas, Informacional, **Ciber**
25. Recolha de informações	Militar, Informações
26. Operações clandestinas	Militar, Informações
27. Infiltração	Militar, Informações
28. Sanções diplomáticas	Político, Económico
29. Boicotes	Político, Económico
30. Embaixadas	Político, Social, Informacional
31. Criação de confusão e narrativas contraditórias	Político, Social, Informacional
32. Migrações como moeda de troca nas relações internacionais	Político, Social
33. Desacreditar a liderança e/ou candidatos	Político, Social
34. Apoio a atores políticos	Político, Social
35. Coação de políticos e/ou governos	Político
36. Aproveitamento da imigração para obter influência política	Político, Social
37. Controlo e interferência nos *media*	Social, Infraestruturas, Informacional
38. Campanhas de desinformação e propaganda	Político, Social, Infraestruturas, Informacional, **Ciber**
39. Influência em currículos e estabelecimentos de ensino	Social, Cultural
40. Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite).	Militar, Económico, Infraestruturas, **Ciber**

Fonte: Adaptado de Giannopoulos et al. (2021, pp. 33–35).

Atendendo que, as ferramentas de AH são um conceito permeável e dinâmico face às alterações do ambiente, e que podem ser iniciadas ou estimuladas por ações no ciberespaço (Danyk et al., 2017), foram identificados indicadores que permitem associar este domínio espacial a outras ferramentas das AH (assinaladas a laranja).

1.1: Na sua visão, concorda que as ferramentas das AH assinaladas possam ser consideradas passíveis de serem aplicadas ou exponenciadas no ciberespaço?
1.2: Das Ferramentas assinaladas qual/quais não concorda que façam parte desta análise e porquê?
1.3 Entende que haja alguma ferramenta não assinalada que possa ser iniciada ou estimulada pelo uso do ciberespaço? Qual/quais e porquê?

Síntese introdutória (pergunta 2)

Após uma análise bibliográfica, referente ao conflito Russo-Georgiano de 2008, identificaram-se indicadores que relacionam os efeitos e ações de Ferramentas das AH na preparação/desenvolvimento do conflito, por parte da Rússia, conforme quadro 2.

Quadro 12 - Ferramentas das AH aplicadas na Geórgia pelo uso do ciberespaço

6. Afetar a economia nacional do oponente
8. Cyber espionagem
9. Operações Cyber
13. Operações convencionais e não convencionais das FFAA
14. Organizações paramilitares (proxies)
15. Exercícios militares
21. Exploração de vulnerabilidades na administração pública (incluindo gestão de emergências)
23. Explorar limites, lacunas e incertezas na legislação
25. Recolha de informações
31. Criação de confusão e narrativas contraditórias
33. Desacreditar a liderança e/ou candidatos
37. Controlo e interferência nos *media*
38. Campanhas de desinformação e propaganda

Fonte: Adaptado de Giannopoulos et al. (2021, pp. 33–35).

2.1: Concorda que, no conflito Rússia-Geórgia, em 2008, as ferramentas de AH assinaladas foram iniciadas e/ou estimuladas no ciberespaço por parte da Rússia?
2.2: Das Ferramentas assinaladas, qual/quais não concorda que façam parte desta análise e porquê?
2.3: Entende que haja alguma ferramenta, que não tenha sido assinalada, e que possa ter sido iniciada ou estimulada pelo uso do ciberespaço? Qual/quais e porquê?

Síntese introdutória (pergunta 3)

Após uma análise bibliográfica, referente ao conflito Russo-Ucraniano de 2013/2014, identificaram-se indicadores que relacionam os efeitos e ações de Ferramentas das AH na preparação/desenvolvimento do conflito, por parte da Rússia, conforme quadro 3.

Quadro 13 - Ferramentas das AH aplicadas na Ucrânia pelo uso do ciberespaço

4. Investimento estrangeiro direto
6. Afetar a economia nacional do oponente
8. Cyber espionagem
9. Operações Cyber
16. Influência através de diásporas
18. Exploração de clivagens socioculturais (étnicas, religiosas e culturais)
19. Promoção da agitação social
21. Exploração de vulnerabilidades na administração pública (incluindo gestão de emergências)
23. Explorar limites, lacunas e incertezas na legislação
25. Recolha de informações
31. Criação de confusão e narrativas contraditórias
33. Desacreditar a liderança e/ou candidatos
37. Controlo e interferência nos *media*
38. Campanhas de desinformação e propaganda
40. Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite).

Fonte: Adaptado de Giannopoulos et al. (2021, pp. 33–35).

3.1: Concorda que, no conflito Rússia-Ucrânia, em 2014, as ferramentas de AH assinaladas, foram iniciadas e/ou estimuladas no ciberespaço por parte da Rússia?
3.2: Das Ferramentas assinaladas, qual/quais não concorda que façam parte desta análise e porquê?
3.3: Entende que haja alguma ferramenta, que não tenha sido assinalada, e que possa ter sido iniciada ou estimulada pelo uso do ciberespaço? Qual/quais e porquê?

Síntese introdutória (pergunta 4)

De acordo com Giannopoulos et al. (2021) as AH atuam, prioritariamente, na sombra ou na **zona cinzenta** entre o aceitável e inaceitável, o legal e ilegal, com uma combinação de ferramentas para reforçar o seu esforço. As três fases referidas são o ***Priming*** (Preparação), a ***Destabilisation*** (Desestabilização) e a ***Coercion*** (coação), não existindo uma separação definida, coexistindo entre as fases, zonas de convergência.

Atendendo à teorização de Berzins (2014) sobre a Guerra não-Linear, imputada à retórica do General *Gerasimov,* e a conceptualização de um modelo doutrinário apresentado nesse documento, citando a visão de Chekinov e Bogdanov (2013), apresentam-se de seguida, um conjunto de atividades integrados nas respectivas fases, sob os quais, os russos desenvolvem a sua atividade no domínio operacional:

Fase I- conflito assimétrico não militar (abrangendo informação, medidas morais, psicológicas, ideológicas, diplomáticas e económicas como parte de um plano para estabelecer uma favorável configuração política, económica e militar).

Fase II- operações especiais para ludibriar os líderes políticos e militares através de medidas coordenadas, levadas a cabo por canais diplomáticos, meios de comunicação, e agentes governamentais e militares, através da fuga de dados falsos, ordens, diretivas e instruções.

Fase III- intimidação, engano e suborno de oficiais governamentais e militares, com o objetivo de os fazer abandonar os seus deveres de serviço.

Fase IV- propaganda desestabilizadora para aumentar o descontentamento entre a população, impulsionada pela chegada de bandos de militantes russos, escalando a subversão.

Fase V- estabelecimento de zonas de exclusão aérea sobre o país a ser atacado, imposição de bloqueios, e utilização extensiva de empresas militares privadas em estreita cooperação com unidades convencionais.

Fase VI- início da Acão militar, imediatamente precedida de missões de reconhecimento e subversivas em grande escala. Todos os tipos, formas, métodos e forças, incluindo forças de operações especiais, espaço, rádio, engenharia de rádio, inteligência eletrónica, diplomática e de serviços secretos, e espionagem industrial.

Fase VII- combinação de operação de informação direcionada, operação de guerra eletrónica, operação aeroespacial, assédio contínuo à força aérea, combinado com o uso de armas de alta precisão lançadas a partir de várias plataformas (artilharia de longo alcance, e armas baseadas em novos princípios físicos, incluindo micro-ondas, radiação, armas biológicas não letais).

Fase VIII- Conquistar os restantes pontos de resistência e destruir unidades inimigas sobreviventes através de operações especiais conduzidas por unidades de reconhecimento para detetar quais as unidades inimigas sobreviventes e transmitir as suas coordenadas às unidades de mísseis e artilharia do atacante; barragens de fogo para aniquilar as unidades do exército resistente (do defensor) através de armas avançadas eficazes; operações aerotransportadas para cercar pontos de resistência; e operações de conquista de território por tropas terrestres.

Pergunta 4. Considerando as principais atividades da "doutrina *Gerasimov"*, na sua opinião, como as integraria nas três fases principais do modelo conceptual das AH?

4.1 Preparação	
4.2 Desestabilização	
4.3 Coação	

Nota: Atendendo às zonas de convergência entre as Fases das AH, pode existir a necessidade de associar um conjunto de tarefas a mais do que uma Fase.

Agradecimento

Agradeço mais uma vez a sua disponibilidade e contributos para a prossecução da presente investigação. Muito obrigado.

Apêndice G – Análise de Conteúdo das Entrevistas Semiestruturadas

Quadro 14 - Matriz das unidades de contexto e de registo da primeira questão

Entrevistado	Unidade de Contexto	Unidade de Registo
E1	- "Concordo na generalidade, algumas das ferramentas assinaladas não parecem ser passíveis de ser aplicadas ou exponenciadas no ciberespaço" - "Pois é muito difícil a aplicação no ciberespaço, porquanto assumem uma dimensão muito física, e a sua exponenciação através de ações realizadas no ciberespaço considero que terão um efeito marginal"	1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23; 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.2.1; 1.2.15;
E2	- "Concordo na sua globalidade" - "Tenho alguma reserva na possibilidade da ferramenta 4 ser aplicada no ciberespaço" - "Ferramenta 20…em conjugação com as Operações de Informação, através de três fatores: pela velocidade de dispersão da informação, pelo alcance proporcionado nos meios digitais, e, pela inexistência de supervisão/controlo editorial"; "Ferramenta 22, pois há um subproduto digital (cripto-moedas) que pode promover os pagamentos, de forma indetetável (*untraceable*), para ações clandestinas e criminosas…ferramenta 35, pois em 2014, o governo eleito em Kiev ficou coagido na sua ação política, através das narrativas Russas, e, em contraponto a ferramenta 34"	1.1.1; 1.1.2; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23; 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.2.4 1.3.20; 1.3.22; 1.3.34; 1.3.35
E3	- "Concordo que sejam passíveis de ser aplicadas no ciberespaço, podendo, contudo, atuar/influenciar outros domínios espaciais". - "Tenho alguma reserva na aplicação da Ferramenta 23, pois, considero que, é o efeito dessa ação que pode estar associado a essa premissa, e não a ação propriamente dita". - "Considero que a ferramenta 35 possa ser exponenciada no ciberespaço, direcionada para dificultar as decisões dos elementos afetados."	1.1.1; 1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.2.23; 1.3.35
E4	- "Concordo que as Ferramentas assinaladas possam ser aplicadas através do uso do Ciberespaço… realço que a ferramenta 6 pode ser considerada apenas nos casos em que o alvo sejam infraestruturas essenciais de um Estado (Ferroviárias, Energéticas)." - "Considero que deva ser considerada a ferramenta 35, num racional de "Cyber stalking", através da exposição mediática de informação pessoal por forma a influenciar a ação do alvo. (i.e.: caso *Dominique Strauss-Kahn*)"	1.1.1; 1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.3.35
E5	- "Concordo com a generalidade das ferramentas assinaladas" - "Tenho alguma reserva na aplicação da ferramenta 1, pois a sua matriz de atuação é bastante física, apesar das operações Ciber poderem contribuir, de forma sincronizada, para esse efeito." -"deve ser incluída nesta análise a ferramenta 7, estando associada aos efeitos provocados na ferramenta 6[…]a ferramenta 17, pelo financiamento através de cripto-moedas; a ferramenta 20 com o uso	1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.2.1

	predominante das redes sociais; e a ferramenta 34, conforme se verifica atualmente, com o apoio à narrativa do Presidente Ucraniano, através das plataformas multimédia e Redes Sociais"	1.3.7; 1.3.17; 1.3.20; 1.3.34
E6	- "Concordo com as ferramentas assinaladas" - "Na minha opinião devem ser incluídas as ferramentas 34 e 35, pois, sendo o ciberespaço um dos principais "enablers" das AH, e tendo em conta o domínio informacional, assiste-se a uma interferência nos atores políticos.	1.1.1; 1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.3.34; 1.3.35
E7	- "Concordo com as ferramentas analisadas" - "Ferramenta 10, numa lógica de deceção, através de ações no ciberespaço podem ser afetados os sistemas de Radar/Sensores, induzindo a existência de aeronaves fictícias, que, por sua vez obrigam os sistemas de defesa antiaérea a ativar os seus meios contra alvos inexistentes" - "Ferramenta 17, através de transações no ciberespaço (i.e. Bitcoins), incrementando a relação entre *Cyber personas* (*untreacable*); - "Ferramenta 26, pois alegadamente no Irão, foram introduzidos vírus *Stuxnet* (em *Pen drives*), que em ligação com os sistemas de controlo de reatores nucleares, provocaram a sua afetação"; - "Ferramenta 34, através de operações de Influência, com uso primordial nas redes sociais, e, Ferramenta 35, em efeito contrário, provoca pressão social no alvo, obrigando-o a abandonar o cargo"	1.1.1; 1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.3.10; 1.3.17; 1.3.26; 1.3.34; 1.3.35
E8	- "Concordo que as ferramentas assinaladas possam ser aplicadas através do ciberespaço" - "ferramenta 34 pelos casos visíveis de apoio a atores políticos (e.g. caso Francês), onde se assistiu uma campanha nas plataformas multimédia e redes sociais […] ferramenta 35…assistiu à influência e afetação de campanhas eleitorais através do ciberespaço, assim como a exposição de familiares de um ator político, afetando diretamente a sua ação e credibilidade (e.g. Caso norte-americano)"	1.1.1; 1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.3.34; 1.3.35
E9	- "Sim, sem dúvidas…a grande questão prende-se com a efetividade da aplicação destas ferramentas num determinado alvo através do ciberespaço… este só será efetivo se este alvo ou os atores sob os quais se pretende criar efeitos, possuem pegada ou presença significativa no ciberespaço" "-Não entendo que devam ser assinaladas outras"	1.1.1; 1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40
E10	- "Concordo com as ferramentas assinaladas" - "devem ser consideradas: a ferramentas 17; a ferramenta 20 (através de manipulação nas redes sociais; a ferramenta 22; a ferramenta 34 (pela manipulação verificada no caso do Brexit), ferramenta 35, ferramenta 36, e ferramenta 39 (sendo uma das preocupações atuais dos EUA no que respeita à propriedade intelectual).	1.1.1; 1.1.2; 1.1.4; 1.1.5; 1.1.6; 1.1.8; 1.1.9; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.18; 1.1.19; 1.1.21; 1.1.23 1.1.24; 1.1.25; 1.1.31; 1.1.33; 1.1.37; 1.1.38; 1.1.40 1.3.17; 1.3.20; 1.3.22; 1.3.34; 1.3.35; 1.3.36; 1.3.39

Quadro 15 - Análise de conteúdo da primeira questão

Categoria	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Ferramentas das AH aplicadas no ciberespaço	Após a análise dos indicadores	1.1.1 Operações físicas contra infraestruturas		x	x	x		x	x	x	x	x	8	80
		1.1.2 Criação e exploração da dependência de infraestruturas	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.4 Investimento estrangeiro direto	x		x	x	x	x	x	x	x	x	9	90
		1.1.5 Espionagem industrial	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.6 Afetar a economia nacional do oponente	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.8 Ciber-espionagem	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.9 Operações Ciber	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.13 Operações Convencionais e não convencionais da FFAA	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.14 Organizações paramilitares (*proxies*)	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.15 Exercícios militares		x	x	x	x	x	x	x	x	x	9	90
		1.1.16. Influência através de diásporas	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.18 Exploração de clivagens socioculturais	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.19 Promoção da agitação social	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.21 Exploração de vulnerabilidades na administração pública	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.23 Explorar limites, lacunas e incertezas na legislação	x	x		x	x	x	x	x	x	x	9	90
		1.1.24 Aproveitamento das regras legais, de processos, instituições e argumentos	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.25 Recolha de Informações	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.31 Criação de confusão e narrativas contraditórias	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.33 Desacreditar a liderança e/ou candidatos	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.37 Controlo e interferência nos media	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.38 Campanhas de desinformação e propaganda	x	x	x	x	x	x	x	x	x	x	10	100
		1.1.40 Operações eletrónicas	x	x	x	x	x	x	x	x	x	x	10	100
	Incluídas pelos entrevistados	1.3.7 Fomento das dificuldades económicas					x						1	10
		1.3.10 Violação do Espaço Aéreo							x				1	10
		1.3.17 Financiamento de grupos culturais e *think tanks*					x		x			x	3	30
		1.3.20 Manipulação de discursos sobre migração para polarizar sociedades e minar democracias liberais		x			x					x	3	30
		1.3.22 Promoção e exploração da corrupção		x								x	2	20
		1.3.26 Operações Clandestinas							x				1	10
		1.3.34 Apoio a atores políticos		x			x	x	x	x		x	6	**60**
		1.3.35 Coação de Políticos e/ou Governos		x	x	x		x	x	x		x	7	**70**
		1.3.36 Aproveitamento da imigração obter influência Política										x	1	10
		1.3.39Influência em currículos e estabelecimento de ensino										x	1	10

Quadro 16 - Matriz das unidades de contexto e de registo da segunda questão

Entrevistado	Unidade de Contexto	Unidade de Registo
E1	- "Sim, de uma forma mais visível, concordo com todas, o que não exclui a possibilidade de terem sido utilizadas outras ferramentas que não foram do conhecimento público" - "Considero que as ferramentas 26 e 27 poderão ter sido utilizadas ou potenciadas com ações realizadas no ciberespaço, uma vez que as operações clandestinas e a infiltração em sistemas de defesa, coordenação, comando e controlo, podem ter sido objeto de desenvolvimento, intrusão ou de denegação"	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.3.26; 2.3.27;
E2	- "Concordo com a utilização das ferramentas assinaladas através do ciberespaço" - "Ferramenta 16, pois considero que os Russos utilizaram ações de *InfoOps* para influenciar a diáspora russófona nesse território, por forma a permitir que estes percecionassem que a ação desenvolvida iria ser benéfica."	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.3.16
E3	- "Concordo, pois, de forma direta ou indiretamente, acabaram-se por constituir como Ameaças Híbridas". - "Tenho alguma reserva na aplicação da Ferramenta 23, pois, considero que, é o efeito dessa ação que pode estar associado a essa premissa, e não a ação propriamente dita". - "Considero que a Ferramenta 35 foi exponenciada pelo ciberespaço numa fase subsequente, por forma a coagir e a limitar a decisão"	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.2.23 2.3.35
E4	- "Concordo com a generalidade das ferramentas assinaladas." - "Considero que a Ferramenta 37 não foi utlizada, pois, o que se verificou foi a negação do acesso aos media, e não a interferência na sua atividade."	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.38 2.2.37
E5	- "Concordo com as ferramentas assinaladas." - "Entendo que deva ser incluída nesta análise a ferramenta 40, pelo uso associado às operações eletromagnéticas"	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.3.40
E6	- "Concordo que as ferramentas assinaladas foram utilizadas no conflito da Geórgia" - "Eu acrescentaria a ferramenta 34, pois a Rússia pretendeu influenciar os atores Políticos, querendo alguém diferente do Presidente *Mikkeil Saakashvili*; Na mesma medida, acrescentaria a ferramenta 35, com o mesmo princípio da ferramenta 34, verificando-se uma influência nos elementos governamentais, antes e logo após o conflito. Atualmente isso já não se verifica."	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.3.34; 2.3.35
E7	- "Concordo com as ferramentas assinaladas"	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38

	- "ferramenta 1, pelas evidências que a capacidade de distribuição elétrica foi afetada por ações no ciberespaço"; - "ferramenta 40 foi utilizada de forma indireta, com o uso de uma ação cyber (ferramenta 9) …os Oficiais de artilharia georgianos usavam uma aplicação de cálculo de tiro, disponível na internet, que ao ser afetada por ação ciber, provocou disrupção na eficácia de tiro das Forças de Georgianas"	2.3.1; 2.3.40
E8	- "No caso do conflito Russo-Georgiano, concordo com as ferramentas assinaladas" - "…deva ser acrescentado a esta análise a ferramenta 1, pois, através de ataques cibernéticos, assistiu-se à afetação de infraestruturas críticas de Comunicações e Comando e Controlo."	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.3.1
E9	- "Concordo com a generalidade… foi a primeira vez que o ciberespaço e as operações ofensivas foram utilizados em sincronismo com operações militares cinéticas. O objetivo era claramente diminuir a força do governo da Geórgia" - "nomeadamente a afetação da economia nacional…prende-se com o efeito que algumas ações conduzidas no ciberespaço realmente tiveram efeitos significativos"	2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.2.6
E10	- "Concordo com as ferramentas identificadas" - "ser consideradas: a ferramenta 16 (pela utilização da diáspora russa na luta contra o governo), a ferramenta 34 (utilizada desde 2008 até à atualidade), ferramenta 40 (os russos "apagaram" os sistemas de guiamento por satélite).	2.1.6; 2.1.8; 2.1.9; 2.1.13; 2.1.14; 2.1.15; 2.1.21; 2.1.23; 2.1.25; 2.1.31; 2.1.33; 2.1.37; 2.1.38 2.3.16; 2.3.34; 2.3.40

Quadro 17 - Análise de conteúdo da segunda questão

Categoria	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Ferramentas das AH aplicadas no ciberespaço no Conflito da Geórgia	Após a análise dos indicadores	2.1.6 Afetar a economia nacional do oponente	x	x	x	x	x	x	x	x		x	9	90
		2.1.8 Ciber-espionagem	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.9 Operações Ciber	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.13 Operações Convencionais e não convencionais das FFAA	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.14 Organizações paramilitares (*proxies*)	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.15 Exercícios militares	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.21 Exploração de vulnerabilidades na administração pública	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.23 Explorar limites, lacunas e incertezas na legislação	x	x		x	x	x	x	x	x	x	9	90
		2.1.25 Recolha de Informações	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.31 Criação de confusão e narrativas contraditórias	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.33 Desacreditar a liderança e/ou candidatos	x	x	x	x	x	x	x	x	x	x	10	100
		2.1.37 Controlo e interferência nos media	x	x	x		x	x	x	x	x	x	9	90
		2.1.38 Campanhas de desinformação e propaganda	x	x	x	x	x	x	x	x	x	x	10	100
		2.3.1 Operações Físicas contra Infraestruturas							x	x			2	20

	Incluídas pelos Entrevistados	2.3.16 Influência através da diáspora		x							x	2	20
		2.3.26 Operações clandestinas	x									1	10
		2.3.27 Infiltração	x									1	10
		2.3.34 Apoio a Atores Políticos						x			x	2	20
		2.3.35 Coação de Políticos e/ou Governos			x			x				2	20
		2.3.40 Operações eletrónicas					x		x		x	3	30

Quadro 18 - Matriz das unidades de contexto e de registo da terceira questão

Entrevistado	Unidade de Contexto	Unidade de Registo
E1	- "Penso que será de considerar todas as assinaladas, pois todas foram materializadas ou potenciadas através do ciberespaço" - "Considero as ferramentas 26 e 27, poderão ter sido potenciadas com ações no ciberespaço, uma vez que as operações clandestinas e a infiltração em sistemas de defesa, coordenação, comando e controlo, podem ter sido objeto de desenvolvimento, intrusão ou de denegação, aquando da intervenção das forças paramilitares nas províncias do *Donetsk* e *Lugasnk*".	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.26; 3.3.27;
E2	- "Sim, concordo com as ferramentas assinaladas". - "Ferramenta 34, pois, através da desacreditação dos oponentes políticos russos, inerentemente, está-se a dar força e apoio aos candidatos pró-russos. - "Ferramenta 35, pois, é evidente que, através desta ferramenta, o governo eleito em Kiev ficou coagido na sua ação política, através das narrativas Russas."	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.34; 3.3.35
E3	- "Concordo com a generalidade das ferramentas assinaladas" - "Tenho alguma Reserva na aplicação da Ferramenta 23 (Explorar limites, lacunas e incertezas na legislação), pois, considero que, é o efeito dessa ação que pode estar associado a essa premissa" - "Considero que a Ferramenta 35 foi exponenciada pelo ciberespaço na fase que antecedeu o conflito, por forma a coagir os Políticos pró-Ocidentais."	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.2.23 3.3.35
E4	- "Concordo com todas as ferramentas assinaladas." - "Entendo que a ferramenta 14 foi exponenciada pelo uso do ciberespaço, pois, foi nítida a utilização de *proxies* (grupos separatistas) e a forma como foram influenciados através do ciberespaço"	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.14
E5	- "Concordo com as ferramentas apresentadas na análise." - "Entendo que deva ser considerada a ferramenta 34, como efeito reverso da ferramenta 33 (desacreditar Liderança)."	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.34

E6	- "Concordo com as ferramentas assinaladas" - "Deve ser incluída a ferramenta 2, pela afetação do gasoduto que atravessa a Ucrânia, mesmo antes de 2014, sendo este um objetivo político russo" - "no meu ponto de vista, a ferramenta 22 pode ser considerada, pela ligação entre oligarcas russos e milionários ucranianos, podendo coexistir influência financeira, usando para isso o ciberespaço" - "Tal como na Geórgia, a ferramenta 34 e 35 foram utilizadas no conflito da Ucrânia através do Ciberespaço"	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.2; 3.3.15; 3.3.22; 3.3.34; 3.3.35
E7	- "Concordo com todas as ferramentas assinaladas" - "Considero que devam ser incrementadas: a ferramenta 34**,** pelo "empowerment" dado aos atores com ligações pró-russas, e, na mesma medida, a ferramenta 35, como forma de coagir os elementos com ligações ao ocidente"	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.34; 3.3.35
E8	- "Concordo com as ferramentas assinaladas" - "neste caso específico, assistiu-se à aplicação da ferramenta 1, pela afetação de infraestruturas e redes de comunicação, através de ações no ciberespaço […] e a aplicação da ferramenta 34, pelo apoio a atores pró-russos, que posteriormente, foram indicados para o governo"	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.1; 3.3.34
E9	- "Concordo na generalidade…É notório que quando comparamos os 2 conflitos, neste mais recente, as ferramentas utilizadas foram mais potenciadas pelo ciberespaço. - "Contudo continuo a ver as ferramentas 4 e 6 como pouco potenciadas pelo ciberespaço, apesar de alguns "danos colaterais" efetivamente terem efeitos nestas 2 ferramentas"	3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.2.4; 3.2.6
E10	- "Concordo com as ferramentas identificadas" - "ferramenta 5 (pela apropriação dos planos de construção das turbinas de navios), ferramenta 34 (pelo apoio dado aos políticos pró-russos) e ferramenta 36 (pela exploração desses focos de imigração para obter influência política).	3.1.4; 3.1.6; 3.1.8; 3.1.9; 3.1.16; 3.1.18; 3.1.19; 3.1.21; 3.1.23; 3.1.25; 3.1.31; 3.1.33; 3.1.37; 3.1.38; 3.1.40 3.3.5; 3.3.34; 3.3.36

Quadro 19 - Análise de conteúdo da terceira questão

Categoria	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Ferramentas das AH aplicadas no ciberespaço no Conflito da Ucrânia	Após a análise dos indicadores	3.1.4 Investimento estrangeiro direto	x	x	x	x	x	x	x	x		x	9	90
		3.1.6 Afetar a economia nacional do oponente	x	x	x	x	x	x	x	x		x	9	90
		3.1.8 Ciber-espionagem	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.9 Operações Ciber	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.16 Influência através de diásporas	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.18 Exploração de clivagens socioculturais	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.19 Promoção da agitação social	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.21 Exploração de vulnerabilidades na administração pública	x	x	x	x	x	x	x	x	x	x	10	100

		3.1.23 Explorar limites, lacunas e incertezas na legislação	x	x		x	x	x	x	x	x	x	9	90
		3.1.25 Recolha de Informações	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.31 Criação de confusão e narrativas contraditórias	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.33 Desacreditar a liderança e/ou candidatos	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.37 Controlo e interferência nos media	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.38 Campanhas de desinformação e propaganda	x	x	x	x	x	x	x	x	x	x	10	100
		3.1.40 Operações eletrónicas	x	x	x	x	x	x	x	x	x	x	10	100
	Incluídas pelos Entrevistados	3.3.1 Operações Físicas contra Infraestruturas								x			1	10
		3.3.2 Criação e exploração da dependência de infraestruturas						x					1	10
		3.3.5 Espionagem Industrial										x	1	10
		3.3.14 Organizações para militares (*Proxies*)				x							1	10
		3.3.15 Exercícios Militares						x					1	10
		3.3.22 Promoção e exploração da corrupção						x					1	10
		3.3.26 Operações clandestinas	x										1	10
		3.3.27 Infiltração	x										1	10
		3.3.34 Apoio a Atores Políticos		x			x	x	x	x		x	6	**60**
		3.3.35 Coação de Políticos e/ou Governos		x	x			x	x				4	40
		3.3.36 Aproveitamento da imigração obter influência Política										x	1	10

Quadro 20 - Matriz das unidades de contexto e de registo da quarta questão

Entrevistado	Unidade de Contexto	Unidade de Registo
E1		4.1.1; 4.1.2; 4.1.3; 4.1.4 4.2.4; 4.2.5 4.3.5; 4.3.6; 4.3.7; 4.3.8
E2	- "A fase III encontra-se numa *border line*, pois quando se corrói elementos estruturais, já se encontra a passar para uma fase de desestabilização" - com a implementação de zonas de exclusão aérea por parte de um possível agressor, a Fase V pode ser considerada numa fase de transição para a de Coação	4.1.1; 4.1.2 4.2.3; 4.2.4; 4.2.5 4.3.5; 4.3.6; 4.3.7; 4.3.8
E3	- "Fase IV no *Priming* com a utilização dos *Little Green Man* e ações de propaganda" - "Fase VII no *Desestabilisation* (considerando a atividade: combinação de operação de informação direcionada)"	4.1.1; 4.1.2; 4.1.3; 4.1.4 4.2.3; 4.2.4; 4.2.5 4.3.5; 4.3.6; 4.3.7; 4.3.8
E4	- "Fase I decisiva no *Priming*" - "Fase IV na desestabilização, pela utilização de *PsyOps*, a fim de possibilitar que o conflito a desenvolver futuramente, se torne mais curto"	4.1.1; 4.1.2 4.2.3; 4.2.4 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.3.7; 4.3.8

E5	- "Considero que a fase I e II são iniciadas na fase *priming*, podendo ser transversais durante todas as Fases de aplicação das Ameaças Híbridas"	4.1.1; 4.1.2 4.2.1; 4.2.2; 4.2.3; 4.2.4 4.3.5; 4.3.6; 4.3.7; 4.3.8
E6	- "As atividades da fase II maioritariamente no *Grey Zone*" - "Fase II na G*ray Zone*, mas já com atividades a integrar a desestabilização" - "As atividades da Fase IV podem ser consideradas na Desestabilização e na Coação, porque por vezes não é claro de onde se iniciam"	4.1.1; 4.1.2 4.2.2; 4.2.3; 4.2.4 4.3.4; 4.3.5; 4.3.6; 4.3.7; 4.3.8
E7	Não respondido	Não Respondido
E8	- "parte das atividades da fase III e Fase IV podem ser relacionadas com a fase de destabilização, retirando-se da opacidade da *Gray Zone*"	4.1.1; 4.1.2; 4.1.3; 4.1.4 4.2.3; 4.2.4; 4.2.5 4.3.6; 4.3.7; 4.3.8
E9		4.1.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.6; 4.3.7; 4.3.8
E10	- "a partir da Fase V enquadram-se num plano de conflito, pois, para impor estas atividades tem que ter impactos cinéticos"	4.1.1;4.1.2 4.2.2; 4.2.3; 4.2.4 4.3.5; 4.3.6; 4.3.7; 4.3.8

Quadro 21 - Análise de conteúdo da quarta questão

Categoria	Subcategorias	Unidades de registo	Entrevistados										Unidades de enumeração	Resultados (%)
			1	2	3	4	5	6	7	8	9	10		
Integração das Fases da Doutrina russa nas Fases das AH	Preparação	4.1.1 Fase I	x	x	x	x	x	x	N	x	x	x	9/9	**100**
		4.1.2 Fase II	x	x	x		x	x	N	x		x	7/9	**78**
		4.1.3 Fase III			x	x			N	x			3/9	33
		4.1.4 Fase IV	x		x				N	x			3/9	33
	Desestabilização	4.2.1 Fase I					x						1/9	11
		4.2.2 Fase II					x	x	N		x	x	4/9	44
		4.2.3 Fase III	x	x	x	x	x	x	N	x	x	x	9/9	**100**
		4.2.4 Fase IV	x	x	x	x	x	x	N	x	x	x	9/9	**100**
		4.2.5 Fase V	x	x	x				N	x			4/9	44
	Coação	4.3.3 Fase III				x			N				1/9	11
		4.3.4 Fase IV				x		x	N				2/9	22
		4.3.5 Fase V	x	x	x	x	x	x	N		x	x	8/9	**89**
		4.3.6 Fase VI	x	x	x	x	x	x	N	x	x	x	9/9	**100**
		4.3.7 Fase VII	x	x	x	x	x	x	N	x	x	x	9/9	**100**
		4.3.8 Fase VIII	x	x	x	x	x	x	N	x	x	x	9/9	**100**